



**CONVENZIONE PER L'AFFIDAMENTO DELLE ATTIVITA' DI REALIZZAZIONE E
GESTIONE DELL'ECOSISTEMA DATI SANITARI (EDS) PREVISTO
DALL'INVESTIMENTO M6C2 - 1.3.1 DEL PNRR**

- FASCICOLO SANITARIO ELETTRONICO –

EX ART. 12 COMMA 15-QUATER DEL DECRETO-LEGGE N. 179 DEL 2012

CUPJ51J21000070006

TRA

la Presidenza del Consiglio dei Ministri, Dipartimento per la trasformazione digitale (di seguito, per brevità, il *Dipartimento*), con sede in Roma, Largo Pietro di Brazzà 86, codice fiscale 80188230587, in persona del Capo Dipartimento *pro tempore* Ing. Mauro Minenna, nominato con decreto del Presidente del Consiglio dei ministri 29 marzo 2021, in qualità di legale rappresentante del *Dipartimento*

E

il Ministero della Salute (C.F 80242250589), con sede legale in Roma in Viale Giorgio Ribotta n.5, in persona del Segretario Generale, dott. Giovanni Leonardi, con incarico conferito con decreto del Presidente del Consiglio dei Ministri 14 maggio 2021, in qualità di legale rappresentante del Ministero

E

la SOGEI - Società Generale d'Informatica S.p.A. (di seguito, per brevità, la *Società*), con sede legale in Roma, via Mario Carucci n. 99, iscritta al registro delle imprese di Roma al n. 02327910580, coincidente con il numero di codice fiscale, partita IVA n. 01043931003, in persona del suo legale rappresentante *pro-tempore* e Amministratore Delegato, dott. Andrea Quacivì che agisce per la stipula del presente Atto in virtù dei poteri conferitigli dal Consiglio di Amministrazione come da delibera del 13 luglio 2021;

E

l'Agenzia Nazionale per i Servizi Sanitari Regionali – AGENAS (C.F. 97113690586), con sede in Roma, Via delle Puglie, 23, rappresentata dal Presidente Prof. Enrico Coscioni, in qualità di legale rappresentante dell'Agenzia

di seguito congiuntamente “*le Parti*”



VISTO il decreto-legge 30 settembre 2003, n. 269, recante disposizioni urgenti per favorire lo sviluppo e per la correzione dell'andamento dei conti pubblici e convertito con modificazioni dalla legge 24 novembre 2003, n. 326, e i relativi decreti attuativi concernenti l'istituzione del Sistema Tessera sanitaria e ricetta elettronica;

VISTO il decreto-legge 18 ottobre 2012, n. 179, e successive modifiche e integrazioni, convertito con modificazioni dalla legge 17 dicembre 2012, n. 221, recante "Ulteriori misure urgenti per la crescita del paese" e, in particolare, l'art. 12 in materia di Fascicolo sanitario elettronico e sistemi di sorveglianza nel settore sanitario;

VISTO il decreto-legge 21 giugno 2013, n. 69, recante "Disposizioni urgenti per il rilancio dell'economia", convertito con modificazioni dalla legge 9 agosto 2013, n. 98;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);

VISTO il Codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196, come modificato dal decreto legislativo 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)";

VISTA l'Intesa tra il Governo, le Regioni e le Province autonome di Trento e Bolzano, sancita dalla Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e Bolzano nella seduta del 7 luglio 2016 (Rep. Atti. n. 123/CSR), sul Patto per la sanità digitale, che attribuisce alla Cabina di Regia del NSIS la governance del medesimo Patto;

VISTO l'Accordo tra il Governo, le Regioni e le Province autonome di Trento e Bolzano sancito dalla Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e Bolzano nella seduta del 7 luglio 2016 (Rep. Atti n. 116/CSR), per l'evoluzione del Nuovo Sistema Informativo Sanitario Nazionale ("NSIS") che attribuisce le funzioni di indirizzo, coordinamento e controllo dell'evoluzione del NSIS alla Cabina di Regia NSIS;

VISTO il decreto del Ministero dell'economia e delle finanze, di concerto con il Ministero della salute, del 4 agosto 2017, recante "Modalità tecniche e servizi telematici resi disponibili dall'infrastruttura nazionale per l'interoperabilità del Fascicolo sanitario elettronico (FSE) di cui all'art. 12, comma 15-ter del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221";

VISTO il decreto del Ministero dell'economia e finanze, di concerto con Ministero della salute, del 25 ottobre 2018, recante "Modifica del decreto ministeriale 4 agosto 2017, concernente le modalità tecniche e i servizi telematici resi disponibili dall'infrastruttura nazionale per l'interoperabilità del Fascicolo sanitario elettronico (FSE)";

VISTO il decreto-legge 19 maggio 2020, n. 34, recante "Misure urgenti in materia di salute, sostegno al lavoro e all'economia, nonché di politiche sociali connesse all'emergenza epidemiologica da COVID-19", convertito con modificazioni dalla legge 17 luglio 2020, n. 77;



VISTA la legge 7 agosto 1990, n. 241, e ss.mm.ii, recante “Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi”;

VISTO il decreto legislativo 18 aprile 2016, n. 50, ss.mm.ii, recante “Codice dei contratti pubblici”;

VISTA la legge 30 dicembre 2020, n. 178, recante disposizioni sul Bilancio di previsione dello Stato per l’anno finanziario 2021 e bilancio pluriennale per il triennio 2021-2023, in G.U. n. 322 del 30 dicembre 2020, che, all’art. 1, comma 1043, prevede l’istituzione del sistema informatico di registrazione e conservazione di supporto dalle attività di gestione, monitoraggio, rendicontazione e controllo delle componenti del PNRR;

VISTO il decreto-legge 1° marzo 2021, n. 22, recante disposizioni urgenti in materia di riordino delle attribuzioni dei Ministeri, e, in particolare, l’art. 8 relativo alle “Funzioni in materia di innovazione tecnologica e transizione digitale e istituzione del Comitato interministeriale per la transizione digitale” (CITD), convertito con modificazioni dalla legge 22 aprile 2021, n. 55;

VISTO il Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021, che istituisce il dispositivo di ripresa e resilienza (regolamento RRF) con l’obiettivo specifico di fornire agli Stati membri il sostegno finanziario al fine di conseguire le tappe intermedie e gli obiettivi delle riforme e degli investimenti stabiliti nei loro piani di ripresa e resilienza;

VISTO il decreto-legge 6 maggio 2021, n. 59, recante “Misure urgenti relative al Fondo complementare al Piano nazionale di ripresa e resilienza e altre misure urgenti per gli investimenti”;

VISTO il decreto-legge del 31 maggio 2021, n. 77, convertito, con modificazioni, dalla legge n. 29 luglio 2021, n. 108 e recante l’individuazione della Governance del Piano nazionale di ripresa e resilienza e delle prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure;

VISTO il “Piano Nazionale di Ripresa e Resilienza” (di seguito anche “PNRR” o “Piano”) presentato alla Commissione europea in data 30 giugno 2021 e approvato in data 13 luglio 2021 con Decisione di esecuzione del Consiglio dell’Unione europea;

VISTO il decreto-legge 9 giugno 2021, n. 80, convertito con modificazioni dalla legge 6 agosto 2021, n. 113, recante “Misure urgenti per il rafforzamento della capacità amministrativa delle pubbliche amministrazioni funzionale all’attuazione del Piano nazionale di ripresa e resilienza (PNRR) e per l’efficienza della giustizia”;

VISTO il Decreto del Presidente del Consiglio dei ministri 9 luglio 2021 recante l’individuazione delle amministrazioni centrali titolari di interventi previsti dal PNRR ai sensi dell’articolo 8, comma 1, del decreto-legge 31 maggio 2021, n. 77;

VISTO il Decreto del Ministero dell’Economia e delle Finanze del 6 agosto 2021 recante l’assegnazione delle risorse finanziarie previste per l’attuazione degli interventi del piano Nazionale di Ripresa e Resilienza (PNRR) e ripartizione di traguardi e obiettivi per scadenze semestrali di rendicontazione;

CONSIDERATA la “Tabella A - PNRR - ITALIA QUADRO FINANZIARIO PER AMMINISTRAZIONI TITOLARI” allegata al Decreto del Ministero dell’Economia e delle Finanze del 6 agosto 2021, che prevede per il sub-investimento “1.3.1 Rafforzamento dell’infrastruttura tecnologica e degli strumenti per la raccolta, l’elaborazione, l’analisi dei dati e la simulazione (FSE)” l’importo complessivo di euro 1.379.989.999,93, di cui, per i “progetti in essere”, un importo pari a euro 569.600.000,00 e per i “nuovi progetti”, oggetto del presente accordo, euro 810.389.999,93;

RILEVATA la necessità di attuare le attività di cui l’accordo tra PCM-DTD e Ministero della Salute



relative all’attuazione dell’intervento “1.3.1 Rafforzamento dell’infrastruttura tecnologica e degli strumenti per la raccolta, l’elaborazione, l’analisi dei dati e la simulazione (FSE)” per l’importo complessivo di euro 810.389.999,93, meglio specificato nell’Allegato 1 – Piano operativo Fascicolo Sanitario Elettronico (FSE) allegato al citato Accordo sottoscritto il 21 settembre 2021 tra PCM-DTD e Ministero della Salute;

CONSIDERATA la Raccomandazione del Consiglio sul programma nazionale di riforma 2020 e sul Programma di stabilità 2020 dell’Italia del 20 maggio 2020;

CONSIDERATE le indicazioni relative al raggiungimento di Milestone e Target contenute negli allegati alla Decisione di esecuzione del Consiglio relativa all’approvazione della valutazione del piano per la ripresa e la resilienza dell’Italia;

CONSIDERATE le indicazioni relative al raggiungimento di Milestone e Target europei allegati del D.M. MEF 6 agosto 2021;

VISTO l’articolo 6 del decreto Legge 31 maggio 2021, n. 77, convertito con modificazioni dalla legge 29 luglio 2021, n. 108, ai sensi del quale sono attribuiti al Servizio centrale per il PNRR, quale punto di contatto nazionale per la Commissione europea ai sensi dell’articolo 22 del Regolamento (UE) 2021/241, funzioni di coordinamento operativo, monitoraggio, rendicontazione e controllo del PNRR;

RITENUTO di poter conseguire le finalità progettuali previste per la realizzazione del repository e del gateway di cui al FSE mediante la sottoscrizione di una convenzione che disciplini lo svolgimento in collaborazione delle attività e che includa la chiara ripartizione delle responsabilità e obblighi connessi alla gestione, controllo e rendicontazione in adempimento a quanto prescritto dalla regolamentazione comunitaria di riferimento e dal decreto-legge del 31 maggio 2021, n. 77, e secondo il Sistema di gestione e controllo del PNRR;

VISTA la legge 7 agosto 1990, n. 241, e successive modifiche e integrazioni e, in particolare, l’articolo 15 che prevede la possibilità per le amministrazioni pubbliche di concludere tra loro accordi, sottoscritti con firma digitale, per disciplinare lo svolgimento in collaborazione di attività di interesse comune;

VISTO l’articolo 5, comma 6, del decreto legislativo 18 aprile 2016, n. 50, ai sensi del quale il Codice dei contratti pubblici non trova applicazione rispetto ad accordi conclusi esclusivamente tra due o più amministrazioni aggiudicatrici al ricorrere di tutte le condizioni ivi previste;

CONSIDERATO che l’ANAC, con la delibera n. 567 del 31 maggio 2017, ha puntualizzato al riguardo che “*(...) la disciplina dettata dal citato art. 5, comma 6, del d.lgs. 50/2016, indica in maniera tassativa i limiti entro i quali detti accordi possono essere conclusi, affinché possa ritenersi legittima l’esonere dal Codice. Si stabilisce, quindi, che la cooperazione deve essere finalizzata al raggiungimento di obiettivi comuni agli enti interessati e che la stessa deve essere retta esclusivamente da considerazioni inerenti all’interesse pubblico*” e che “*La norma contempla, quindi, una specifica disciplina degli accordi tra soggetti pubblici, quale istituto già previsto in passato e in linea generale dall’art. 15 della l. 241/1990, ai sensi del quale «anche al di fuori delle ipotesi previste dall’articolo 14, le amministrazioni pubbliche possono sempre concludere tra loro accordi per disciplinare lo svolgimento in collaborazione di attività di interesse comune».* Si tratta, com’è evidente, di un modello convenzionale di svolgimento delle pubbliche funzioni, finalizzato alla collaborazione tra amministrazioni pubbliche.”;

CONSIDERATO, che il fine perseguito è un interesse di natura pubblica a beneficio e vantaggio della collettività, che dalla presente convenzione tra le parti discende una reale suddivisione di



compiti e responsabilità in relazione alle rispettive funzioni istituzionali e che, pertanto gli enti e le Amministrazioni coinvolte forniranno il proprio rispettivo contributo;

CONSIDERATO, nello specifico, che rappresenta interesse comune delle parti collaborare in funzione della realizzazione del PNRR e che la collaborazione tra le parti risulta essere lo strumento più idoneo per il perseguimento dei reciproci fini istituzionali e, in particolare, per la realizzazione del Progetto che richiede un supporto mirato così come sancito dalle diverse disposizioni sopra riportate;

CONSIDERATO, altresì, che il Progetto è realizzato con le reciproche risorse interne portatrici di competenze e *know how* specifico, e che le conseguenti movimentazioni finanziarie costituiscono ristoro delle eventuali spese effettivamente sostenute per le attività svolte, essendo escluso il pagamento di un corrispettivo, comprensivo di un margine di guadagno;

RITENUTO che, nel caso di specie, ricorrono i presupposti per attivare una convenzione tra Enti Pubblici, ai sensi dell'articolo 5 del decreto legislativo 18 aprile 2016, n. 50, nel rispetto delle vigenti normative e della giurisprudenza consolidata e che si rende necessario, pertanto, disciplinare gli aspetti operativi ed economico-finanziari della collaborazione di cui trattasi;

RICHIAMATO il verbale della seduta del 30 giugno 2021 del Comitato Interministeriale sulla Transizione Digitale (CITD) operante presso la Presidenza del Consiglio dei Ministri, che ha approvato il sistema di governance del sub-intervento M6C2 1.3.1- Fascicolo Sanitario Elettronico del PNRR;

CONSIDERATO che il sistema di governance individuato dal CITD prevede la creazione di un Comitato Guida Interministeriale, composto dai Ministri della salute, dell'economia e delle finanze e dell'innovazione tecnologica e transizione digitale quale principale organo decisionale responsabile per la definizione dell'indirizzo, degli obiettivi, dei tempi di realizzazione, dell'allocazione delle risorse e del monitoraggio delle attività, di un Gruppo di lavoro FSE con funzioni di coordinamento per assicurare che la progettualità e l'esecuzione siano coerenti con l'indirizzo politico, le tempistiche del PNRR e le esigenze dei territori, che coordina il lavoro del partner scientifico e dell'Unità di progetto FSE, attuatore con responsabilità per l'esecuzione materiale degli interventi;

CONSIDERATO che, pertanto, i compiti di attuazione per il sub-investimento M6C2 1.3.1 - Fascicolo Sanitario Elettronico, in base alle indicazioni del CITD, possono essere svolti dal Dipartimento per la trasformazione digitale (DTD) su delega del Ministero della salute e in coerenza con il delineato modello di governance;

CONSIDERATO che l'investimento previsto dal PNRR (M6C2 1.3.1) si compone di linee di attività relative a: a) repository centrale, digitalizzazione documentale, servizi e interfaccia user-friendly; b) adozione e utilizzo FSE da parte delle Regioni; c) utilizzo del Fondo per il finanziamento degli investimenti e lo sviluppo infrastrutturale - Tessera Sanitaria Elettronica, e che quest'ultima si riferisce a progetti già in essere;

CONSIDERATO che il predetto sub-investimento 1.3.1.c) utilizzo del Fondo per il finanziamento degli investimenti e lo sviluppo infrastrutturale - Tessera Sanitaria Elettronica è riconducibile a progetti già in essere, la cui attuazione rimane attribuita al MEF;

RICHIAMATO il verbale della seduta del 11 ottobre 2021 del Comitato Interministeriale sulla Transizione Digitale (CITD) operante presso la Presidenza del Consiglio dei Ministri, che ha approvato il piano architettonico del sub-intervento M6C2 1.3.1- Fascicolo Sanitario Elettronico del PNRR che prevede la creazione di un nuovo Ecosistema Dati Sanitari comprensivo di un repository centrale in dati FHIR e una gateway presso le strutture sanitarie che alimenti il repository centrale;



VISTO il decreto del Presidente del Consiglio dei Ministri 11 febbraio 2014, n. 59, pubblicato in G.U. n. 82 dell'8 aprile 2014, sul regolamento di organizzazione del Ministero della salute;

VISTO il decreto del Presidente del Consiglio dei Ministri 19 giugno 2019, pubblicato in G.U. n. 199 del 26 agosto 2019, concernente la modifica al decreto del Presidente del Consiglio dei Ministri 1° ottobre 2012, recante "Ordinamento delle strutture generali della Presidenza del Consiglio dei ministri", per la istituzione del Dipartimento per la trasformazione digitale quale struttura generale della Presidenza del Consiglio dei ministri;

VISTA la nota prot. 16527 del 14 settembre 2021 con la quale il Ministro della Salute ha comunicato al Ministro per l'innovazione tecnologica e la transizione digitale l'intendimento di avvalersi del Dipartimento per la trasformazione digitale quale soggetto attuatore dell'intervento di investimento PNRR M6C2 1.3.1 Fascicolo Sanitario Elettronico a titolarità del Ministero della salute;

VISTA la nota prot. MIN_ITTD-0001864 del 15 settembre 2021 con la quale il Ministro per l'innovazione tecnologica e la transizione digitale ha confermato al Ministro della Salute la possibilità di avvalersi del Dipartimento per la trasformazione digitale quale soggetto attuatore dell'intervento di investimento PNRR M6C2 1.3.1 Fascicolo Sanitario Elettronico a titolarità del Ministero della salute;

TENUTO CONTO che, essendo la linea di intervento del PNRR M6C2 1.3.1 realizzata in modalità a regia, l'Amministrazione attuatrice è responsabile della richiesta del Codice Unico di Progetto (CUP) da associare a ciascun progetto d'investimento pubblico come previsto dall'art. 11 della legge 16 gennaio 2003, n. 3 e che, a tal fine, dovrà attivare la procedura di richiesta del suddetto codice in fase attuativa e solo a seguito della sottoscrizione del presente accordo, nel rispetto delle procedure previste dal citato articolo 11 della legge 16 gennaio 2003, n. 3, con contestuale comunicazione all'Amministrazione titolare;

VISTO il decreto del Presidente del Consiglio dei ministri 1° ottobre 2012, recante l'ordinamento generale della Presidenza del Consiglio dei ministri, come modificato dal predetto decreto del Presidente del Consiglio dei ministri 19 giugno 2019, e, in particolare, l'articolo 24-ter, ai sensi del quale il Dipartimento per la trasformazione digitale è preposto alla promozione e coordinamento delle azioni del Governo finalizzate alla definizione di una strategia unitaria in materia di trasformazione digitale e di modernizzazione del Paese attraverso le tecnologie digitali e, a tal fine, dà attuazione alle direttive del Presidente in materia e assicura il coordinamento e l'esecuzione dei programmi di trasformazione digitale delle pubbliche amministrazioni, anche fornendo supporto tecnico alle attività di implementazione di specifiche iniziative previste dall'Agenda digitale italiana, secondo i contenuti presenti nell'Agenda digitale Europea;

VISTO il decreto del Presidente del Consiglio dei ministri 29 marzo 2021, con cui è stato conferito all'Ing. Mauro Minenna l'incarico di Capo del Dipartimento per la trasformazione digitale a decorrere dal 31 marzo 2021;

VISTO il decreto del Presidente del Consiglio dei ministri 14 maggio 2021 con i quale il dott. Giovanni Leonardi è stato nominato Segretario Generale del Ministero della Salute;

VISTO l'articolo 83, comma 15, del decreto-legge 25 giugno 2008, n. 112, convertito con modificazioni dalla legge 6 agosto 2008, n. 133, secondo cui i diritti dell'azionista della Sogei S.p.A. sono esercitati dal Ministero dell'Economia e delle Finanze – Dipartimento del Tesoro;

VISTO l'articolo 26 dello statuto della Società, che prevede l'affidamento al Ministero dell'Economia e delle Finanze – Dipartimento delle Finanze dell'esercizio del controllo analogo;

VISTO l'art. 4, comma 3-ter del decreto-legge 6 luglio 2012, n. 95 convertito con modificazioni



dall’art. 1, comma 1 della legge 7 agosto 2012, n. 135, secondo il quale Sogei S.p.A., sulla base di apposita convenzione disciplinante i relativi rapporti nonché i tempi e le modalità di realizzazione delle attività, si avvale di Consip S.p.A. nella sua qualità di centrale di committenza, per le acquisizioni di beni e servizi;

VISTO il Decreto legislativo, n. 82 del 7 marzo 2005 “Codice dell’amministrazione digitale” (CAD) e successive modifiche, che attribuisce all’Agenzia per l’Italia Digitale la responsabilità dei pareri tecnici sugli schemi di contratti e accordi quadro da parte delle pubbliche amministrazioni centrali concernenti l’acquisizione di beni e servizi relativi a sistemi informativi automatizzati per quanto riguarda la congruità tecnico-economica;

VISTO l’art. 4, comma 1, dello Statuto di Sogei S.p.A., ai sensi del quale la Società ha per oggetto prevalente la prestazione di servizi strumentali all’esercizio delle funzioni pubbliche attribuite al Ministero dell’economia e delle finanze;

VISTO l’art. 4, comma 2, dello Statuto di Sogei S.p.A., ai sensi del quale la Società ha, altresì, quale oggetto lo svolgimento, nel rispetto della normativa vigente, di ogni attività di natura informatica per conto dell’Amministrazione pubblica centrale;

VISTO l’art. 26, comma 7 , dello Statuto di Sogei S.p.A. il quale prevede che per l’affidamento diretto delle attività di cui al predetto art. 4 comma 4, la Società sottoscrive con le Pubbliche Amministrazioni affidanti apposite convenzioni o contratti esecutivi previa comunicazione al Dipartimento delle Finanze e all’Azionista ai fini della verifica del mantenimento dell’equilibrio economico – finanziario;

VISTA la nota del Dipartimento delle Finanze del Ministero dell’economia e delle finanze, prot. n. 25463/2022 del 23 maggio, con la quale il suddetto Dipartimento ha espresso il nulla osta alla stipula della convenzione in oggetto da parte di Sogei S.p.A.;

VISTA altresì la nota del Dipartimento del Tesoro del Ministero dell’economia e delle finanze, prot. DT 49849 - del 26/05/2022, con il quale il suddetto Dipartimento ha espresso la mancanza di motivi ostativi alla stipula della Convenzione in oggetto da parte di Sogei S.p.A.;

VISTA la nota n. 361-P, del 14 aprile 2022, con la quale la Presidenza del Consiglio dei Ministri - Dipartimento per la Trasformazione Digitale ha richiesto ad AgID il parere di congruità tecnico-economica ai sensi dell’art. 14bis, comma 2, lett. f) del C.A.D;

VISTO il parere AgID n. 11/2022 riguardante la convenzione in oggetto, reso ai sensi dell’art. 14bis, comma 2, lett. f) del C.A.D, sopra citato;

VISTO il decreto legislativo 30 giugno 1993, n. 266 e s.m.i. recante “Riordinamento del Ministero della sanità” che all’art. 5 ha istituito l’Agenzia Nazionale per i Servizi Sanitari Regionali – AGENAS, con compiti di supporto delle attività regionali, di valutazione comparativa dei costi e dei rendimenti dei servizi resi ai cittadini e di segnalazione di disfunzioni e sprechi nella gestione delle risorse personali e materiali e nelle forniture, di trasferimento dell’innovazione e delle sperimentazioni in materia sanitaria.

VISTO il decreto legge 14 giugno 2021 n. 82, convertito con modificazioni dalla legge 4 agosto 2021 n. 109 recante “Disposizioni urgenti in materia di cybersicurezza, definizione dell’architettura nazionale di cybersicurezza e istituzione dell’Agenzia per la cybersicurezza nazionale” ai sensi del quale l’Agenzia (ACN) è preposta alla promozione della cultura della sicurezza cibernetica, alla consapevolezza del settore pubblico, privato e della società civile sui rischi e le minacce cyber;

VISTO il decreto legislativo 30 luglio 1999 n. 286 recante “Riordino e potenziamento dei meccanismi e strumenti di monitoraggio e valutazione dei costi, dei rendimenti e dei risultati dell’attività svolta dalle amministrazioni pubbliche, a norma dell’articolo 11 della L. 15 marzo 1997,



n. 59” e in particolare l’art. 2;

VISTA la legge 31 dicembre 2009, n. 196, recante “Legge di contabilità e finanza pubblica”, come modificata dalla legge 7 aprile 2011, n. 39, recante “Modifiche alla legge 31 dicembre 2009, n. 196, conseguenti alle nuove regole adottate dall’Unione europea in materia di coordinamento delle politiche economiche degli Stati membri”;

VISTA la legge 13 agosto 2010, n. 136, e s.m.i., recante “Piano straordinario contro le mafie, nonché delega al governo in materia di normativa antimafia”;

VISTO il decreto legislativo 30 giugno 2011, n. 123, concernente “Riforma dei controlli di regolarità amministrativa e contabile e potenziamento dell’attività di analisi e valutazione della spesa, a norma dell’articolo 49 della legge 31 dicembre 2009, n. 196”;

VISTO il decreto legislativo 14 marzo 2013, n. 33 recante “Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni”;

VISTO il decreto-legge 16 luglio 2020, n. 76, convertito, con modificazioni, dalla legge 11 settembre 2020, n. 120, recante “Misure urgenti per la semplificazione e l’innovazione digitale” e in particolare l’articolo 41, comma 1, che ha modificato l’art.11 della legge 16 gennaio 2003, n.3, istitutiva del CUP prevedendo che “Gli atti amministrativi anche di natura regolamentare adottati dalle Amministrazioni di cui all’articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, che dispongono il finanziamento pubblico o autorizzano l’esecuzione di progetti d’investimento pubblico, sono nulli in assenza dei corrispondenti codici di cui al comma 1 che costituiscono elemento essenziale dell’atto stesso”;

VISTO il Regolamento (UE) 2018/1046 del Parlamento europeo e del Consiglio del 18 luglio 2018 che stabilisce le regole finanziarie applicabili al bilancio generale dell’Unione, che modifica i regolamenti (UE) n. 1296/2013, (UE) n. 1301/2013, (UE) n. 1303/2013, (UE) n. 1304/2013, (UE) n. 1309/2013, (UE) n. 1316/2013, (UE) n. 223/2014, (UE) n. 283/2014 e la decisione n. 541/2014/UE e abroga il regolamento (UE, Euratom) n. 966/2012;

VISTO il Regolamento (UE) 2020/852 del Parlamento europeo e del Consiglio, del 18 giugno 2020 relativo all’istituzione di un quadro che favorisce gli investimenti sostenibili e recante modifica del regolamento (UE) 2019/2088, e in particolare l’art.17 “Danno significativo agli obiettivi ambientali”;

VISTO il Regolamento (UE, Euratom) 2020/2092 del Parlamento europeo e del Consiglio, del 16 dicembre 2020, relativo a un regime generale di condizionalità per la tutela del bilancio dell’Unione;

VISTO il Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio, del 12 febbraio 2021, che istituisce il dispositivo per la ripresa e la resilienza;

CONSIDERATO che l’art. 5, comma 2 del Regolamento (UE) 2021/241, prevede, “Il dispositivo finanziaria unicamente le misure che rispettano il principio «non arrecare un danno significativo»”;

VISTO il Piano Nazionale di Ripresa e Resilienza per l’Italia (di seguito anche “PNRR” o “Piano”) presentato alla Commissione europea in data 30 giugno 2021 ai sensi dell’art. 18 del Regolamento (UE) 2021/241;

VISTA la decisione di esecuzione del Consiglio ECOFIN del 13 luglio 2021, recante “Approvazione della Valutazione del Piano per la ripresa e resilienza dell’Italia”, notificata all’Italia dal Segretariato generale del Consiglio con nota LT161/21, del 14 luglio 2021;



CONSIDERATE le indicazioni relative al raggiungimento di Milestone e Target contenute negli allegati alla Decisione di esecuzione del Consiglio relativa alla “Approvazione della valutazione del Piano per la ripresa e la resilienza dell’Italia”;

VISTI i principi trasversali previsti dal PNRR, quali, tra l’altro, il principio del contributo all’obiettivo climatico e digitale (c.d. tagging), il principio di parità di genere e l’obbligo di protezione e valorizzazione dei giovani;

VISTA la legge 30 dicembre 2020, n.178, recante “Bilancio di previsione dello Stato per l’anno finanziario 2021 e bilancio pluriennale per il triennio 2021-2023” e, in particolare:

- l’articolo 1, comma 1042 ai sensi del quale con uno o più decreti del Ministro dell’economia e delle finanze sono stabilite le procedure amministrativo-contabili per la gestione delle risorse di cui ai commi da 1037 a 1050, nonché le modalità di rendicontazione della gestione del Fondo di cui al comma 1037;
- l’articolo 1, comma 1043, secondo periodo ai sensi del quale, al fine di supportare le attività di gestione, di monitoraggio, di rendicontazione e di controllo delle componenti del Next Generation EU, il Ministero dell’economia e delle finanze - Dipartimento della Ragioneria generale dello Stato sviluppa e rende disponibile un apposito sistema informatico;

VISTO il decreto-legge 6 maggio 2021, n. 59, convertito con modificazioni dalla legge 1° luglio 2021, n.101, recante “Misure urgenti relative al Fondo complementare al Piano nazionale di ripresa e resilienza e altre misure urgenti per gli investimenti”;

VISTO l’art. 9, primo comma, del decreto-legge del 31 maggio 2021, n. 77, che attualmente prevede che *“Alla realizzazione operativa degli interventi previsti dal PNRR provvedono le Amministrazioni centrali, le Regioni, le Province autonome di Trento e di Bolzano e gli enti locali, sulla base delle specifiche competenze istituzionali, ovvero della diversa titolarità degli interventi definita nel PNRR, attraverso le proprie strutture, ovvero avvalendosi di soggetti attuatori esterni individuati nel PNRR, ovvero con le modalità previste dalla normativa nazionale ed europea vigente”*;

VISTO l’art. 51 del decreto-legge 26/10/2019, n. 124, Convertito in legge, con modificazioni, dall’art. 1, comma 1, della legge 19 dicembre 2019, n. 157 recante “Disposizioni urgenti in materia fiscale e per esigenze indifferibili”, il cui comma 2 prevede che *“In coerenza con gli obiettivi generali indicati al comma 1, possono avvalersi della Società di cui all’articolo 83, comma 15, del decreto-legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133: ... f-quater) il Ministero della salute, al fine della realizzazione dell’Ecosistema Dati Sanitari (EDS) di cui all’articolo 12 del decreto-legge 18 ottobre 2012, n. 179, convertito con modificazioni dalla legge 17 dicembre 2012, n. 221 ... f-quinquies) l’Agenzia nazionale per i servizi sanitari regionali (AGENAS), nella qualità di Agenzia nazionale per la sanità digitale, per la gestione dell’EDS di cui all’articolo 12 del decreto-legge n. 179 del 2012, convertito, con modificazioni, dalla legge n. 221 del 2012 e per la messa a disposizione alle strutture sanitarie e sociosanitarie di specifiche soluzioni software, necessarie ad assicurare, coordinare e semplificare la corretta e omogenea formazione dei documenti e dei dati che alimentano il Fascicolo sanitario elettronico (FSE)” .*

VISTO il decreto del Ministro dell’economia e delle finanze 6 agosto 2021, adottato ai sensi dell’articolo 7, primo comma, ultimo periodo, del decreto-legge 9 giugno 2021, n. 80, recante l’individuazione delle amministrazioni titolari di interventi previsti nel PNRR, e i target e le milestone da raggiungere per ciascun investimento e sub-investimento;



VISTO il decreto del Presidente del Consiglio dei ministri 9 luglio 2021, che individua la Presidenza del Consiglio dei ministri - Ministro per l'innovazione tecnologica e la transizione digitale quale struttura presso la quale istituire l'Unità di Missione ai sensi dell'articolo 8, comma 1, del decreto-legge 31 maggio 2021, n. 77,

VISTO il decreto del Presidente del Consiglio dei ministri 30 luglio 2021, che istituisce, nell'ambito del Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri, l'Unità di missione di livello dirigenziale ai sensi dell'art.8, comma, 1 del decreto-legge 31 maggio 2021, n. 77 e del decreto del Presidente del Consiglio dei ministri del 9 luglio 2021;

VISTO il decreto del Ministro senza portafoglio per l'innovazione tecnologica e la transizione digitale di concerto con il Ministro dell'economia e delle finanze 24 settembre 2021, recante l'organizzazione interna della predetta Unità di missione;

VISTO il decreto del Presidente del Consiglio dei ministri del 15 settembre 2021, recante le modalità, le tempistiche e gli strumenti per la rilevazione dei dati di attuazione finanziaria, fisica e procedurale nonché dei milestone e target degli investimenti e delle riforme e di tutti gli ulteriori elementi informativi previsti nel PNRR necessari per la rendicontazione alla Commissione Europea;

VISTO il decreto-legge 21 settembre 2021, n.121 e in particolare l'art.10 recante "Procedure di attuazione del Piano Nazionale di Ripresa e Resilienza e modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni";

VISTO il decreto del Ministro dell'economia e delle finanze dell'11 ottobre 2021, che definisce procedure amministrativo contabili in ordine alla gestione del Fondo di rotazione, al flusso degli accrediti, alle richieste di pagamento, alle modalità di rendicontazione per l'attuazione dell'iniziativa Next Generation EU Italia;

VISTO il decreto-legge 6 novembre 2021, n. 152 recante "Disposizioni urgenti per l'attuazione del Piano Nazionale di Ripresa e Resilienza (PNRR) e per la prevenzione delle infiltrazioni mafiose";

VISTI, in particolare, gli articoli 9 e 10 del decreto-legge 31 maggio 2021 n. 77, ai sensi dei quali ciascuna Amministrazione centrale titolare di interventi previsti nel Piano può, rispettivamente, avvalersi del supporto tecnico-operativo assicurato per il PNRR da società a prevalente partecipazione pubblica, ovvero, del supporto tecnico-operativo di società in house qualificate ai sensi dell'articolo 38 del decreto legislativo 18 aprile 2016, n. 50;

VISTO l'accordo di collaborazione tra il Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei Ministri ed il Ministero della Salute, stipulato in data 21 settembre 2021 ai sensi dell'art. 15 della legge 7 agosto 1990 n. 241, con il quale vengono disciplinate le modalità di collaborazione ai fini della realizzazione del Fascicolo Sanitario Elettronico, così come dettagliate nell'Allegato 1 al citato accordo, che garantiscono un'attuazione più efficace ed efficiente in linea con i target del PNRR in coerenza con gli interessi comuni delle parti e in conformità alle norme di riferimento;

VISTO, altresì l'art. 12 comma 15-quater del decreto-legge 18 ottobre 2012, n. 179, convertito con modificazioni in legge 17 dicembre 2012, n. 221, così come successivamente modificato dall'art. 21 del decreto-legge 27 gennaio 2022, n.4, convertito con modificazioni in legge 28 marzo 2022, n. 25 ai sensi del quale " *Al fine di garantire il coordinamento informatico e assicurare servizi omogenei sul territorio nazionale per il perseguimento delle finalita' di cui al comma 2 il Ministero della Salute, d'intesa con la struttura della Presidenza del Consiglio dei ministri competente per l'innovazione tecnologica e la transizione digitale, assicurando l'adeguatezza delle infrastrutture tecnologiche e la sicurezza cibernetica in raccordo con l'Agenzia per la cybersicurezza nazionale,*



cura la realizzazione dell'Ecosistema Dati Sanitari (di seguito EDS), avvalendosi della societa' di cui all'articolo 83, comma 15, del decreto-legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133, con cui stipula apposita convenzione. L'EDS è alimentato dai dati trasmessi dalle strutture sanitarie e socio-sanitarie, dagli enti del Servizio sanitario nazionale e da quelli resi disponibili tramite il sistema Tessera Sanitaria. Il Ministero della salute è titolare del trattamento dei dati raccolti e generati dall'EDS, la cui gestione operativa è affidata all'AGENAS, che la effettua in qualita' di responsabile del trattamento per conto del predetto Ministero e che all'uopo si avvale, mediante la stipula di apposita convenzione, della società di cui all'articolo 83, comma 15, del decreto-legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133. Con decreto del Ministro della salute, adottato di concerto con il Ministro delegato per l'innovazione tecnologica e la transizione digitale e con il Ministero dell'economia e delle finanze, e acquisiti i pareri dell'Autorita' garante per la protezione dei dati personali e dell'Agenzia per la cybersicurezza nazionale, sono individuati i contenuti dell'EDS, le modalita' di alimentazione dell'EDS, nonché i soggetti che hanno accesso all'EDS, le operazioni eseguibili e le misure di sicurezza per assicurare i diritti degli interessati. Al fine di assicurare, coordinare e semplificare la corretta e omogenea formazione dei documenti e dei dati che alimentano il FSE, l'AGENAS, d'intesa con la struttura della Presidenza del Consiglio dei ministri competente per l'innovazione tecnologica e la transizione digitale e avvalendosi della societa' di cui all'articolo 83, comma 15, del decreto-legge n. 112 del 2008, convertito, con modificazioni, dalla legge n. 133 del 2008, rende disponibili alle strutture sanitarie e socio-sanitarie specifiche soluzioni da integrare nei sistemi informativi delle medesime strutture con le seguenti funzioni:

- a) di controllo formale e semantico dei documenti e dei corrispondenti dati correlati prodotti dalle strutture sanitarie per alimentare FSE;*
- b) di conversione delle informazioni secondo i formati standard di cui al comma 15-octies;*
- c) di invio dei dati da parte della struttura sanitaria verso l'EDS e, se previsto dal piano di attuazione del potenziamento del FSE di cui al comma 15-bis, verso il FSE della regione territorialmente competente per le finalita' di cui alla lettera a-bis) del comma 2";*

CONSIDERATA la strategicità del progetto FSE e che, per quanto sopra detto, Sogei S.p.A. è il soggetto normativamente legittimato ad attuare il Progetto relativo al Fascicolo Sanitario Elettronico (FSE);

RAVVISATA l'urgenza, alla luce dei target indicati dal PNRR per il predetto sub-investimento M6C2 1.3.1 - Fascicolo Sanitario Elettronico, di procedere celermente all'avvio della misura citata e considerato di poter conseguire i target indicati mediante la stipula di una convenzione rispettivamente con la Società generale d'informatica S.p.A. (Sogei) per la realizzazione del EDS e con AGENAS per la gestione del citato EDS e con la Società generale d'informatica S.p.A. (Sogei) per la realizzazione del gateway e con AGENAS per la sua messa a disposizione e quindi per la complessiva attuazione del suddetto investimento.

tanto premesso le Parti, come sopra individuate, convengono e stipulano quanto segue.

Articolo 1

(PREMESSE, ALLEGATI E DEFINIZIONI)

1. Le premesse e gli allegati costituiscono parte integrante e sostanziale della presente *Convenzione*.
2. Ai fini della presente *Convenzione* si intende per:
 - a) *Amministrazione titolare*: Ministero della Salute;
 - b) *Soggetto attuatore*: PCM-Dipartimento per la trasformazione digitale;



- c) *Soggetto gestore*: Agenzia Nazionale per i Servizi Sanitari Regionali, incaricata della gestione dell'EDS;
- d) *Società*: SOGEI - Società Generale d'Informatica S.p.A, incaricata della realizzazione e gestione per conto di AGENAS dell'EDS;
- e) *Consip*: concessionaria di servizi informativi pubblici – Società per Azioni partecipata al 100% dal Ministero dell'Economia e delle Finanze, la quale, come sopra specificato, ai sensi dell'art. 4, comma 3-ter del decreto-legge 6 luglio 2012, n. 95 convertito con modificazioni dall'art. 1, comma 1 della legge 7 agosto 2012, n. 135, sulla base di apposita convenzione, nella sua qualità di centrale di committenza, per le acquisizioni di beni e servizi, acquisisce gli stessi per conto di Sogei;
- f) *Convenzione*: il presente documento stipulato fra le Parti;
- g) *Intervento*: “la Realizzazione e gestione di un archivio centrale interoperabile come definito nel sub-investimento M6C2 - 1.3.1 (“Fascicolo Sanitario Elettronico”)” del Piano nazionale di ripresa e resilienza ovvero Ecosistema Dati Sanitari;
- h) *Gateway*: specifica soluzione da integrare nei sistemi informativi delle medesime strutture con le seguenti funzioni:
 - i. di controllo formale e semantico dei documenti e dei corrispondenti dati correlati prodotti dalle strutture sanitarie per alimentare FSE;
 - ii. di conversione delle informazioni secondo i formati standard di cui al comma 15-octies dell'art. 12 del decreto legge 18 ottobre 2012, n. 179;
 - iii. di invio dei dati da parte della struttura sanitaria verso l'EDS e, se previsto dal piano di attuazione del potenziamento del FSE, di cui al comma 15-bis, dell'art. 12 del decreto legge 18 ottobre 2012, n. 179, verso il FSE della regione territorialmente competente per le finalità di prevenzione di cui alla lettera a-bis) del comma 2 dell'art. 12 del decreto legge 18 ottobre 2012, n. 179;
- i) *Piani operativi*: documenti redatti annualmente dalla Sogei S.p.A. che individuano gli obiettivi e le attività da svolgere;
- j) *Piano Operativo Pluriennale*: documento di cui all'**Allegato B** alla presente Convenzione, denominato “Piano Operativo Pluriennale che riporta le attività di massima e gli importi relativi al periodo di vigenza contrattuale;
- k) *Rapporto Periodico*: il rapporto redatto dalla Sogei S.p.A. sullo stato di avanzamento dei *Piani operativi*;

Articolo 2

(*OGGETTO E FINALITÀ*)

1. La presente *Convenzione* disciplina i rapporti giuridici tra il *Dipartimento per la trasformazione Digitale, il Ministero della Salute, l'AGENAS* e la *Società* per la realizzazione e la gestione dell'EDS incluso nel sub-investimento 1.3.1 della Missione 6 Componente 2 - Asse 3 del PNRR, come individuato nel *Piano Operativo Pluriennale* di cui all'**Allegato B** alla presente *Convenzione* e dettagliati nei *Piani operativi* di cui al successivo articolo 9.

Articolo 3

(*REFERENTI DELLE PARTI E COMITATO DI ATTUAZIONE*)

1. Ai fini dell'attuazione della presente *Convenzione* ciascuna delle *Parti* individua un referente per la gestione e per il coordinamento delle attività oggetto della presente *Convenzione*.



2. I referenti designati dalle parti sono:

- per il Dipartimento: il Capo del Dipartimento della trasformazione digitale (o un suo delegato);
 - per il Ministero della Salute: il Segretario Generale (o un suo delegato);
 - per l'AGENAS: il Direttore Generale (o un suo delegato);
 - per la SOGEI: l'amministratore delegato (o un suo delegato).
3. Ciascuna *Parte* si riserva il diritto di sostituire i propri referenti dandone tempestiva comunicazione a mezzo PEC all'altra *Parte*;
4. Le *Parti*, inoltre, costituiscono un *Comitato di attuazione*, composto da nove componenti, di cui tre, tra i quali il Presidente, nominati dal Dipartimento, due dal Ministero della Salute, due da AGENAS e due dalla *Società*;
5. Il *Comitato di Attuazione* viene costituito entro 15 (quindici) giorni dall'approvazione della presente *Convenzione*, tramite scambio di comunicazioni via PEC tra le *Parti* in cui saranno indicati i referenti delle stesse.
6. Il *Comitato di Attuazione* supporta le *Parti* nell'esercizio delle funzioni di coordinamento tecnico operativo delle attività oggetto della presente *Convenzione* e, in particolare:
- esamina e rende un parere sotto il profilo tecnico operativo relativamente al *Piano operativo* annuale e alle sue eventuali varianti;
 - garantisce il costante monitoraggio delle attività, anche al fine di proporre adeguate soluzioni ad eventuali criticità emergenti in corso di attuazione;
 - verifica, attraverso attività di monitoraggio, il grado di raggiungimento degli obiettivi definiti nel *Piano operativo* mediante riunioni di avanzamento da svolgersi indicativamente ogni 20 giorni; l'esito dell'attività deve essere formalizzato in uno specifico resoconto sottoscritto dai referenti e inviato alle parti;
 - mette in atto le azioni necessarie o opportune per rimuovere le criticità che dovessero emergere con particolare riferimento a quelle che hanno un impatto sul rispetto dei tempi;
 - esamina i contenuti dei report prodotti dalla *Società* nel corso dell'attuazione dell'EDS ed evidenzia eventuali scostamenti rispetto alle attività programmate nel *Piano Operativo Pluriennale* e nei *Piani operativi* annuali e ai relativi tempi di attuazione previsti;
 - assicura che non siano effettuate attività in sovrapposizione con altri interventi del PNRR e/o con altre forme di finanziamento;
 - verifica la compatibilità dell'esecuzione della presente *Convenzione*, alla luce di eventuali mutamenti normativi, organizzativi o tecnologici o qualsiasi altra circostanza imprevista che abbia un notevole impatto sull'oggetto della stessa *Convenzione* e propone le occorrenti revisioni e adeguamenti;
 - analizza, valuta e definisce eventuali altri aspetti connessi con l'attuazione della presente *Convenzione*, ivi compreso dirimere controversie e definire questioni sorte tra le strutture tecniche e operative delle *Parti*.
7. Nell'ambito del *Comitato di Attuazione* verranno, infine, monitorate le attività eventualmente contemplate in altri investimenti finanziati dal PNRR e/o da altre fonti finanziarie funzionali al raggiungimento degli obiettivi del sub-investimento in oggetto, al fine di concordare le azioni più opportune per il raggiungimento di milestone e target inerenti all'intervento oggetto della presente *Convenzione*. In particolare, sarà cura dei referenti della *Società* segnalare per tempo ai referenti delle altre parti eventuali ritardi nel completamento di interventi previsti nei *Piani operativi* annuali che possono incidere sul raggiungimento di milestone e target.

Articolo 4



(COMPITI IN CAPO AL MINISTERO DELLA SALUTE)

1. Il *Ministero* della Salute, in quanto Amministrazione titolare del sub-investimento M6C2-1.3.1, si obbliga a:
 - a. vigilare affinché le attività poste in essere dal soggetto attuatore siano coerenti con le indicazioni contenute nel PNRR e assicurare il coordinamento delle attività di gestione; monitorare lo stato di attuazione nonché curare il controllo complessivo dell’investimento e assicurare la rendicontazione al Servizio centrale per il PNRR di cui all’articolo 6 del decreto-legge 31 maggio 2021, n. 77, per l’espletamento degli adempimenti a questi demandati e in particolare, per la presentazione alla Commissione europea delle richieste di pagamento ai sensi dell’articolo 24, paragrafo 2, del medesimo regolamento.
 - b. trasmettere al Servizio centrale per il PNRR i dati finanziari e di realizzazione fisica e procedurale degli investimenti e delle riforme, nonché dell’avanzamento dei relativi milestone e target, attraverso le specifiche funzionalità del sistema informatico di cui all’articolo 1, comma 1043, della legge 30 dicembre 2020, n. 178 (ReGIS);
 - c. vigilare sulla regolarità delle procedure e delle spese da parte del soggetto attuatore e adottare tutte le iniziative necessarie a prevenire, correggere e sanzionare le irregolarità e gli indebiti utilizzi delle risorse, nonché adottare le iniziative necessarie a prevenire le frodi, i conflitti di interesse ed evitare il rischio di doppio finanziamento pubblico degli interventi;
 - d. garantire l’avvio delle procedure di recupero e restituzione delle risorse indebitamente utilizzate da parte del soggetto attuatore, ovvero oggetto di frode o doppio finanziamento pubblico;
 - e. fornire tempestivamente al soggetto attuatore le informazioni necessarie e pertinenti all’esecuzione dei compiti assegnati e a comunicare ogni eventuale variazione del piano d’azione del PNRR;
 - f. garantire il massimo e tempestivo supporto al soggetto attuatore per il raggiungimento degli obiettivi prefissati e per l’adozione di tutti gli atti ritenuti necessari e rientranti nelle materie di propria competenza;
 - g. curare la gestione del flusso finanziario per il tramite del servizio centrale del Ministero dell’economia e delle finanze, impegnandosi a rendere tempestivamente disponibili le risorse finanziarie destinate all’attuazione dell’investimento in funzione della loro fruibilità;
 - h. elaborare le informazioni fornite dal soggetto attuatore ai fini della presentazione alla Commissione europea delle relazioni di attuazione periodiche e finali;
 - i. collaborare alla risoluzione di eventuali problematiche o difficoltà attuative segnalate dall’Amministrazione attuatrice, anche attraverso la partecipazione al Gruppo di Lavoro-FSE.

Articolo 5

(COMPITI IN CAPO AL DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE)

1. Il *Dipartimento* ha il compito di curare il coordinamento tecnico-operativo dei processi necessari all’esecuzione del progetto fino al suo completamento; in particolare:
 - a. assicurare le funzioni di indirizzo e controllo di intesa con il *Ministero e Agenas*, e nel rispetto di quanto previsto dall’art. 12 comma 15-quater del decreto-legge 18 ottobre 2012, n. 179, in ordine fra l’altro:



- a) alla realizzazione per conto del Ministero della Salute del repository centrale, attraverso la Società;
 - b) all’assistenza, per la durata del PNRR, ad AGENAS per la gestione del repository centrale, sempre attraverso la Società;
 - c) alla realizzazione del Gateway, attraverso la Società, che AGENAS metterà poi a disposizione delle strutture sanitarie;
- b. provvedere, d’intesa con il Ministero della Salute, alla gestione dell’iter amministrativo necessario per la definizione dei *Piani operativi* di cui all’art. 9 della presente *Convenzione*;
- c. garantire il costante monitoraggio delle attività stesse e dei relativi costi, nonché la verifica dello stato di avanzamento dei lavori, anche al fine di risolvere con tempestività eventuali criticità emerse e verifica l’esatto adempimento delle attività contrattuali;
- d. approvare i documenti progettuali e i report previsti ed effettuare le verifiche degli output contrattuali provvedendo alla trasmissione dei relativi esiti al *Ministero e ad Agenas*;
2. Inoltre, il *Dipartimento* ha il compito di:
- a. vigilare che le attività realizzate dalla *Società* siano coerenti con le indicazioni contenute nel PNRR;
 - b. curare il coordinamento delle attività di gestione, la rendicontazione e il controllo complessivo del sub-investimento;
 - c. presidiare in modo continuativo l’avanzamento degli interventi e dei relativi milestone e target, vigilando costantemente su ritardi e criticità attuative, ponendo in essere le eventuali azioni correttive e assicurando la regolarità e tempestività dell’esecuzione di tutte le attività previste per l’attuazione dell’intervento nel rispetto dell’Accordo sottoscritto con il Ministero della Salute il 21/09/2021;
 - d. rappresentare, attraverso l’Unità di missione istituita con DPCM 30 luglio 2021, il punto di contatto con il Ministero della Salute e il Servizio centrale per il PNRR di cui all’articolo 6 del decreto-legge 31 maggio 2021, n. 77, per l’espletamento degli adempimenti previsti dal Regolamento (UE) 2021/241 e, in particolare, per la presentazione alla Commissione europea delle richieste di pagamento ai sensi dell’articolo 24, paragrafo 2, del medesimo regolamento;
 - e. verificare che la *Società* svolga una costante e completa attività di rilevazione dei dati di monitoraggio finanziario, fisico e procedurale, relativi agli interventi definiti nei *Piani operativi* annuali afferenti a milestone e target di pertinenza degli interventi finanziati, in base alle indicazioni fornite dal Servizio Centrale PNRR;
 - f. trasmettere al Ministero della Salute ovvero al Servizio Centrale per il PNRR i dati finanziari e di realizzazione fisica e procedurale degli investimenti e delle riforme, nonché dell’avanzamento dei relativi milestone e target, attraverso le specifiche funzionalità del sistema informatico di cui all’ articolo 1, comma 1043, della legge 30 dicembre 2020, n. 178;
 - g. adottare le iniziative di propria competenza necessarie a prevenire le frodi, i conflitti di interesse ed evitare il rischio di doppio finanziamento degli interventi, secondo le disposizioni del Regolamento (UE) 2021/241;
 - h. garantire l’avvio delle procedure di propria competenza per il recupero e restituzione delle risorse indebitamente utilizzate, ovvero oggetto di frode o doppio finanziamento pubblico;
 - i. vigilare, qualora pertinenti, sull’applicazione dei principi trasversali e in particolare sul principio di “non arrecare un danno significativo agli obiettivi ambientali” di cui all’art. 17 del Regolamento (UE) 2020/852 e sul principio del tagging clima e digitale;
 - j. vigilare, qualora pertinenti, sull’applicazione dei principi della parità di genere, della



- protezione e valorizzazione dei giovani e del superamento dei divari territoriali;
- k. vigilare sugli obblighi di informazione e pubblicità di cui all'art. 34 del Regolamento (UE) 2020/2021;
 - l. fornire alla Società le informazioni necessarie e pertinenti all'esecuzione dei compiti assegnati;
 - m. garantire il necessario supporto alla Società per il raggiungimento degli obiettivi prefissati e per l'adozione di tutti gli atti ritenuti necessari e rientranti nelle materie di propria competenza;
 - n. curare l'esecuzione dei pagamenti a favore della Società utilizzando le risorse finanziarie messe a disposizione per il tramite del Servizio Centrale del Ministero dell'economia dal Ministero della salute;
 - o. elaborare le informazioni fornite dalla Società ai fini della presentazione di relazioni di attuazione periodiche e finali.

Articolo 6

(COMPITI IN CAPO ALL'AGENAS)

1. Con la sottoscrizione della presente *Convenzione*, l'AGENAS provvede a:

- a. gestire l'Ecosistema Dati Sanitari di cui all'art. 12 comma 15-quater del decreto-legge n. 179 del 2012 e s.m.i. avvalendosi della Società di cui all'articolo 83, comma 15, del decreto-legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133.
- b. rendere disponibili alle strutture sanitarie e sociosanitarie il Gateway, realizzato dal Dipartimento per la trasformazione digitale avvalendosi della Società;
- c. curare la gestione operativa dei dati raccolti e generati dall'EDS, in qualità di responsabile del trattamento per conto del Ministero della salute, avvalendosi all'uopo della Società.

Articolo 7

(COMPITI IN CAPO ALLA SOCIETÀ)

1. Con la sottoscrizione della presente *Convenzione*, la Società si obbliga a:

- a. garantire la realizzazione operativa dell'intervento secondo quanto riportato nei *Piani operativi*, nel rispetto delle tempistiche ivi indicate, anche in funzione del raggiungimento dei milestone e target riferiti al sub-investimento di cui all'Allegato alla presente *Convenzione*;
- b. garantire la realizzazione, messa a disposizione e gestione dell'infrastruttura tecnologica centrale costituita dal repository e dagli strumenti per la raccolta, l'elaborazione, l'analisi e l'interoperabilità dei dati, conformemente a quanto previsto dall'art. 51 comma 2 lett. f-quinquies del decreto-legge 26 ottobre 2019, n. 124;
- c. erogare i servizi di cui all'articolo 11 secondo le modalità riportate nell'Allegato A alla presente *Convenzione*, nonché provvedere all'acquisizione dei beni e servizi, nel rispetto delle previsioni dei *Piani operativi*;
- d. assicurare i più elevati standard tecnologici di mercato in merito alle policy ed alle metodologie da adottare nell'ambito del processo produttivo, della sicurezza, della *privacy* e della qualità delle informazioni;
- e. favorire la cooperazione informatica ed i servizi di interconnessione con altre Amministrazioni dando impulso all'attuazione delle linee strategiche per la riorganizzazione



e digitalizzazione adottate dal *Dipartimento* coerentemente con quanto previsto nei *Piani operativi*;

- f. individuare eventuali fattori che possano determinare ritardi che incidano in maniera considerevole sulla tempistica attuativa e di spesa, definita nel cronoprogramma, relazionando alle altre parti;
- g. rispettare quanto previsto dall'articolo 11 della legge 16 gennaio 2003, n. 3, in merito alla richiesta dei Codici Unici di Progetto (CUP) e garantirne l'indicazione su tutti gli atti amministrativo-contabili relativi all'attuazione del sub-investimento;
- h. assicurare la completa tracciabilità dei flussi finanziari come previsto dall'art. 3 legge 3 agosto 2016, n. 136 e la tenuta di un'apposita codificazione contabile per l'utilizzo delle risorse del PNRR;
- i. presentare al Dipartimento la rendicontazione delle attività svolte nel rispetto delle tempistiche stabilite nei *Piani operativi* annuali e della spesa, nei tempi e nei modi previsti dal successivo articolo 20, nonché di milestone e target;
- j. adottare misure adeguate volte a rispettare il principio di sana gestione finanziaria secondo quanto disciplinato nel Regolamento finanziario (UE, Euratom) 2018/1046, in particolare in materia di prevenzione dei conflitti di interessi, delle frodi, della corruzione, di recupero e restituzione dei fondi che sono stati indebitamente versati e di evitare il rischio di doppio finanziamento degli interventi, secondo quanto disposto dall'art. 22 del Regolamento (UE) 2021/241;
- k. porre in essere tutte le azioni utili a perseguire gli obiettivi prefissati, dare esecuzione, nei tempi e nei modi ivi previsti, alle attività specificate rispettivamente nell'Allegato A alla presente *Convenzione* ovvero nei *Piani operativi* annuali, per conseguire milestone e target previsti al fine di evitare il disimpegno delle risorse da parte della Commissione;
- l. fornire i dati necessari a garantire l'alimentazione del sistema informatico di registrazione e conservazione di supporto alle attività di gestione, monitoraggio, rendicontazione e controllo delle componenti del PNRR necessari alla sorveglianza, alla valutazione, alla gestione finanziaria, secondo quanto indicato all'art. 20;
- m. garantire, laddove applicabile con riferimento alle attività da realizzare, il rispetto degli obblighi in materia di informazione e pubblicità di cui all'art. 34 del Regolamento (UE) 2021/241, assicurando, in particolare, che tutte le azioni di informazione e pubblicità poste in essere siano coerenti con le condizioni d'uso dei loghi e di altri materiali grafici (logo PNRR e immagine coordinata) e dalla Commissione europea (emblema dell'UE) per accompagnare l'attuazione del PNRR, incluso il riferimento al finanziamento da parte dell'Unione europea e all'iniziativa Next Generation EU utilizzando la frase "finanziato dall'Unione europea – Next Generation EU";
- n. garantire, laddove applicabile con riferimento alle attività da realizzare, l'applicazione dei principi trasversali e in particolare del principio di non arrecare un danno significativo agli obiettivi ambientali (DNSH) di cui all'art. 17 del Regolamento (UE) 2020/852 e del principio del tagging climatico e digitale;
- o. garantire, laddove applicabile con riferimento alle attività da realizzare, l'applicazione dei principi della parità di genere, della protezione e valorizzazione dei giovani e del superamento dei divari territoriali;
- p. conservare tutti gli atti e la relativa documentazione giustificativa su supporti informatici adeguati, secondo quanto previsto al successivo art. 8, comma 4, e renderli disponibili per le attività di controllo e di audit, inclusi quelli a comprova dell'assolvimento del DNSH e, ove pertinente, comprensiva di indicazioni tecniche specifiche per l'applicazione progettuale delle prescrizioni finalizzate al rispetto dei tagging climatici e digitali stimati;



- q. provvedere alla trasmissione di tutta la documentazione afferente all'esecuzione delle attività e al conseguimento degli obiettivi di cui ai *Piani operativi* annuali, ivi inclusa quella di competenza a comprova del conseguimento di milestone e target, e di quella a comprova dell'assolvimento del DNSH (se applicabile) e, ove pertinente in base al sub-investimento, fornire indicazioni tecniche specifiche per l'applicazione progettuale delle prescrizioni finalizzate al rispetto dei tagging climatici e digitali stimati;
- r. fornire su richiesta del *Dipartimento* ogni informazione utile per la predisposizione delle informazioni utili agli adempimenti dell'*Amministrazione titolare* e/o del Ministero dell'Economia e delle Finanze;
- s. garantire e periodicamente aggiornare la definizione e orientamento della progettazione nonché della realizzazione dei servizi digitali erogati secondo quanto definito dal decreto legislativo 7 marzo 2005, n. 82 (CAD) e dalle linee guida adottate ai sensi dell'art. 71 dello stesso decreto.
- t. collaborare all'adempimento di ogni onere o obbligo previsto dalla normativa vigente a carico delle altre *Parti* per tutta la durata della presente *Convenzione*.

Articolo 8

(OBBLIGHI E RESPONSABILITÀ DELLE PARTI)

1. Ciascuna *Parte* si impegna, in esecuzione della presente *Convenzione*, in conformità al *Piano Operativo Pluriennale* e ai *Piani operativi* annuali con le scadenze ivi previste, a contribuire allo svolgimento delle attività di propria competenza con la massima cura e diligenza e a tenere informata le altre parti, sulle attività effettuate.
2. Le *Parti* sono direttamente responsabili della corretta realizzazione delle attività di spettanza e della loro conformità al *Piano Operativo Pluriennale* e ai *Piani operativi* annuali, ciascuna per quanto di propria competenza e in conformità con quanto previsto dalla presente *Convenzione*, nel rispetto della tempistica concordata.
3. Le *Parti* si impegnano al rispetto delle norme in tema di prevenzione della corruzione e delle frodi nonché in materia di trasparenza, secondo i regolamenti e le misure adottate da ciascuna *Parte*.
4. Le *Parti* garantiscono la conservazione e la messa a disposizione degli organismi nazionali ed europei preposti ai controlli della documentazione di cui al Regolamento (UE) 241/2021 nei limiti temporali previsti, fatta salva in ogni caso la normativa nazionale sulle modalità e i tempi di conservazione di atti e documenti della Pubblica Amministrazione.
5. Una volta definiti gli ambiti, le linee e le strategie di intervento e ottenuta l'approvazione degli stessi, anche attraverso l'approvazione dei Piani Operativi, la responsabilità delle scelte tecniche da operare per l'attuazione dei progetti finalizzati allo sviluppo, evoluzione, di soluzioni/piattaforme del Sistema informativo definiti nei *Piani operativi* è demandata alla *Società*, fermo restando che qualora le stesse scelte tecniche abbiano particolare rilevanza strategica, economica e organizzativa per il *Dipartimento*, saranno con questa concordate.
6. Fatto salvo quanto previsto al precedente articolo 7 lett.t, la *Società* non potrà essere ritenuta responsabile per eventuali danni materiali o patrimoniali, diretti o indiretti, qualora la *Società* stessa abbia correttamente adempiuto alle obbligazioni contrattuali ed abbia operato nel rispetto della normativa vigente e in aderenza alle direttive impartite dal *Dipartimento*.



Articolo 9

(PIANIFICAZIONE)

1. Le attività oggetto della presente *Convenzione* inerenti agli obblighi della Società sono condotte nel rispetto delle linee di intervento definite nel *Piano Operativo Pluriennale*, **Allegato B** alla presente *Convenzione*, contenente le attività di massima e gli importi relativi all’intero periodo di validità contrattuale.
2. Nell’ambito del *Piano Operativo Pluriennale* viene predisposta l’apposita tabella riepilogativa contenente la quantificazione del massimale riferito all’intera durata della *Convenzione*.
3. In coerenza con il *Piano Operativo Pluriennale*, per ogni anno di riferimento, verrà redatto dalla Società il *Piano Operativo* annuale di dettaglio, strutturato secondo quanto previsto al paragrafo 2 dell’**Allegato C** alla presente *Convenzione* denominato “Processo di pianificazione, rendicontazione e fatturazione”.
4. Il *Piano Operativo* annuale riporterà le attività da svolgere e le prestazioni da erogare con l’indicazione delle tempistiche e delle relative quantificazioni economiche, e verrà redatto con cadenza annuale e comunque, tranne che per il primo anno, entro il 1° dicembre dell’anno precedente a quello di riferimento e dovrà essere approvato, dal Dipartimento, previo esame del *Comitato di attuazione*, in tempo utile al fine di consentire il perseguitamento degli obiettivi ivi previsti.
5. Il *Piano operativo* annuale del primo anno verrà consegnato entro 30 giorni dalla stipula della presente *Convenzione* e approvato dal Dipartimento previo esame del Comitato di attuazione, in tempo utile al fine di consentire il perseguitamento degli obiettivi ivi previsti.
6. Il *Piano operativo* può essere oggetto di rimodulazione o variazione con l’approvazione del Dipartimento previo esame del Comitato di attuazione per far fronte ad esigenze di ripianificazione emerse in sede di attuazione. Tali variazioni sono adottate in tempo utile per consentire alla Società di adeguare corrispondentemente le prestazioni erogate.
7. Qualora non sia possibile provvedere in tempo utile alla rimodulazione o variazione del *Piano operativo*, in conformità a quanto previsto al precedente comma 6, la Società provvederà all’erogazione dei *Servizi* previa richiesta scritta del Dipartimento concordata con il Ministero e Agenas.
8. Le *Parti* si danno atto che, qualora nelle ipotesi previste ai precedenti commi 5 e 6, si rendesse necessario, nel corso di durata della presente *Convenzione*, provvedere a variazioni degli importi complessivi annuali previsti nei *Piani operativi*, ferma restando la necessaria copertura entro i limiti di massimale, saranno convenute e rese operanti attraverso uno scambio di corrispondenza avente a oggetto una nuova Tabella riepilogativa. Non appena possibile, dovrà comunque procedersi ad aggiornare il corrispondente *Piano Operativo*.
9. Qualora le variazioni e/o i nuovi obiettivi, anche definiti in norma primaria, rendano necessaria la modifica dell’importo massimale di cui al precedente articolo 2, comma 1, le *Parti* provvederanno alla stipula di appositi atti aggiuntivi alla presente *Convenzione*.
10. Resta, altresì, inteso che il Dipartimento può procedere anche all’attuazione parziale della presente *Convenzione*.

Articolo 10

(RAPPORTI PERIODICI E A CHIUSURA)

1. La Società darà conto al Dipartimento delle attività svolte e delle prestazioni erogate in attuazione dei *Piani operativi* mediante appositi *Rapporti Periodici*, redatti secondo lo schema di cui



all’Allegato C:

- a) Rendicontazione contabile di cui al paragrafo 4, ricadente al termine di ciascun bimestre dell’anno, per le informazioni di natura contabile,
 - b) Rendicontazione economico funzionale di cui al paragrafo 3, ricadente almeno al termine di ciascun mese, per quanto riguarda le informazioni di avanzamento economico-funzionale.
2. I Rapporti Periodici di cui al comma 1 lettera a) dovranno essere inviati al *Dipartimento* entro 25 (venticinque) giorni dalla fine del bimestre, con sistema di posta elettronica certificata, all’indirizzo indicato dal *Dipartimento*, fermo restando che il Rapporto Periodico relativo all’ultimo bimestre dell’anno di riferimento verrà inviato entro 45 (quarantacinque) giorni dal termine del bimestre stesso.
 3. I Rapporti periodici cui al comma 1 lettera a) dovranno essere oggetto di approvazione da parte del *Dipartimento*.
 4. Le eventuali osservazioni sui Rapporti Periodici di cui al precedente comma 3 da parte del *Dipartimento* dovranno essere comunicate entro 30 (trenta) giorni dal loro ricevimento. Trascorso inutilmente tale termine, i Rapporti Periodici si intenderanno approvati ad ogni effetto.
 5. Entro il termine previsto per l’invio del Rapporto Periodico, relativo all’ultimo bimestre dell’anno di riferimento, di cui al precedente comma 2, la *Società* provvederà ad inviare anche il consuntivo relativo ai beni e servizi eventualmente acquisiti a rimborso ai fini della realizzazione delle attività previste dal *Piano operativo* annuale, le cui fatture non siano state ancora acquisite nella contabilità della *Società*, sul quale il *Dipartimento* comunicherà le proprie osservazioni entro il 28 febbraio, termine decorso il quale il consuntivo si intenderà approvato.
 6. Resta inteso che, decorsi 60 (sessanta) giorni dalla data di approvazione del Rapporto Periodico relativo all’ultimo bimestre di ciascun anno, la *Società* resterà esonerata dalle penali di cui al successivo articolo 21.
 7. A chiusura della *Convenzione*, la *Società* trasmette il Rapporto finale al *Dipartimento* dopo la scadenza della *Convenzione*, prevista al 31 dicembre 2026, come indicato all’articolo 30. In merito si procede ai sensi dei precedenti commi 3 e 5.
 8. In seguito alla presentazione e approvazione dei Rapporti periodici e finale si procede alla fatturazione secondo l’art.18.

Articolo 11

(SERVIZI EROGATI)

1. Nell’esecuzione della presente *Convenzione* la *Società* effettuerà le attività ed erogherà le prestazioni indicate nei *Piani operativi* annuali.
2. Le modalità di erogazione dei *Servizi* ed i relativi corrispettivi e Livelli di servizio sono definiti nell’**Allegato A** alla presente *Convenzione*.
3. I *Servizi* di cui al precedente comma 1, saranno remunerati sulla base dei corrispettivi congruiti con i pertinenti pareri AGID.
4. I processi e i flussi di comunicazione relativi a Servizi di sviluppo e *professional* fra la *Società* ed il *Dipartimento* sono definiti nell’ambito dell’**Allegato D** denominato “Processo e flusso di comunicazione per i servizi di sviluppo e professionali” alla presente *Convenzione*.

Articolo 12

(AFFIDAMENTI A FORNITORI)



1. Per lo svolgimento delle attività previste, la *Società* può avvalersi di propri fornitori, del cui operato è responsabile in via esclusiva, garantendo, nelle relative procedure di affidamento, l’osservanza delle norme nazionali ed unionale in materia di appalti pubblici e di ogni altra normativa o regolamentazione prescrittiva pertinente.

Articolo 13

(BENI E SERVIZI DA ACQUISIRE)

1. La *Società* provvederà ad acquisire i beni e i servizi, strumentali e individuati nei *Piani operativi*, nel rispetto delle disposizioni di cui in premessa, che prevedono che la *Società*, sulla base di apposita convenzione disciplinante i relativi rapporti nonché i tempi e le modalità di realizzazione delle attività, si avvalga di Consip S.p.A. nella sua qualità di centrale di committenza per le acquisizioni di beni e servizi, per effetto dell’art. 4, comma 3-ter, del predetto D.L. n. 95/2012, e comunque secondo la normativa vigente.
2. Nell’ipotesi in cui la *Società*, in relazione a quanto previsto negli specifici *Piani operativi* annuali, dovesse provvedere ad acquisire beni o servizi a rimborso attraverso la Consip S.p.A., il *Dipartimento* rimborserà i costi eventualmente sostenuti dalla *Società* nei confronti di Consip nell’ambito dei massimali previsti dagli specifici *Piani operativi* in conformità a quanto previsto al successivo comma 4.
3. Per l’acquisizione di beni e di servizi a rimborso:
 - a) la scelta delle procedure da seguire per la selezione dei fornitori di beni e servizi, ivi inclusa la fase dell’affidamento è effettuata sulla base di quanto previsto al precedente comma 1;
 - b) la gestione tecnico-amministrativa dei relativi contratti è operata dalla *Società* sotto la sua esclusiva responsabilità, nel rispetto della normativa comunitaria e nazionale in materia di procedura ad evidenza pubblica per l’acquisto di beni e servizi;
 - c) la *Società* provvederà a stipulare i contratti per l’acquisizione di beni e di servizi prevedendo specifici livelli di servizio e di penali, in conformità alla normativa vigente; gli importi eventualmente derivanti dall’applicazione di penali corrisposti dai fornitori sono riconosciuti, nel rispetto delle vigenti norme fiscali e tributarie, al *Dipartimento* attraverso l’emissione di apposite note di credito;
 - d) la *Società* procederà alla verifica di conformità dei beni acquisiti, le cui risultanze faranno stato tra la *Società* e il *Dipartimento*, fatta salva l’eventuale responsabilità della *Società* in caso di non adeguato o non completo svolgimento delle attività di verifica, provvedendo altresì a dare comunicazione ai fornitori, dell’esito positivo;
4. Il *Dipartimento*, sulla base dei trasferimenti disposti dal Ministero della Salute, rimborserà alla *Società* gli importi da questa effettivamente corrisposti ai fornitori nonché gli eventuali importi corrisposti dalla *Società* a Consip S.p.A. a fronte dello svolgimento della procedura di affidamento.
5. I diritti e le responsabilità in relazione ai beni acquisiti dalla *Società*, di cui al precedente comma 3, si intendono a titolarità del *Ministero* che li affida a far data dalla loro installazione o, ove non prevista, alla data della loro consegna ad Agenas presso i luoghi da questa indicati.
6. Per effetto di quanto sopra, resta inteso che la *Società* è esonerata da ogni responsabilità in ordine alla custodia dei beni di cui al comma 5 successivamente alla predetta data di installazione/consegna, quale risultante dall’apposito documento sottoscritto dal fornitore e da un rappresentante del *Ministero*.



7. In caso di ricorso alle convenzioni quadro definite dalla Consip S.p.A., di cui al precedente comma 1, la ripartizione delle responsabilità tra fornitore dei beni e il Ministero e la gestione e l'esecuzione del relativo contratto verranno regolamentate secondo le modalità e i termini previsti dalle convenzioni stesse.

Articolo 14

(PRESTAZIONI ESTERNE)

1. Per l'esecuzione di quanto previsto nella presente *Convenzione*, la *Società*, per far fronte a specifiche esigenze organizzative, potrà avvalersi, rimanendo pienamente responsabile, di imprese terze, nonché di esperti e professionisti in possesso di adeguata qualificazione ed in grado di garantire la qualità delle prestazioni, selezionati sulla base delle procedure ad evidenza pubblica di cui al decreto legislativo 18 aprile 2016, n. 50 e nel rispetto della normativa vigente.
2. Nell'ipotesi di cui al precedente comma 1, per le voci di cui al precedente articolo 11, remunerate secondo la Metrica Tempo e Spesa, il *Dipartimento* rimborserà alla *Società*, sulla base delle risorse effettivamente impiegate, gli oneri sostenuti nell'ambito degli importi complessivi annuali previsti per le suddette voci.

Articolo 15

(BREVETTI E DIRITTI D'AUTORE)

1. Resta esclusa qualsiasi responsabilità del *Dipartimento* nel caso la *Società* usi, per l'esecuzione della presente *Convenzione*, dispositivi e soluzioni di cui altri siano titolari di diritti di privativa.
2. La *Società*, conseguentemente, manleverà e terrà indenne il *Dipartimento* da ogni pretesa e dagli oneri relativi ad azioni per violazione dei diritti di autore o di qualsiasi marchio italiano o straniero.

Articolo 16

(PROPRIETÀ DEI RISULTATI E DIRITTI DI UTILIZZAZIONE)

1. Le applicazioni software di cui al precedente articolo 13 – fatti salvi i diritti spettanti ai titolari delle licenze dei prodotti software utilizzati per lo sviluppo ed evoluzione di soluzioni basate su parametrizzazioni e personalizzazioni di pacchetti software di mercato – e gli eventuali prodotti realizzati nell'ambito di Prodotti/Servizi specifici, identificati e definiti nei *Piani operativi*, diverranno di proprietà del *Ministero*.
2. La *Società* si impegna, alla scadenza della presente *Convenzione* o su richiesta del *Dipartimento*, a trasferire al *Dipartimento e/o al Ministero* tutta la documentazione ed il materiale necessario all'effettivo sfruttamento di detti diritti di proprietà.
3. Resta, peraltro, inteso che, in relazione a specifiche esigenze, il *Ministero* potrà autorizzare la *Società* a commercializzare le applicazioni software ed i prodotti di cui al precedente comma 1. In tale ipotesi la *Società* riconoscerà al *Ministero* le “*royalty*” il cui ammontare sarà di volta in volta determinato secondo criteri che verranno definiti di comune accordo.

Articolo 17

(IMPORTO DELLA CONVENZIONE)

1. Per la realizzazione dell'intervento oggetto della presente *Convenzione*, il *Dipartimento* riconosce alla *Società* l'importo massimo di € **103.537.897,42** (centotremilionicinquecentotrentasettemilaottocentonovantasette/42) oltre l'IVA, complessivamente pari a € **126.316.234,85**



(centoventiseimilionitrecentosedicimiladuecentotrentaquattro/85) comprensivi di IVA, a valere sulle risorse per l’attuazione del sub-investimento 1.3.1 della Missione 6 – Componente 2 - Asse 3 del PNRR.

Articolo 18

(FATTURAZIONE)

1. Atteso che la *Società* è una società per azioni a totale capitale pubblico, al fine di evitare l’insorgere di oneri finanziari che andrebbero comunque a gravare sul bilancio dello Stato, il *Dipartimento* trasferirà alla *Società* una quota a titolo di anticipo, non superiore al 10% dell’importo complessivo annuale previsto dai *Piani operativi* ripartito linearmente nei mesi, su richiesta della *Società* da inoltrare dopo l’approvazione del *Piano operativo annuale*.
2. Successivamente all’approvazione dei *Rapporti Periodici*, di cui all’articolo 10, comma 3 e comma 7, in conformità agli stessi ed in unica soluzione, verrà effettuato il conguaglio tra quanto corrisposto dal *Dipartimento* ai sensi del precedente comma 1 e quanto risultante dai predetti *Rapporti Periodici* e a chiusura delle attività.
3. Qualora il *Dipartimento* richieda la sospensione o l’annullamento di un’attività di sviluppo software, la *Società* procederà alla fatturazione di un importo determinato in base al corrispettivo e alla percentuale di stato avanzamento lavori nota alla data.
4. Resta inteso che la documentazione di riferimento e le fatture delle risorse esterne e dei servizi acquisiti e dei beni installati saranno detenute presso la sede della *Società* e tenute a disposizione del *Dipartimento* per l’effettuazione di eventuali ulteriori controlli per tutto il periodo previsto dalla normativa vigente.
5. Le fatture devono essere emesse previa approvazione da parte del *Dipartimento*, dei Rapporti presentati dalla *Società* (periodici e finale), come previsto dal precedente art.8 comma 8.

Articolo 19

(PAGAMENTI)

1. Il *Dipartimento* provvederà al pagamento delle fatture di cui alla precedente art. 18, da effettuarsi sul conto corrente appositamente indicato dalla *Società* nelle fatture stesse, entro 30 (trenta) giorni dalla data di ricezione della singola fattura.
2. In caso di ritardato pagamento, la *Società* potrà richiedere il pagamento degli interessi in conformità a quanto previsto dalla normativa vigente.

Articolo 20

(MONITORAGGIO)

1. Il *Dipartimento* deve registrare i dati di avanzamento finanziario nel sistema informativo ReGiS messo a disposizione dal Ministero dell’Economia e delle Finanze - o su altra piattaforma informatica per la quale sia garantita la piena interoperabilità con il sistema ReGiS - caricando la documentazione attestante il conseguimento dei milestone e target ed ogni altro documento richiesto a tal fine e conservando la documentazione specifica relativa a ciascuna procedura di affidamento e a ciascun atto giustificativo di spesa e di pagamento, al fine di consentire l’espletamento delle verifiche indicate dal Ministero dell’economia e delle finanze.



2. La *Società*, pertanto, secondo le indicazioni fornite dal *Dipartimento*, deve fornire i dati necessari all'alimentazione del sistema informativo ReGiS messo a disposizione dal Ministero dell'Economia e delle Finanze - o su altra piattaforma informatica per la quale sia garantita la piena interoperabilità con il sistema ReGiS – compresa la documentazione attestante il conseguimento degli obiettivi del Progetto indicati nel *Piano Operativo Pluriennale* e la documentazione di competenza attestante milestone e target, eventualmente previsti nei *Piani operativi* annuali.

Articolo 21

(LIVELLI DI SERVIZIO)

1. I Livelli di servizio che la *Società* dovrà assicurare nell'erogazione dei Servizi e le eventuali penali dovute sono riportati nell'**Allegato A** alla presente *Convenzione*, fatto salvo quanto ulteriormente previsto nei *Piani operativi* relativamente ai Prodotti/servizi specifici.
2. Ai fini del controllo dei Livelli di servizio e della conseguente applicazione delle penali, ogni quadrimestre si procederà come segue:
 - a) la *Società* comunicherà i livelli di servizio effettivamente conseguiti e gli eventuali scostamenti verificatisi;
 - a) la *Società* manterrà a disposizione del *Dipartimento*, per 60 (sessanta) giorni dalla data di approvazione dell'ultimo Rapporto Periodico di cui al precedente articolo 10, comma 6, le registrazioni e/o le rilevazioni analitiche;
 - b) la *Società*, per l'effettuazione dei controlli, dovrà rendere disponibili le registrazioni e/o le rilevazioni analitiche effettuate, secondo le modalità di accesso e di sicurezza fisica e logica vigenti presso la *Società*.
3. Tutte le penali previste dalla presente *Convenzione* potranno essere applicate previa contestazione dell'addebito fatta a mezzo PEC e previa valutazione da parte del *Dipartimento* delle deduzioni al riguardo addotte dalla *Società*, che dovranno essere presentate non oltre il termine di 30 (trenta) giorni dal ricevimento della comunicazione contenente la contestazione stessa.
4. Il *Dipartimento*, valutate le predette deduzioni, potrà decidere di dare corso all'applicazione delle penali dandone comunicazione scritta alla *Società* non oltre il termine di 30 (trenta) giorni dal ricevimento delle deduzioni.
5. Le Parti si danno atto che, in caso di violazione dei Livelli di servizio che riguardino obiettivi per i quali siano previsti valori di soglia incrementali, verrà applicata esclusivamente la penale che si riferisce al valore più alto riscontrato.
6. La *Società* provvederà a riconoscere al *Dipartimento* quanto indicato nella comunicazione di cui al precedente comma 4. Le Parti si danno peraltro atto che, qualora la *Società* ritenga di non condividere le conclusioni del *Dipartimento*, il pagamento di cui sopra non potrà costituire in nessun caso riconoscimento di responsabilità e/o di debito ove la *Società* dia inizio alla procedura di cui al successivo articolo 27 entro 60 (sessanta) giorni dal pagamento stesso.
7. Resta inteso che, nel caso in cui gli inadempimenti siano determinati da astensione dal lavoro del personale della *Società*, che si configuri come causa di forza maggiore, nessuna pretesa risarcitoria potrà essere avanzata dal *Dipartimento* nei confronti della *Società* stessa.
8. La responsabilità della *Società* per qualsiasi pretesa del *Dipartimento*, in qualunque modo relativa alla presente *Convenzione*, non potrà in ogni caso – incluso ove la violazione abbia comportato l'applicazione di penali ai danni della *Società* e/o lo scioglimento a qualsiasi titolo della presente *Convenzione* - eccedere (per tutti i danni) gli importi previsti dalla contrattualistica pubblica.



Articolo 22

(*RISOLUZIONE E RIDUZIONE DELL'IMPORTO DELLA CONVENZIONE*)

1. Il *Dipartimento* si riserva facoltà di risolvere, anche in parte, in qualsiasi momento la presente *Convenzione*, in caso di grave ed importante inadempimento ai sensi dell'art. 1453 e seguenti del Codice Civile e nelle ipotesi di cui al successivo comma 3.
2. Nel caso di risoluzione, la *Società* ha diritto al pagamento delle prestazioni regolarmente eseguite alla data di risoluzione della presente *Convenzione*. Sono fatti salvi i diritti risarcitorii delle parti nei confronti della *Società*.
3. L'eventuale riduzione del sostegno da parte della Commissione europea, correlato al mancato raggiungimento di milestone e target dell'intervento oggetto della presente *Convenzione*, ovvero alla mancata tutela degli interessi finanziari dell'Unione europea come indicato nell'art. 22 del Reg. (UE) 2021/241, ovvero al mancato rispetto del principio DNSH o, ove pertinenti per l'investimento, del rispetto delle prescrizioni finalizzate al rispetto dei tagging climatici e digitali stimati, può comportare la conseguente riduzione proporzionale delle risorse di cui all'articolo 17 comma 1, fino all'eventuale risoluzione della presente *Convenzione*, come stabilito dall'articolo 8, comma 5 del decreto-legge 31 maggio 2021, n.77.
4. Qualora il mancato raggiungimento di milestone e target associati al sub-investimento oggetto della presente *Convenzione* non sia imputabile alle attività/responsabilità attribuite alla *Società*, come riportate specificamente nei *Piani operativi*, verrà comunque assicurato il pagamento delle attività utilmente svolte da quest'ultima.
5. Al fine di evitare quanto previsto al comma precedente, nonché l'esercizio dei poteri sostitutivi di cui al successivo articolo 28, nel caso in cui sopravvengano problematiche tali da incidere anche solo potenzialmente sulla corretta e puntuale attuazione degli interventi oggetto della presente *Convenzione*, in ossequio al principio di leale collaborazione, di imparzialità e buon andamento dell'Amministrazione, la *Società* si impegna a comunicare tempestivamente al *Dipartimento* tali problematiche.
6. Qualora dalle verifiche del *Dipartimento*, anche nell'ambito del Comitato di attuazione di cui all'articolo 3, risulti che la *Società* è in ritardo sulle tempistiche previste nel Piano Operativo, il *Dipartimento* comunica il ritardo alla *Società* che, entro 10 (dieci) giorni espone le ragioni del ritardo e individua le possibili soluzioni al fine di recuperare il ritardo accumulato. Le parti si impegnano a concordare un Piano di rientro, tale da consentire il rispetto dei termini previsti e a monitorare periodicamente lo stato di avanzamento di tale piano.
7. Nel caso di reiterati ritardi rispetto ai termini fissati dal Piano Operativo allegato e/o di mancato rispetto dei Piani di rientro di cui al comma 3 del presente articolo, il *Dipartimento* potrà agire secondo quanto previsto nel precedente comma 1. Allo stesso modo il *Dipartimento* potrà agire ai sensi del comma 3 nel caso di superamento del tetto massimo delle penali.
8. Il *Dipartimento* adotta tutte le iniziative volte ad assicurare il raggiungimento di target e milestone stabiliti nel PNRR: laddove comunque essi non vengano raggiunti per cause non imputabili alla *Società*, la copertura finanziaria degli importi percepiti o da percepire per l'attività realizzata e rendicontata è stabilita dal *Dipartimento* in accordo con il Servizio Centrale per il PNRR sulla base delle disposizioni vigenti in materia di gestione finanziaria delle risorse previste nell'ambito del PNRR.

Articolo 23

(*ONERI E SPESE CONTRATTUALI*)



1. Sono a carico della *Società* le spese relative alla stipula della presente *Convenzione*, ad eccezione di quelle che, per legge, fanno carico alle altre parti.
2. A tal fine la *Società* dichiara che le prestazioni contrattuali sono effettuate nell'esercizio d'impresa e che trattasi di operazioni imponibili non esenti dall'imposta sul valore aggiunto che la *Società* è tenuta a versare, con diritto di rivalsa. Conseguentemente, alla presente *Convenzione* dovrà essere applicata l'imposta di registro in misura fissa, ai sensi dell'articolo 40 del decreto del Presidente della Repubblica 26 aprile 1986, n. 131, e successive modificazioni e integrazioni.

Articolo 24

(VALORE DEGLI ALLEGATI)

Alla presente *Convenzione* vengono allegati i seguenti documenti:

- Allegato A “Descrizione dei Servizi, Livelli di servizio e Corrispettivi”;
- Allegato B “Piano operativo pluriennale e impegno economico”;
- Allegato C “Processo di pianificazione, rendicontazione e fatturazione”;
- Allegato D “Processo e flusso di comunicazione per i servizi di sviluppo e professional”;
- Allegato E “Attribuzione del ruolo e degli obblighi di cui all’art. 28 del Regolamento UE 2016/679” da parte del Ministero alla *Società* per la realizzazione dell’EDS;
- Allegato F “Attribuzione del ruolo e degli obblighi di cui all’art. 28 del Regolamento UE 2016/679” da parte del Ministero ad Agenas per la gestione dell’EDS;
- Allegato G “Attribuzione del ruolo e degli obblighi di cui all’art. 28 del Regolamento UE 2016/679 da parte di Agenas alla *Società* in qualità di sub responsabile per la gestione dell’EDS.

Articolo 25

(SICUREZZA DEL SISTEMA)

1. Fermo restando quanto previsto dall’art. 12 comma 15-quater del decreto-legge n.179 del 2012, attesa la specificità dei dati oggetto di trattamento e la loro rilevanza per il Paese, la *Società* è tenuta ad assicurare i livelli di sicurezza previsti dalle disposizioni di legge e normative nazionali e unionali, con particolare riguardo all’implementazione di strumenti per monitorare la regolarità e la sicurezza degli accessi all’infrastruttura
2. La *Società* in materia di sicurezza cibernetica opera con il proprio CERT.
3. A tale scopo la *Società* dovrà operare attraverso l’adozione di idonee misure organizzative, tecniche ed operative, per la protezione dei dati e delle informazioni gestite, delle apparecchiature e dei sistemi di elaborazione utilizzati, nonché delle reti di comunicazione.
4. La protezione di cui sopra dovrà essere assicurata riguardo sia alle apparecchiature e alle reti interne alla *Società*, utilizzate per l’espletamento del suo incarico, sia alla trasmissione di dati attraverso reti esterne.
5. La *Società* si obbliga espressamente a manlevare e tenere indenne il *Dipartimento* da tutte le conseguenze derivanti dall’eventuale inosservanza delle norme e prescrizioni tecniche vigenti in materia di sicurezza.



Articolo 26

(RISERVATEZZA E PROTEZIONE DEI DATI PERSONALI)

1. Le *Parti* hanno l'obbligo di mantenere riservati i dati, le informazioni di natura tecnica, economica, commerciale e amministrativa e i documenti di cui vengano a conoscenza o in possesso in esecuzione della presente *Convenzione* o, comunque, in relazione a esso, in conformità alle disposizioni di legge applicabili, di non divulgare in alcun modo e in qualsiasi forma e di non farne oggetto di utilizzazione a qualsiasi titolo per scopi diversi da quelli strettamente necessari all'esecuzione della *Convenzione*, per la durata della *Convenzione* stessa.
2. Le *Parti* si obbligano a far osservare ai propri dipendenti, incaricati e collaboratori la massima riservatezza su fatti e circostanze di cui gli stessi vengano a conoscenza, direttamente e/o indirettamente, per ragioni del loro ufficio, durante l'esecuzione della presente *Convenzione*. Gli obblighi di riservatezza di cui al presente articolo rimarranno operanti fino a quando gli elementi soggetti al vincolo di riservatezza non divengono di pubblico dominio.
3. Con la sottoscrizione della presente *Convenzione*, i legali rappresentanti pro-tempore delle *Parti* acconsentono espressamente al trattamento dei propri dati personali.
4. Le *Parti* si impegnano a concordare le eventuali modalità di pubblicizzazione o comunicazione esterna, anche a titolo individuale, della presente *Convenzione*.
5. La *Società* prende atto ed acconsente che in adempimento agli obblighi di legge che impongono la trasparenza amministrativa i dati e/o la documentazione che la legge impone di pubblicare siano pubblicati e diffusi tramite il sito internet del *Dipartimento*, nella sezione relativa alla trasparenza.
6. Nel corso dell'esecuzione delle attività oggetto della presente *Convenzione*, ciascuna delle Parti potrà trovarsi nella condizione di dover trattare dati personali riferibili a dipendenti e/o collaboratori dell'altra Parte, motivo per cui le stesse si impegnano sin d'ora a procedere al trattamento di tali dati personali in conformità alle disposizioni di cui al Regolamento Europeo (UE) 679/2016 in materia di protezione dei dati personali (GDPR) nonché di tutte le norme di legge di volta in volta applicabili.
7. Le *Parti* si impegnano a condurre le suddette attività di trattamento sulla base dei principi di correttezza, liceità, trasparenza e tutela della riservatezza dei soggetti interessati e per il solo ed esclusivo fine di perseguire le finalità di cui alla presente *Convenzione*, nonché degli eventuali obblighi di legge alla stessa connessi. Tali dati saranno trattati dalle Parti con sistemi cartacei e/o automatizzati - ad opera di propri dipendenti e/o collaboratori che, in ragione della propria funzione e/o attività, hanno la necessità di trattarli, per le sole finalità suindicate e limitatamente al periodo di tempo necessario al loro conseguimento.
8. Qualora, nell'ambito dello svolgimento delle attività di cui alla presente *Convenzione*, una delle *Parti* si trovi nella condizione di affidare all'altra, attività di trattamento di dati personali di propria titolarità o di cui è stata nominata responsabile del trattamento da parte del relativo Titolare, quest'ultima si impegna fin da ora al pieno rispetto di tutte le istruzioni che saranno impartite dalla prima e a sottoscrivere una separata *Convenzione* volta a formalizzare la nomina a responsabile o a sub-responsabile del trattamento, al fine di procedere a una corretta gestione delle attività di trattamento di dati personali, nel rispetto delle disposizioni di cui all'art. 28 GDPR.
9. Con la presente convenzione ed in particolare attraverso l'Allegato "E" denominato "Atto di attribuzione del ruolo di responsabile ai sensi dell'art 28 del regolamento UE 2016/679 per la realizzazione dell'ecosistema dati sanitari", il Ministero, in qualità di titolare del trattamento dei



dati, nomina SOGEI nel ruolo di Responsabile degli obblighi di cui all'art. 28 del Regolamento UE 2016/679; attraverso l'Allegato "F" denominato "Attribuzione del ruolo e degli obblighi di cui all'art. 28 del Regolamento UE 2016/679", il Ministero, in qualità di titolare del trattamento dei dati, nomina AGENAS nel ruolo di Responsabile degli obblighi di cui all'art. 28 del Regolamento UE 2016/679 per la gestione dell'ecosistema dati sanitari.

10. AGENAS accetta la nomina di cui al precedente comma e si obbliga, nel trattamento dei dati personali, ad attenersi alle disposizioni del regolamento (UE) 2016/679 relative al registro dei trattamenti del responsabile esterno nonché alla procedura di notifica di violazioni di dati personali (*data breach management*) di cui agli articoli 30 e 33 del citato Regolamento, contenuti nel medesimo Allegato alla presente *Convenzione*.
11. AGENAS con la presente convenzione ed in particolare attraverso l'Allegato G, denominato "Attribuzione del ruolo e degli obblighi di cui all'art. 28 del Regolamento UE 2016/679" nomina la *Società Sub-Responsabile* del trattamento dati *ex articolo 28* del Regolamento Europeo n. 2016/679.
12. La *Società* accetta la nomina di cui al precedente comma e si obbliga, nel trattamento dei dati personali, ad attenersi alle disposizioni del regolamento (UE) 2016/679 relative al registro dei trattamenti del responsabile esterno nonché alla procedura di notifica di violazioni di dati personali (*data breach management*) di cui agli articoli 30 e 33 del citato Regolamento, contenuti nel medesimo Allegato alla presente *Convenzione*.

Articolo 27

(CONTROVERSIE E FORO COMPETENTE)

1. Nel caso di controversie di qualsiasi natura che dovessero insorgere tra le Parti in ordine alla interpretazione o all'esecuzione della presente *Convenzione*, o comunque direttamente od indirettamente connesse alla *Convenzione* stessa, ciascuna Parte comunicherà per iscritto all'altra l'oggetto ed i motivi della contestazione.
2. Al fine di comporre amichevolmente la controversia le Parti si impegnano ad esaminare congiuntamente la questione, entro il termine massimo di 5 (cinque) giorni dalla data di ricezione della contestazione, ed a pervenire ad una composizione entro il successivo termine di 5 (cinque) giorni.
3. In caso di esito negativo del tentativo di composizione di cui al precedente comma 2, la questione verrà rimessa al Foro competente.
4. Il Foro competente è esclusivamente quello di Roma.
5. Resta, peraltro, inteso che le controversie in atto non pregiudicheranno in alcun modo la regolare esecuzione delle attività della presente *Convenzione*, né consentiranno alcuna sospensione delle prestazioni dovute dall'una e dall'altra Parte, fermo restando che riguardo alle questioni oggetto di controversia, le Parti si impegnano a concordare di volta in volta, in via provvisoria, le modalità di parziale esecuzione che meglio garantiscano il pubblico interesse ed il buon andamento dell'attività amministrativa.



Articolo 28

(*POTERI SOSTITUTIVI*)

1. La presente Convenzione rientra nell’ambito di applicazione dei poteri sostitutivi previsti all’art. 12, comma 3 del decreto-legge 31 maggio 2021, n. 77, finalizzati all’attuazione del PNRR.

Articolo 29

(*MODIFICHE*)

1. La presente *Convenzione* può essere modificata o integrata, nel periodo di validità, mediante atto aggiuntivo sottoscritto dalle *Parti* e sottoposto, al ricorrere dei presupposti di legge, ai competenti Organi di controllo, in relazione a nuove e sopravvenute esigenze connesse alla realizzazione del suo oggetto.

Articolo 30

(*DURATA ED EFFICACIA*)

1. La presente *Convenzione* ha durata sino al 31/12/2026.
2. Eventuali proroghe potranno essere concordate per iscritto tra le *Parti*, sulla base di apposita richiesta sorretta da comprovati motivi e pervenuta almeno 6 (sei) mesi prima della scadenza della *Convenzione*, nel rispetto della normativa vigente nazionale ed eurounitaria di riferimento.
3. In caso di mancato rinnovo, le *Parti* concordano con apposito atto tutti gli adempimenti e le operazioni necessarie a garantire la prosecuzione delle attività previste dalla presente *Convenzione*, senza soluzione di continuità, ivi incluso il trasferimento del know-how e delle competenze al *Ministero* e/o a terze parti da quest’ultimo individuate.
4. I corrispettivi saranno rideterminati, d’accordo tra le parti, in conformità alle eventuali variazioni dei corrispettivi unitari derivanti da successivi pareri rilasciati da AGID ai sensi dell’Articolo 14 bis, comma 2, lettera f) del CAD per la definizione di altre convenzioni fra Sogei S.p.A. e il *Dipartimento*.

Articolo 31

(*DISPOSIZIONI FINALI*)

1. Per quanto non espressamente previsto o disciplinato all’interno della presente *Convenzione*, trovano applicazione le disposizioni normative vigenti.
2. La presente *Convenzione* dovrà essere registrata presso i competenti organi di controllo, al ricorrere dei presupposti di legge e acquisiterà efficacia dalla data di registrazione.
3. La presente *Convenzione* si compone di n. 31 articoli e di n. 6 allegati, sottoscritti digitalmente dalle parti.



Letto, approvato e sottoscritto digitalmente dalle *Parti*.

PCM - Dipartimento per la Trasformazione Digitale

Il Capo Dipartimento

Ing. Mauro Minenna



MINENNA MAURO
PRESIDENZA
CONSIGLIO DEI
MINISTRI
20.06.2022 07:42:52
GMT+01:00

Ministero della Salute

Il Segretario Generale

Dott. NARDI GIOVANNI Leonardi



2022.06.21 21:51:40

CN=LEONARDI GIOVANNI
C=IT
2.5.4.4=LEONARDI
2.5.4.42=GIOVANNI

RSA/2048 bits

AGENAS – Agenzia Nazionale per i Servizi Sanitari Regionali

Il Presidente

Prof. Enrico Coscioni

SOGEI – Società Generale d'Informatica S.p.A.

Amministratore Delegato

Dott. Andrea Quaciv



ANDREA QUACIVI
SOGEI S.P.A.
AMMINISTRATORE
DELEGATO
24.06.2022 07:30:09
UTC



CONVENZIONE PER L'AFFIDAMENTO DELLE
ATTIVITÀ DI REALIZZAZIONE E GESTIONE
DELL'ECOSISTEMA DATI SANITARI (EDS) PREVISTO
DALL'INVESTIMENTO M6C2 - 1.3.1 DEL PNRR -
FASCICOLO SANITARIO ELETTRONICO – EX ART. 12
COMMA 15-QUATER DEL DECRETO-LEGGE N. 179 DEL
2012

ALLEGATO A

DESCRIZIONE DEI SERVIZI, LIVELLI DI SERVIZIO E
CORRISPETTIVI

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 2 di 95

INDICE

1.	PREMESSA	5
	SERVIZI PROFESSIONAL E ACCESSORI	9
2.	SERVIZI PROFESSIONAL	10
2.1	SUPPORTO	11
2.2	GOVERNANCE	12
2.3	LIVELLI DI SERVIZIO.....	13
3.	SERVIZI ACCESSORI	14
	SERVIZI DI SVILUPPO.....	16
4.	PROGETTAZIONE E SVILUPPO SERVIZI ICT	17
4.1	SVILUPPO E MANUTENZIONE EVOLUTIVA DEL SOFTWARE AD HOC	
	17	
4.1.1	Livelli di Servizio	21
4.2	PERSONALIZZAZIONE DEL SOFTWARE DI MERCATO	23
4.2.1	Livelli di Servizio	25
	SERVIZI DI BASE DI CONDUZIONE	27
5.	SERVIZI DI BASE DI GESTIONE, CONDUZIONE E	
	MANUTENZIONE	28
5.1	GESTIONE E CONDUZIONE SERVIZI ICT	28
5.1.1	Manutenzione servizi ICT	28
5.1.1.1	<i>Livelli di Servizio</i>	29
5.1.2	Servizio di customer care	30
5.1.2.1	<i>Customer Management</i>	31
5.1.2.2	<i>Servizio di collaborazione specialistica.....</i>	36
5.1.2.3	<i>Erogazione del servizio con operatore in lingua</i>	37

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 3 di 95

<i>5.1.2.4 Esercizio del servizio in modalità automatica tramite IVR</i>	37
<i>5.1.2.5 Erogazione del servizio in modalità automatica tramite chatbot.</i>	38
<i>5.1.2.6 Canali aggiuntivi per l'accesso al Customer Care</i>	39
<i>5.1.2.7 Gestione campagne di outbound</i>	41
<i>5.1.2.8 Knowledge Base</i>	41
<i>5.1.2.9 Supporto per assistenza specifica.....</i>	43
<i>5.1.2.10 Dashboard.....</i>	44
5.2 GESTIONE E CONDUZIONE INFRASTRUTTURA	44
<i>5.2.1 Server</i>	45
<i>5.2.1.1 Livelli di Servizio.....</i>	49
<i>5.2.2 Storage</i>	50
<i>5.2.2.1 Livelli di Servizio.....</i>	51
<i>5.2.3 Appliance</i>	53
<i>5.2.3.1 Livelli di Servizio.....</i>	56
<i>5.2.4 Piattaforma Big Data</i>	57
<i>5.2.4.1 Livelli di Servizio.....</i>	59
<i>5.2.5 Piattaforma NOSQL</i>	59
<i>5.2.5.1 Livelli di Servizio.....</i>	61
5.3 SERVIZI DI COLLABORATION E COMMUNICATION	62
<i>5.3.1 Servizi navigation Internet.....</i>	62
<i>5.3.1.1 Livelli di Servizio.....</i>	63
<i>5.3.2 Virtual Private Network utente</i>	63
<i>5.3.2.1 Livelli di Servizio.....</i>	64
<i>5.3.3 Servizi di Digital WorkSpace</i>	64
<i>5.3.3.1 Livelli di Servizio.....</i>	68
5.4 SERVIZI DI TIPOLOGIA CLOUD	68
<i>5.4.1 Piattaforma IaaS.....</i>	68
<i>5.4.1.1 Livelli di Servizio.....</i>	75

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 4 di 95

SERVIZI DI BASE DIVERSI DA QUELLI DI CONDUZIONE ..76**6. PIATTAFORME ASP77****6.1 SERVIZI DI SICUREZZA.....77****6.1.1 Piattaforme di sicurezza IAM (Identity Access Management).....77****6.1.1.1 *Livelli di Servizio*78****6.1.2 Piattaforme di sicurezza SOC (Security Operation Center) 78****6.1.2.1 *Livelli di Servizio*81****7. SERVIZIO SITO/PORTALE WEB E COMPONENTI ACCESSORI.....81****7.1 LIVELLI DI SERVIZIO85****ASPETTI GESTIONALI87****8. CORRISPETTIVI.....88**

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 5 di 95

1. PREMESSA

Nel presente allegato, parte integrante e sostanziale alla presente Convenzione stipulata tra Sogei e la Presidenza del Consiglio dei Ministri, Dipartimento per la trasformazione digitale, il Ministero della Salute e l’Agenzia Nazionale per i Servizi Sanitari Regionali, vengono definiti i Servizi erogati, i relativi corrispettivi ed i Livelli di servizio da garantire.

Il rapporto contrattuale prevede da parte di Sogei l’erogazione di servizi corredati di facility che ne consentano la piena fruibilità in termini di sicurezza, monitoraggio e integrazione. In tale contesto Sogei si pone come responsabile di tutti gli aspetti applicativi, tecnologici, architetturali, di qualità e di sicurezza dell’intero Sistema Informativo, operando le scelte più opportune in base alle esigenze dell’Amministrazione. L’Amministrazione si configura come fruitore dei servizi di cui ha fatto richiesta monitorando la loro erogazione.

Per Servizio ICT si intende “*l’insieme di applicazioni informatiche omogenee e della relativa infrastruttura tecnologica, in grado di supportare lo svolgimento di un processo/sottoprocesso amministrativo e per le quali sia comunque opportuno esercitare il controllo/monitoraggio a livello di unica entità. Nei casi previsti dalla normativa (GDPR) può essere collegato ad uno o più “trattamento” dei dati*”

Per gli indicatori relativi ai Servizi vengono realizzati sistemi di rilevazione specifici normalmente disponibili dal secondo quadrimestre di erogazione del servizio stesso; a riguardo si specifica che:

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 6 di 95

- la rilevazione è per tutti su base quadrimestrale a meno che diversamente specificato;
- la rilevazione di alcuni LDS potrebbe richiedere un periodo di osservazione e/o di sviluppo della modalità di rilevazione stessa;
- nei casi in cui si verifichi un fermo di Servizio concordato con l'Amministrazione, la fascia temporale corrispondente verrà esclusa ai fini del calcolo dei Livelli di servizio stessi.

Termini/Definizioni dei Livelli di servizio

Si riportano nel seguito i termini e le definizioni di riferimento utilizzati nelle descrizioni dei Livelli di servizio relativi ai prodotti/servizi forniti.

- Arrotondamenti
 - ai fini del calcolo dello scostamento tra le percentuali effettive e quelle contrattuali le prime devono essere arrotondate:
 - nel caso di aumenti o riduzione dello 0,1%, si arrotonda allo 0% per scostamenti compresi tra lo 0,000% e lo 0,049% ed allo 0,1% per scostamenti superiori;
 - nel caso di aumenti o riduzioni dell'1%, si arrotonda allo 0% per scostamenti compresi tra lo 0,00% e lo 0,49% ed all'1% per scostamenti superiori.
 - ai fini del calcolo delle ore di ritardo, le frazioni sono così arrotondate:
 - da 1 a 29 minuti: zero ore;

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 7 di 95

- da 30 a 59 minuti: 1 ora.
- Errore software - si considera un errore software ogni intervento correttivo sul software innescato da uno o più problemi. Verranno considerati tutti i problemi segnalati, sullo strumento utilizzato per tracciatura del servizio di assistenza alla data di completa distribuzione della versione corretta del software. Resta inteso che più segnalazioni relative allo stesso problema software vengono considerate una sola volta ai fini del conteggio nel livello di servizio.
La modalità di rilevazione degli errori sarà definita dalla “Procedura di rilevazione dell’errore” che sarà fornita all’Amministrazione.
- Finestra Temporale di erogazione del servizio - arco di tempo in cui il servizio deve essere erogato; i livelli di servizio sono calcolati sugli orari di erogazione dei servizi oggetto del presente documento, salvo diversa esplicita indicazione.
- Giorni - giorni lavorativi, salvo ove espressamente indicato.
- Ore - ore lavorative ovvero ore ricadenti nella finestra temporale di erogazione, salvo diversa esplicita indicazione (festivi esclusi a meno del riferimento ad H24).
- Periodo di osservazione contrattuale - arco di tempo a cui è relativa la misurazione dei livelli di servizio.
Viene fissata su base quadriennale.

In caso di violazione di Livelli di servizio che riguardino

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 8 di 95

obiettivi per i quali siano previsti valori di soglia incrementali, verrà applicata esclusivamente la penale che si riferisce al valore più alto riscontrato.

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 9 di 95

SERVIZI PROFESSIONAL E ACCESSORI

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 10 di 95

2. SERVIZI PROFESSIONALI

Il Servizio comprende l'insieme di attività professionali di Supporto ai clienti su tematiche di natura organizzativa, istituzionale, di innovazione e operativa nonché nell'ambito dell'iter di acquisizione.

I Servizi di Supporto e Governance, indipendentemente dal contesto in cui sono erogati, prevedono il ricorso a risorse con diverse professionalità che possono essere identificate nelle seguenti figure professionali:

- **Operativa:** personale con competenze e professionalità “tecniche” e padronanza sulla materia di competenza su cui viene coinvolto.
- **Specialistica:** personale con competenze di alto livello su specifiche filiere “tecniche” e che esprime piena padronanza sulle conoscenze tecnico-professionali di ruolo, agendo anche come punto di riferimento operativo per gli specialisti impegnati nei processi di interesse.
- **Di coordinamento:** personale il cui profilo è finalizzato ad assicurare il raggiungimento di importanti risultati tecnici, economici e qualitativi attraverso il coordinamento di risorse e progetti complessi. Governano programmi e progetti, relazioni organizzative interne ed esterne articolate, e rapporti fiduciari e negoziali con i clienti.

Nell'ambito dei Servizi Professional viene offerto il mix di competenze e professionalità più opportuno sulla base del tipo di supporto richiesto dall'Amministrazione, condiviso con la stessa; l'impegno economico che ne deriva sarà

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 11 di 95
calcolato sulla base della tipologia di professionalità
richiesta.

2.1 ***SUPPORTO***

Il Servizio di supporto offerto può essere erogato nei contesti di seguito descritti:

- Contesto organizzativo
 - nelle attività di certificazione di qualità dei processi operativi dei clienti e per le indagini di customer satisfaction;
 - nelle metodologie di progettazione e conduzione di un sistema di ascolto del contribuente;
 - nella partecipazione a commissioni, gruppi di lavoro e seminari;
 - nell’assistenza anche telefonica non informatica.
- Contesto istituzionale
 - nello svolgimento dei compiti istituzionali di competenza dei clienti attraverso il trattamento ottimale delle informazioni presenti nel Sistema informativo;
 - nella individuazione di soluzioni finalizzate all’attuazione della normativa di riferimento dell’Amministrazione;
 - nelle attività per lo scambio di informazioni fra i Clienti e tra queste ed i cittadini;
 - nella gestione degli aspetti amministrativi e gestionali di specifici programmi e/o progetti finanziati con fondi europei;

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 12 di 95

– Contesto di innovazione

- nella produzione di documentazione tecnica e prototipi di soluzioni innovative;
- nella progettazione, implementazione e attuazione delle misure di sicurezza dei sistemi informativi di responsabilità nonché di quelle relative alla qualità del sistema informativo;
- nella progettazione e implementazione di architetture e applicazioni particolarmente innovative.

– Contesto Operativo

- nella formazione e tutoraggio, nonché addestramento all’uso dei servizi informatici;
- nell’attivazione tecnica delle apparecchiature acquisite nonché nell’attivazione funzionale delle soluzioni realizzate, presso le sedi dei clienti;
- nelle attività operative specifiche di settore dei singoli clienti;
- nell’assistenza tecnica periferica;
- nei servizi accessori di assistenza.

2.2 *Governance*

Il Servizio di Governance può essere erogato nei contesti di seguito descritti:

- Governance degli approvvigionamenti – comprende le attività necessarie per l’acquisizione, attraverso il ricorso al mercato, di beni e servizi a rimborso tesi al soddisfacimento dei bisogni dell’Amministrazione

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 13 di 95
 relativi allo sviluppo, alla evoluzione ed alla conduzione
 del Sistema Informativo;

- Governance dei Contratti - comprende le attività necessarie a supportare l’Amministrazione nell’attuazione delle varie fasi dei processi di pianificazione pluriennale, di programmazione annuale, di controllo e di monitoraggio per garantire il governo dei processi di gestione della Convenzione, per gli aspetti specifici derivanti dai processi dell’Amministrazione.

2.3 LIVELLI DI SERVIZIO

Servizio	Professional	
Livelli di Servizio	Soglia	Penale
		€ 250,00 per ogni giorno di ritardo successivo al decimo e sino al trentesimo giorno
Mantenimento data di consegna dell'output condivisa con l'Amministrazione	10 giorni dalla data di consegna dell'output condivisa con l'Amministrazione	€ 500,00 per ogni giorno di ritardo successivo al trentesimo e sino al sessantesimo giorno
		€ 750,00 per ogni giorno di ritardo successivo al sessantesimo

Il Livello di servizio è applicabile solo nel caso in cui il servizio di supporto abbia natura progettuale e quindi preveda

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 14 di 95

output precisamente identificabili e previsti nel Piano operativo condiviso tra le Parti.

La data di consegna dell'output di riferimento per il LdS è definita nel Piano operativo condiviso tra le Parti ed eventualmente modificata mediante scambio di comunicazione.

3. SERVIZI ACCESSORI

Si tratta di servizi accessori funzionali allo sviluppo, evoluzione e conduzione del Sistema Informativo.

In particolare comprende:

- le trasferte da effettuare su richiesta dell'Amministrazione presso i propri uffici periferici o comunque presso sedi fuori il comune di appartenenza delle sedi della Sogei utilizzando i seguenti mezzi di trasporto:
 - aereo;
 - treno;
 - altri mezzi pubblici urbani ed extra-urbani: (pullman, autobus, ecc.);
 - taxi: limitato ai soli spostamenti iniziali e terminali del viaggio di trasferimento o quando costituisca l'unico mezzo disponibile o particolari motivi di disagio o di urgenza lo richiedano;
 - autovetture a noleggio in casi eccezionali previa esplicita autorizzazione del dirigente responsabile;

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 15 di 95

- autovettura personale in casi eccezionali previa esplicita autorizzazione del dirigente responsabile.

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 16 di 95

SERVIZI DI SVILUPPO

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 17 di 95

4. PROGETTAZIONE E SVILUPPO SERVIZI ICT

Include i servizi finalizzati allo sviluppo, modifica, evoluzione e personalizzazione di soluzioni innovative rispondenti alle esigenze dei clienti.

Per l'erogazione del Servizio la Sogei adotta un Processo di produzione proprietario standardizzato, certificato secondo le norme ISO 9001:2015 e conforme con la normativa ISO 27001:2013, e ISO 25012:2014 in materia di controlli sulla sicurezza e qualità dei dati nonché alle regole introdotte dal GDPR.

Tale processo è basato sui modelli metodologici di sviluppo Evolutivo/Incrementale, RUP – Rational Unified Process e Agile applicati in funzione dei contesti di sviluppo per ottimizzare i fattori produttivi e gestionali.

La Sogei opera nell'ambito dell'Application Lifecycle Management (ALM) che identifica un approccio strategico alla gestione delle informazioni, dei processi e delle risorse a supporto del ciclo di vita delle applicazioni software.

La Manutenzione migliorativa sarà considerata parte integrante dell'effort di sviluppo e manutenzione evolutiva in quanto attività essenziale per il raggiungimento della qualità attesa nel software prodotto.

4.1 ***SVILUPPO E MANUTENZIONE EVOLUTIVA DEL SOFTWARE AD HOC***

Sogei ha la responsabilità di governare gli obiettivi di sviluppo e manutenzione evolutiva attraverso le seguenti attività:

- analisi dei requisiti;

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 18 di 95

- attuazione intervento;
- avviamento;
- verifica di conformità;
- supporto sistemistico per lo sviluppo e la manutenzione evolutiva;
- estensione.

La verifica di conformità viene eseguita in un ambiente, predisposto da Sogei, equivalente a quello di esercizio.

Per un periodo di 365 (trecentosessantacinque) giorni solari decorrenti dalla data di inizio estensione delle applicazioni software realizzate, la Sogei è impegnata a prestare, a propria cura e spese, la manutenzione correttiva delle applicazioni software.

L'effort dello sviluppo di applicazioni viene misurato mediante nuove metodologie che tengono conto delle moderne modalità di sviluppo Agile e DevOps e su architetture maggiormente complesse. Il modello dei requisiti è composto da:

- Requisiti funzionali;
- Requisiti non funzionali;
- Requisiti di progetto/ambito.

Per ciascuna di queste componenti viene stimato l'effort che essa genera utilizzando, ove possibile, unità di misura standard.

- Requisiti funzionali

Misura Funzionale = metrica compatibili con lo standard ISO/IEC 14143-1:2007 (di seguito FSM) in generale non

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 19 di 95
necessariamente function point IFPUG oppure Simple Function Point oppure COSMIC etc..

Ad oggi si utilizza come metrica funzionale di riferimento IFPUG FP versione 4.3.

– Requisiti non funzionali

Misura Impatto Non Funzionale = % di impatto sulla produttività derivante da una misura non funzionale compatibile con la ISO/IEC 25010, tenendo conto delle sottocategorie definite dalla metrica stessa (in questa fase si prende a riferimento SNAP IFPUG v2.4).

– Logiche di Operazione sui dati

- Logiche di Validazione dei dati in ingresso,
- Livello di Complessità delle Operazioni Logico e Matematiche,
- Formattazione Dati (o livello) di Movimentazione dei dati interni all'Applicazione,
- Livello di configurabilità dell'applicazione che aggiunge valore all'utente senza necessità di interventi software,

– Disegno dell'interfaccia

- Complessità delle Interfacce utente,
- Disponibilità di Guide e Manuali dell'applicazione,
- Metodi di inserimento dati tramite modalità aggiuntive,

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 20 di 95

- Metodi di presentazione dati tramite modalità aggiuntive,

– Ambiente Tecnologico

- Grado di utilizzo Piattaforme multiple aggiuntive,
- Operazione ed interventi sul database,
- Processi batch,

– Architetture software

- Grado di utilizzo di Componenti Software nell'applicazione,
- Grado di estensione delle interfacce software per motivi tecnici.

In funzione delle sottocategorie interessate, ad oggi, verrà determinato il numero di giornate aggiuntive per realizzare la componente non funzionale sulla base di uno schema di riferimento che potrà andarsi a perfezionare nel tempo.

A seguire, a fronte della disponibilità di una banca dati delle misure, si potrà introdurre una metrica di valutazione più puntuale.

– Requisiti di progetto/ambito

Misura dell'impatto dell'ambito = % di impatto sulla produttività derivante dalla complessità/instabilità dell'ambito in termini di:

- complessità della normativa di riferimento con conseguente difficoltà interpretative o alta probabilità di cambiamento,
- forte instabilità dei requisiti,

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 21 di 95

- alta numerosità degli stakeholder,
- nuovo dominio,
- dipendenze da altri progetti esterni al di fuori del controllo diretto,
- dipendenze da altri progetti interni al di fuori del controllo diretto.

Sogei, per tutti gli sviluppi che si debbano integrare con un prodotto di mercato, garantisce il pieno e corretto funzionamento della soluzione nella sua interezza. Ove, in fase di realizzazione, emergano evidenze dell'impossibilità di garantire ciò, Sogei ne darà visibilità all'Amministrazione per condividere se e come proseguire.

4.1.1 *Livelli di Servizio*

Servizio		Sviluppo e manutenzione evolutiva del software ad hoc	
Livelli di Servizio		Soglia	Penale
Difettosità alla prima verifica di conformità	0 errori (rispetto ai casi di test previsti nel piano di test)	€ 300,00 per ogni errore riscontrato	
Indice di difettosità per il software fuori garanzia (calcolato secondo la formula indicata)	Indice di difettosità <= 4 per 1000 FP in esercizio a fine periodo di rilevazione	€ 3.500,00 per ogni scostamento unitario rispetto al valore di soglia	
Indice di difettosità per software in garanzia (calcolato secondo la formula indicata)	Indice di difettosità <= 40 per 1000 FP in esercizio a fine periodo di rilevazione	€ 1.700,00 per ogni scostamento unitario rispetto al valore di soglia	

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 22 di 95

Servizio		Sviluppo e manutenzione evolutiva del software ad hoc	
Livelli di Servizio	Soglia	Penale	
		€ 250,00 per ogni giorno di ritardo successivo al decimo e sino al trentesimo giorno	
Mantenimento data di "Disponibilità alla Verifica di conformità" condivisa con l'Amministrazione	10 giorni dalla data di consegna del software condivisa con l'Amministrazione	€ 500,00 per ogni giorno di ritardo successivo al trentesimo e sino al sessantesimo giorno	
		€ 750,00 per ogni giorno di ritardo successivo al sessantesimo	

Premesso che per Applicazione si intende una “*Collezione integrata di procedure automatizzate e dati che forniscono supporto ad un obiettivo applicativo; essa è formata da uno o più componenti, moduli, o sottosistemi*”, il calcolo dell’indice di difettosità del software avviene applicando per ciascuna delle fasce di garanzia previste per il software in esercizio la seguente formula:

$$\text{difettosità}_j = \frac{\sum_{k=1}^{N_j} \text{difetti}_{jk}}{\sum_{k=1}^{N_j} fp_{jk}} * 1000$$

in cui al numeratore troviamo la sommatoria dei difetti

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 23 di 95

segnalati nel periodo di osservazione per ciascuna Applicazione (K) nella fascia (f) e al denominatore la sommatoria di tutti i FP delle Applicazioni (k) nella fascia di garanzia (f).

Il software si considera in esercizio dall'inizio della fase di estensione; il software si considera in garanzia nei primi dodici mesi di esercizio.

Le date di "Disponibilità alla Verifica di Conformità" di riferimento per il LdS vengono definite inizialmente nel Piano operativo condiviso e approvato tra le Parti e successivamente possono essere modificate mediante scambio di comunicazione.

4.2 **PERSONALIZZAZIONE DEL SOFTWARE DI MERCATO**

Il Servizio è finalizzato alla realizzazione di soluzioni basate su parametrizzazione e personalizzazione di pacchetti software acquistati sul mercato.

La Sogei applica tale servizio in caso di:

- personalizzazione/parametrizzazione di prodotti software di mercato (con particolare riferimento ai sistemi ERP - Enterprise Resource Planning);
- realizzazione di interventi di Data Warehouse (DW) e business intelligence (B.I.).

In particolare, il servizio di personalizzazione del software di mercato consiste in:

- sviluppo residuale di funzioni fortemente integrate con il prodotto nell'ambito del quale la personalizzazione viene effettuata che comporta la conoscenza del prodotto e dell'eventuale linguaggio proprietario;

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 24 di 95

- interventi effettuati su prodotti con tecnologie/linguaggi non dimensionabile correttamente attraverso l'uso del FP (ad esempio BI).

Gli sviluppi esterni al prodotto che ne consentono l'estensione in termini di funzionalità, sono invece considerati sviluppi ad hoc e come tali dimensionati e remunerati.

Tale servizio viene erogato attraverso un processo di produzione che:

- parte da un'analisi comparativa, tra il prodotto base ed i requisiti dell'utente (gap-analysis), volta ad evidenziare quali requisiti non sia possibile soddisfare mediante l'attività di parametrizzazione e per i quali di conseguenza occorrerebbero degli interventi di personalizzazione;
- si sviluppa in attività progressive di affinamento di un modello iniziale standard;
- condivide con l'Amministrazione ogni attività di affinamento;
- utilizza estensivamente un approccio prototipale.

Per quanto riguarda gli interventi di Datawarehouse e BI il servizio prevede l'utilizzo di specifiche tecnologie quali i tool di modellazione dei dati, gli strumenti di gestione dei metadati (Repository), i tool di ETL, gli strumenti di visualizzazione oltre che la realizzazione di software dedicato.

Indipendentemente dalle tecnologie adottate, il processo presenta caratteristiche omogenee relativamente all'articolazione in fasi (analisi dei requisiti, attuazione,

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 25 di 95

avviamento, verifica di conformità) e alla documentazione prodotta a supporto.

Sogei garantisce che le personalizzazioni si integrino correttamente con il prodotto di base e segnalera anticipatamente all'Amministrazione se, l'intervento richiesto, in fase di realizzazione facesse emergere problematiche in tal senso.

Per un periodo di 365 (trecentosessantacinque) giorni solari, decorrenti dalla data di inizio estensione delle applicazioni software, la Sogei è impegnata a prestare, a propria cura e spese, la manutenzione correttiva delle personalizzazioni effettuate.

4.2.1 *Livelli di Servizio*

Servizio		Personalizzazione del software di mercato	
Livelli di Servizio		Soglia	Penale
Difettosità alla prima verifica di conformità	0 errori rispetto ai casi di test previsti nel piano di test	€ 300,00 per ogni errore riscontrato	
Mantenimento data di "Disponibilità alla Verifica di conformità" condivisa con l'Amministrazione	10 giorni dalla data di consegna del software condivisa con l'Amministrazione	€ 250,00 per ogni giorno di ritardo successivo al decimo e sino al trentesimo giorno € 500,00 per ogni giorno di ritardo successivo al trentesimo e sino al sessantesimo	

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 26 di 95

Servizio	Personalizzazione del software di mercato		
	Livelli di Servizio	Soglia	Penale
		giorno € 750,00 per ogni giorno di ritardo successivo al sessantesimo	

Le date di “Disponibilità alla Verifica di Conformità” di riferimento per il LdS vengono definite inizialmente nel Piano operativo condiviso e approvato tra le Parti e successivamente possono essere modificate mediante scambio di comunicazione.

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 27 di 95

SERVIZI DI BASE DI CONDUZIONE

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 28 di 95

5. SERVIZI DI BASE DI GESTIONE, CONDUZIONE E MANUTENZIONE

In tale ambito rientrano i servizi di gestione e conduzione infrastrutturale, i servizi di manutenzione adeguativa e correttiva delle applicazioni rilasciate e il servizio di Customer Care.

5.1 **GESTIONE E CONDUZIONE SERVIZI ICT**

5.1.1 **Manutenzione servizi ICT**

Il servizio comprende le attività necessarie per garantire il corretto funzionamento del Sistema Informativo tramite la manutenzione del software in esercizio.

Il servizio si applica sia alle applicazioni realizzate attraverso il servizio di “Sviluppo e Manutenzione Evolutiva di software ad hoc” sia a quanto realizzato attraverso il servizio di “Personalizzazione di prodotti di mercato”. Per queste ultime, il servizio riguarda solamente la componente software realizzata da Sogei come personalizzazione.

Il servizio di manutenzione del software in esercizio, nel seguito denominato MAC (Manutenzione Adeguativa e Correttiva), comprende le seguenti tipologie di interventi:

- Manutenzione correttiva: modifica reattiva di un prodotto software consegnato per correggere i problemi rilevati. La modifica sarà misurata sulla base di interventi software volti a rimuovere i malfunzionamenti (incident) segnalati dagli utenti o rilevati proattivamente da Sogei stessa; la remunerazione della manutenzione correttiva decorre dalla data di termine del periodo di garanzia del software;
- Manutenzione adeguativa: comprende le modifiche necessarie ad allineare il software ai cambiamenti dell’ambiente tecnologico. In particolare la manutenzione

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 29 di 95

sarà calcolata sulla base di interventi sul software che adeguano ai mutamenti intervenuti nell'ambiente tecnologico di riferimento (sistema operativo, database, etc.). La remunerazione della manutenzione adeguativa decorre dalla data di avvenuta estensione del software.

Orario di servizio: lunedì-venerdì dalle 8:00 alle 18:00

5.1.1.1 Livelli di Servizio

Servizio		Manutenzione servizi ICT	
Livelli di Servizio	Soglia	Penale	Orario di osservazione
Tempo massimo di intervento	entro 12 h lavorative nel 96% dei casi	€ 1.000,00 per ogni evento di violazione occorsa	8.00 - 18.00 lun – ven
	e comunque entro 18 h lavorative nel 100% dei casi	€ 1.800,00 per ogni evento di violazione occorsa	
Tempo massimo di ripristino	entro 24 h lavorative nel 96% dei casi	€ 1.200,00 per ogni evento di violazione occorsa	
	e comunque entro 36 h lavorative nel 100% dei casi	€ 2.000,00 per ogni evento di violazione occorsa	

Di seguito alcune precisazioni.

Tempo di intervento: tempo intercorrente tra la segnalazione del disservizio e la notifica all'utente della diagnosi di massima e del tempo di ripristino previsto.

Tempo di ripristino: tempo intercorrente tra la notifica

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 30 di 95

all’utente del tempo di ripristino previsto e l’effettivo ripristino (previa correzione) delle funzionalità oggetto dell’intervento.

Le segnalazioni pervengono attraverso il sistema di tracciatura dell’assistenza applicativa relativa al Sistema informativo di PCM; verranno conteggiati anche gli interventi eseguiti a seguito di una rilevazione effettuata direttamente da Sogei in modalità proattiva (il ticket risolto non sarà oggetto di consuntivazione).

5.1.2 *Servizio di customer care*

Il servizio di Customer Care è finalizzato ad offrire supporto agli utenti per:

- risposta ad esigenze informative;
- soluzione di problematiche tecniche, anche collegate alle postazioni di lavoro del personale dell’Amministrazione;
- soluzione di problematiche inerenti ai Servizi ICT erogati;
- anticipare le esigenze dei clienti e prevenire le richieste di servizio;
- fornire una Customer Service proattiva e completa ai fini di un servizio di assistenza più efficiente ed efficace, realizzando, laddove è possibile, sistemi autonomatici di risposta o invio di informazioni verso caselle di posta o numeri telefonici.

Il Servizio di Customer Care è costituito da un insieme di servizi modulari sia di tipo infrastrutturale che organizzativo utilizzabili anche singolarmente.

È possibile, per soddisfare esigenze strategiche di utenti definiti VIP e/o a fronte di Servizi ICT di particolare

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 31 di 95

rilevanza, prevedere modalità di assistenza specifiche.

5.1.2.1 Customer Management

Il Servizio comprende l'assistenza agli utenti interni ed esterni all'Amministrazione per la soluzione di problemi che l'utente stesso può incontrare nell'interazione con il Sistema Informativo.

L'assistenza è erogata tramite una struttura di Customer Support con escalation alle strutture specialistiche Sogei dei diversi domini ICT, tecnici e applicativi dando origine ad interventi di Supporto Specialistico.

Il sistema è stato strutturato per offrire una soluzione completa di “Customer Relationship Management” (CRM), ovvero un sistema per organizzare le informazioni di contatto, gestire le relazioni, tracciare le interazioni con i clienti al fine di efficientare la produttività. Il servizio è stato integrato con tecnologie di tipo “cognitivo”, basate sull’analisi e sulla comprensione del linguaggio naturale, in grado di auto apprendere dalla continua analisi dei dati e dall’interazione con altri sistemi o con il personale.

Le richieste possono essere di diversa tipologia: Informative, Incidents (hardware, software, ecc.), Service Request e possono essere effettuate tramite:

- canale telefonico;
- canale web, con l'utilizzo dello strumento email o ticket di assistenza, con soluzioni self-service a partire dalle Faq;
- canali social dedicati per fornire risposte rapide e permettere ai clienti di entrare direttamente in contatto con il servizio di assistenza;

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 32 di 95

- “live caring” ovvero l’assistenza via chat per fornire risposte in tempi rapidi etc..

Dal punto di vista dell’offerta alcuni dei servizi descritti possono essere attivati a richiesta.

Il servizio comprende la formazione del personale in risposta al Customer Support, il controllo e il reporting del servizio.

L’erogazione del Customer Support può avvenire secondo diverse classi di servizio:

- Base: lun-ven 8,00-18,00 e sab 8,00-14,00;
- Ampliato: per “ora” aggiuntiva in funzione delle esigenze dell’Amministrazione fino ad una copertura h24 7 giorni su 7.

La remunerazione è in termini di canone per la disponibilità del servizio e di corrispettivi unitari per le richieste di assistenza risolte dal Customer Support e dal Supporto Specialistico.

Per l’ampliamento dell’orario del Customer Support è prevista una remunerazione in termini di giornate secondo quanto previsto nell’ambito dei servizi Professional dimensionati in accordo con l’Amministrazione.

Si precisa che non verrà corrisposto nessun importo per le seguenti tipologie di richieste:

- solleciti;
- chiamate su problemi precedentemente chiusi, ma la cui soluzione non è risultata soddisfacente;
- cadute linea;
- chiamate dirette ad altro Call Center;

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 33 di 95

- chiamate “improprie”;
- richieste "chiuse d'ufficio", comprese quelle di tipo specialistico gestite dalle strutture competenti Sogei (una richiesta si intende "chiusa d'ufficio" se è non risolta, non sospesa, pervenuta almeno 60 gg solari prima della rilevazione e senza solleciti nei 30 gg precedenti la rilevazione).

5.1.2.1.1 Livelli di Servizio

Servizio		Customer Management	
Livelli di Servizio	Soglia	Penale	Orario di osservazione
Disponibilità del servizio	Indisponibilità del servizio nel quadri mestre < 1 h nell'orario della classe di appartenenza	€ 455,00 per ogni ora di mancata disponibilità del servizio (in caso di più Amministrazioni aderenti alla medesima piattaforma, la penale si intende relativa ad ogni Amministrazione)	lun-ven 8,00-18,00 e sab 8,00-14,00
Tempo di attesa prima della risposta	entro 40 sec nel 95% dei casi nell'orario della classe di appartenenza	€ 200,00 a superamento della soglia nel periodo (in caso di più Amministrazioni aderenti alla	classe di

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 34 di 95

Servizio		Customer Management	
Livelli di Servizio	Soglia	Penale	Orario di osservazione
		medesima piattaforma, la penale si intende relativa ad ogni Amministrazione)	servizio ampliata fino ad un massimo di H24
	entro 120 sec (target massimo) nel 100% dei casi nell'orario della classe di appartenenza	€ 300,00 a superamento della soglia nel periodo (in caso di più Amministrazioni aderenti alla medesima piattaforma, la penale si intende relativa ad ogni Amministrazione)	
Chiamate dissuase	<=5% chiamate dissuase su totale chiamate pervenute nell'orario della classe di appartenenza	€ 0,10 per ogni evento che non rispetta il LdS (in caso di più Amministrazioni aderenti alla medesima piattaforma, la penale si intende	

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 35 di 95

Servizio		Customer Management	
Livelli di Servizio	Soglia	Penale	Orario di osservazione
		relativa ad ogni Amministrazione)	
Tempo soluzione di richieste al Customer Support	entro 20 min nel 60% dei casi nell'orario della classe di appartenenza	€ 0,2 per ogni richiesta che non rispetta il LdS	8.00 - 18.00 lun - ven
	entro 4 ore nel 100% dei casi nell'orario della classe di appartenenza	€ 0,6 per ogni richiesta che non rispetta il LdS	
Tempo soluzione di richieste al Supporto Specialistico (di tipo applicativo)	entro 12 ore per il 70% dei casi	€ 0,7 per ogni richiesta che non rispetta il LdS	8.00 - 18.00 lun - ven
	entro 24 ore per l'85% dei casi	€ 1,4 per ogni richiesta che non rispetta il LdS	
	entro 3 giorni per il 100% dei casi	€ 2 per ogni richiesta che non rispetta il LdS	
Tempo soluzione di richieste al Supporto Specialistico (di tipo tecnico per utenti esterni)	entro 1 giorno per il 70% dei casi	€ 0,7 per ogni richiesta che non rispetta il LdS	8.00 - 18.00 lun - ven
	entro 5 Giorni per il 97% dei casi	€ 1,4 per ogni richiesta che non rispetta il LdS	
	entro 20 Giorni per il 100% dei casi	€ 2 per ogni richiesta che non rispetta il LdS	

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 36 di 95

Di seguito alcune precisazioni.

Per tutti gli indicatori suddetti, ad eccezione della “Disponibilità del servizio”, ai fini del calcolo delle penali verranno escluse le violazioni indotte da un numero di chiamate pervenute superiori al volume massimo che dovrà essere definito sulla base del quale verrà organizzato il servizio.

Si procederà alla “chiusura di ufficio” su rilevazione mensile di tutte le richieste di assistenza non risolte e non sospese per le quali si verificano entrambe le seguenti condizioni:

- la richiesta è pervenuta almeno 60 giorni solari prima del giorno di rilevazione;
- la richiesta non ha avuto solleciti nei 30 giorni solari precedenti il giorno di rilevazione.

Per ciascuna di tali richieste non verrà riconosciuto a Sogei alcun corrispettivo.

Per chiamate dissuase si intendono le chiamate alla quale si risponde automaticamente con un messaggio di invito a richiamare successivamente. Tale messaggio viene proposto quando gli addetti sono tutti occupati e non ci sono più posizioni di coda disponibili.

5.1.2.2 Servizio di collaborazione specialistica

Nel caso in cui si abbia la necessità di gestire un picco di richieste di assistenza che coinvolgano il Supporto Specialistico Sogei, si può configurare un servizio di collaborazione che prenda in carico aspetti di classificazione delle richieste, razionalizzazione ed efficientamento dell'intervento del Supporto Specialistico Sogei e metta in

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 37 di 95

campo competenze necessarie per la risoluzione di richieste di assistenza che non possano essere risolte dal Customer Support (ad esempio per impossibilità di accesso ad applicazioni o basi dati). Nel servizio è inclusa la formazione del personale coinvolto.

Il Servizio assume l'orario dell'equivalente Servizio di Customer Management del Customer Support richiesto.

I problemi risolti in tale contesto non sono oggetto di remunerazione nell'ambito del Servizio di assistenza del Supporto Specialistico e sono remunerati in termini di giornate, secondo quanto previsto nell'ambito del servizio di Professional.

5.1.2.3 Erogazione del servizio con operatore in lingua

Tale servizio è finalizzato ad estendere il Servizio di Customer Support erogato in lingua italiana anche alle lingue inglese, tedesco e francese.

Verranno fornite report che diano evidenza della modalità di erogazione del servizio stesso.

Il Servizio assume l'orario dell'equivalente Servizio di assistenza richiesto.

I problemi risolti in tale contesto sono remunerati in termini di giornate nell'ambito del servizio Professional e non secondo la remunerazione del Servizio di Customer Support.

5.1.2.4 Esercizio del servizio in modalità automatica tramite IVR

Tale servizio si basa sull'utilizzo di applicazioni vocali accessibili tramite canale telefonico grazie alle quali erogare contenuti informativi di carattere generale (FAQ, news etc).

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 38 di 95

Dopo l’interazione con tale strumento è possibile prevedere o meno il passaggio ad un operatore di Customer Support.

La predisposizione delle applicazioni vocali è remunerata in termini di giornate secondo quanto previsto nell’ambito del servizio Professional.

5.1.2.5 Erogazione del servizio in modalità automatica tramite chatbot

Il servizio consente di gestire un’interazione automatica via chat tra l’utente ed un sistema di AI opportunamente addestrato sugli argomenti inerenti il dominio di interesse.

La “formazione” dello strumento per la gestione delle risposte può essere effettuata utilizzando FAQ o documentazione di riferimento. Nella fase di addestramento del prodotto è necessaria la disponibilità di personale dell’Amministrazione con esperienza sul contesto trattato.

La progettazione del dialogo utente-sistema sulla base delle esigenze di comunicazione dell’Amministrazione consente di realizzare una soluzione ad hoc per le specifiche esigenze.

La finestra di dialogo via web può essere resa disponibile su siti dell’Amministrazione ed opportunamente personalizzata in termini di grafica e di elementi di comunicazione.

Successivamente alla messa in linea dello strumento è possibile prevedere opzionalmente la disponibilità di un servizio di supporto e monitoraggio per l’analisi del servizio erogato in termini quantitativi e qualitativi, ai fini di un efficientamento del servizio.

Il servizio prevede distinte voci di remunerazione:

- sistema di chatbot in termini di volume di conversazioni tra utente e sistema;

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 39 di 95

- finestra di dialogo via web in termini di giornate di sviluppo, nell’ambito del servizio “Personalizzazione del software di mercato”, in funzione delle esigenze dell’Amministrazione;
- formazione dello strumento, supporto e monitoraggio in termini di giornate nell’ambito del servizio Professional.

Orario del Servizio: H24

5.1.2.5.1 Livelli di Servizio

Servizio	Erogazione del servizio in modalità automatica tramite chatbot		
Livelli di Servizio	Soglia	Penale	Orario di osservazione
Disponibilità del servizio	98%	€ 0,25 per ogni punto percentuale di diminuzione rispetto al valore prefissato (in caso di più Amministrazioni aderenti alla medesima piattaforma, la penale si intende relativa ad ogni Amministrazione)	H24

5.1.2.6 Canali aggiuntivi per l’accesso al Customer Care

Il servizio consente di ampliare la modalità di contatto tra utente ed erogatore del servizio in modo da facilitare l’utente nella scelta della modalità di interazione che preferisce.

I canali di contatto aggiuntivi a quello telefonico e via web mail, già ricompresi nel servizio base, sono i seguenti:

- Chat con operatore;

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 40 di 95

- Social (Facebook, Twitter etc);
- SMS;
- E-mail.

Il servizio è remunerato in termini di importo iniziale di sottoscrizione/attivazione dei canali e canone per la disponibilità all'utilizzo. Remunerazione specifica, è prevista per l'invio di messaggi in funzione dei volumi. Per la remunerazione delle richieste di assistenza risolte e pervenute da questi canali, si fa riferimento a quanto riportato nel servizio di Customer Management.

Orario del Servizio: lunedì-venerdì 8:00-18:00 e sabato 8:00-14:00

Ore aggiuntive per il Customer Support fino ad un massimo di H24

5.1.2.6.1 Livelli di Servizio

Servizio	Canali aggiuntivi per l'accesso al Customer Care		
Livelli di Servizio	Soglia	Penale	Orario di osservazione
Disponibilità del servizio	98%	<p>€ 0,25 per ogni punto percentuale di diminuzione rispetto al valore prefissato (in caso di più Amministrazioni aderenti alla medesima piattaforma, la penale si intende relativa ad</p>	<p>nell'orario della classe di appartenenza rilevazione quadriennale</p>

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 41 di 95

Servizio		Canali aggiuntivi per l'accesso al Customer Care		
Livelli di Servizio	Soglia	Penale	Orario di osservazione	
		ogni Amministrazione)		

Dall'applicazione dei Livelli di servizio sono escluse le disponibilità degli strumenti Social come Facebook e Twitter in quanto dovute a problematiche non direttamente dipendenti da Sogei.

5.1.2.7 Gestione campagne di outbound

Il servizio comprende il supporto e gli strumenti necessari per la gestione di campagne di outbound per la realizzazione di campagne comunicative o per la rilevazione della customer satisfaction sui servizi erogati.

Sulla base delle specifiche esigenze la comunicazione con l'utente può avvenire tramite uno o più canali di contatto anche in modalità integrata.

Il servizio è remunerato in termini di importo iniziale di sottoscrizione/attivazione e canone per la disponibilità all'utilizzo.

Una remunerazione specifica aggiuntiva è prevista nel caso di campagne di outbound che utilizzano canali con invio di messaggi e si basa sul volume dei messaggi inviati.

5.1.2.8 Knowledge Base

Nell'ambito del Knowledge Management il servizio comprende il supporto e gli strumenti necessari per la predisposizione di strumenti di assistenza su web per permettere all'utente di gestire in autonomia le sue necessità

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 42 di 95

di supporto.

Il sistema è orientato alla rappresentazione granulare delle informazioni, come best practice, procedure e soluzioni, più direttamente rilevanti per uno specifico adempimento amministrativo e/o per lo svolgimento di una determinata attività lavorativa.

Le unità di "conoscenza" possono essere organizzate in base alla gerarchia degli argomenti, o "albero della conoscenza". Un'altra possibilità è data dall'utilizzo di reti di nodi interconnessi tramite relazioni logiche. Reti e alberi di conoscenza possono essere modellati e alimentati in modo diverso dalle diverse comunità di utenti, raggruppati secondo il loro profilo e il loro schema concettuale, attraverso forum di discussione o sezioni personalizzabili in cui è possibile creare unità informative strutturate.

Le KB, a fronte di specifiche esigenze dell'Amministrazione, possono essere rese disponibili con la componente aggiuntiva di community tramite la quale è possibile rendere disponibili servizi e funzionalità quali:

- accesso autenticato per l'utente con organizzazione dei contenuti informativi profilati;
- area personale per l'apertura, la tracciatura dello stato di lavorazione, lo storico dei propri "case";
- creazione automatica di contenuti informativi da poter pubblicare, anche tramite workflow approvativo, attingendo informazioni tramite strumenti di intelligenza artificiale da diverse fonti quali canali social e "case" relativi alla pluralità dei canali di contatto utilizzati per il

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 43 di 95

servizio di assistenza. Il contenuto informativo gestito con tale strumento ha la peculiarità di non scaturire unicamente da una produzione redazionale di tipo classico, bensì dalle necessità effettive degli utenti espresse sia tramite richieste di supporto ed assistenza alle strutture preposte, sia in modo spontaneo tramite i canali social.

Questi sistemi hanno generalmente diversi tipi di utenti per i quali è previsto un ruolo supportato dalla soluzione tecnologica adottata: il lettore, o consumatore della "conoscenza", il redattore, o produttore della "conoscenza" (che in alcuni casi può contribuire alla creazione della "conoscenza", in altri dà anche la propria opinione al riguardo), il coordinatore, il cui ruolo è quello di sovrintendere ai contributi, e infine l'esperto.

È prevista una remunerazione in termini di giornate nell'ambito del servizio Professional, per la predisposizione di strumenti di assistenza web e dei loro contenuti informativi; mentre una specifica remunerazione, è prevista per le utenze di redazione eventualmente richieste dall'Amministrazione e per la componente di community.

5.1.2.9 Supporto per assistenza specifica

Il servizio prevede la disponibilità di personale Sogei per svolgere attività di assistenza su particolari processi o servizi non previste negli altri Servizi di assistenza agli utenti. In questo caso l'effort sarà valutato e remunerato nell'ambito del servizio Professional.

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 44 di 95

5.1.2.10 *Dashboard*

Il servizio prevede per gli utenti dell'Amministrazione la disponibilità di dashboard per il monitoraggio e l'analisi dei dati relativi ai servizi di customer management e servizio di collaborazione specialistica, chatbot, KB.

La dashboard, messa a disposizione dell'utente per la consultazione, utilizza anche strumenti di intelligenza artificiale per il discovery delle informazioni di riferimento.

Per la predisposizione della dashboard è prevista una remunerazione in termini di giornate nell'ambito del servizio di Professional di cui al paragrafo 2; inoltre per l'utilizzo della dashboard predisposta è prevista una specifica remunerazione, sia in relazione al numero di utenze richiesta dall'Amministrazione che per l'attivazione del servizio stesso.

5.2 *GESTIONE E CONDUZIONE INFRASTRUTTURA*

La gestione dei sistemi include le attività necessarie per condurre, mantenere funzionante ed aggiornata l'infrastruttura hardware e software utilizzata per l'erogazione di più servizi informatici. Questo insieme di Servizi si identifica come la gestione dell'esercizio dei sistemi la cui criticità necessita di essere garantita h24x365 e con reperibilità, interventi festivi e notturni, per mantenere la piena efficienza anche a fronte di problematiche.

Riguarda questa classe di servizi l'insieme degli investimenti, costi, risorse, infrastrutture che concorrono a garantire la conduzione, lo sviluppo tecnologico e l'erogazione dei servizi ICT ospitati nel Data Center Sogei o che usufruiscono anche

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 45 di 95

di piattaforme esterne (cloud) comunque gestite e selezionate da Sogei.

Si precisa che il buon funzionamento di Server, Storage, Appliance e Piattaforma bigdata è misurato attraverso livelli di servizio i cui i indicatori (tempi di ripristino in caso di disastro e tempi di disponibilità) si intendono riferiti ai Servizi ICT erogati su tali piattaforme:

Livelli di Servizio	Soglia	Penale	Orario di osservazione
Tempo di ripristino in caso di disastro	24 ore solari	€ 70,00 rispetto ad ogni ora di ritardo per Servizio ICT successiva alla soglia fissata	
Disponibilità del Servizio ICT erogato attraverso l'infrastruttura sottostante	99,0%	€ 1.250,00 per ogni decimo di punto percentuale di diminuzione rispetto al valore prefissato	H24

5.2.1 *Server*

La Conduzione centrale – Server comprende la conduzione tecnico operativa e sistemistica del componente Server dei sistemi open centrali, incluse le attività relative alla sicurezza e alla rete in ambiente Open centrale.

La struttura dei servizi, inclusi nel driver SERVER, si può suddividere in:

- Infrastrutture IT,
- Piattaforme & DATI,

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 46 di 95

- Applicazioni.

Infrastrutture IT

Comprende la gestione dei sistemi sino al sistema operativo e le relative componenti di base in termini di configurazione e tuning, redazione di procedure di controllo, allestimento e gestione di ambiti virtuali, produzione di report analitici sull'operatività degli ambienti, ecc.).

Rientrano nel servizio le piattaforme hardware a supporto, nonché le attività di predisposizione delle infrastrutture server fino all'hypervisor, ove presente, per tutte le tipologie di sistemi e le relative componenti software di base al di fuori di quelle che rientrano nell'ambito del servizio IAM e Appliance.

Sono incluse inoltre tutte le licenze software di base, del sistema operativo, dell'hypervisor, dei gestori di volumi, delle componenti di alta affidabilità, dei software di automazione e di tutte le componenti necessarie al provisioning e configurazione dei sistemi, nonché le attività ad essi correlate di configurazione, mantenimento ed evoluzione.

Si aggiungono a queste tutte le componenti legate alla parte di connettività e di sicurezza. Sono incluse in questo ambito anche tutte le componenti ed i servizi relativi a strumenti di automazione, software defined, orchestrazione etc, che concorrono all'erogazione dei servizi di infrastruttura (di tipo IaaS) secondo modelli di tipo ‘cloud’.

Sono inoltre incluse tutte le componenti tecnologiche hw e sw ed i relativi servizi associati, per il controllo ed il monitoraggio delle componenti infrastrutturali.

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 47 di 95

Tale monitoraggio è organizzato e strutturato, secondo il paradigma ITIL, in una Service Control Room che contempla tutti i tre livelli in cui l'ambito server è qui ‘descritto’.

Piattaforme & Dati

Comprende la gestione del middleware applicativo ovvero tutta la parte costituita da Application Server o analoghi in cui fisicamente venga collocato il codice applicativo, nonché i vari prodotti a supporto. Sono incluse in questo ambito anche tutte le componenti ed i servizi relativi a strumenti di automazione, software defined, orchestrazione etc, che concorrono all’erogazione dei servizi di piattaforma secondo modelli di tipo ‘cloud’.

Alla gestione di questi ambiti va aggiunto quanto necessario per quelli che concorrono all’erogazione complessiva dei servizi al di fuori dei classici tier della pila WEB: in particolare trattasi di sistemi di elaborazione destinati al trattamento dei dati ricevuti, soprattutto attraverso canali telematici.

Anche questo livello comprende l’area destinata al monitoraggio.

Applicazioni

Si tratta del livello più elevato della pila infrastrutturale a supporto delle applicazioni. Comprende i servizi di deploy strutturato delle applicazioni e tutte le attività ad esse correlate.

Anche questo livello comprende l’area destinata al monitoraggio: in particolare, rientrano qui le attività di analisi delle problematiche e delle ottimizzazioni.

Continuità Operativa – Disaster recovery Servizi ICT

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 48 di 95

Per Continuità Operativa ICT si intende l'insieme delle misure tecnico-organizzative volte a garantire che le prestazioni rese dai processi ICT asserviti al business dell'Organizzazione siano sempre disponibili.

Nell'ambito della Conduzione centrale SERVER si inquadra il servizio Disaster Recovery della componente di business che ha come fine quello di permettere agli utenti la ripresa delle attività produttive, sui servizi che ritiene critici, in caso di disastro che colpisca il sito primario che si trova a Roma. Con tale servizio viene messa a disposizione la capacità elaborativa necessaria alla ripresa delle attività e la relativa connettività presso una sede remota appositamente strutturata. Il Servizio comprende le attività necessarie per la realizzazione di una soluzione tecnologica in linea con le esigenze dell'Amministrazione e comprendente la predisposizione e l'attrezzaggio di un sito alternativo (o di DR) che consenta la ripartenza dei servizi ICT in caso di indisponibilità del sito primario. Include anche le attività di conduzione del sito di DR e l'esecuzione di test periodici per verificare l'adeguatezza della soluzione realizzata.

Per la connettività si attestano sul sito di recovery i link usati per il back-up. Il servizio ha come presupposto la disponibilità della copia dei dati effettuata con il servizio di Disaster Recovery delle banche dati (storage), che se non specificamente rifiutato da parte dell'Amministrazione, è attivato di norma, a garanzia della costante disponibilità del dato. La verifica della correttezza delle azioni di predisposizione viene effettuata ogni 6 mesi con la ripartenza sul sito di recovery delle applicazioni di backup. Con cadenza

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 49 di 95
 annuale viene effettuata una prova di ripartenza con la partecipazione di un selezionato numero di utenti finali.

L'orario del servizio è H24.

5.2.1.1 Livelli di Servizio

In caso in cui venga richiesto un orario H24 senza possibilità di prevedere fermi concordati, ne verrà valutata la fattibilità e attivato un apposito servizio PLATINUM remunerato sulla base delle risorse aggiuntive necessarie.

Servizio	Server			
	Livelli di Servizio	Soglia	Penale	
Disponibilità del Servizio ICT erogato attraverso l'infrastruttura sottostante (cpu, ram immagine)	vedi tabella par. 5.2 "Gestione e conduzione infrastruttura"			
Tempo di ripristino del Servizio ICT in caso di disastro	vedi tabella par.5.2 "Gestione e conduzione infrastruttura"			H24
Tempi di risposta	I Servizi ICT oggetto di analisi e la relativa soglia, verranno definiti fra le Parti nel corso di definizione del Piano Operativo annuale	€ 100,00 per ogni decimo di punto percentuale di diminuzione rispetto al valore prefissato		

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 50 di 95

Servizio	Server			
	Livelli di Servizio	Soglia	Penale	Orario di osservazione
	corrispondono ai requisiti espressi in fase di sviluppo/MEV.			
Esito positivo, per Servizio ICT, della prova di verifica periodica in data concordata (nel rispetto del calendario concordato)	10 giorni di ritardo rispetto alla data concordata	€ 50,00 per ogni giorno di ritardo dall'undicesimo al trentesimo; € 100,00 per ogni giorno di ritardo dal trentunesimo al sessantesimo; € 150,00 per ogni giorno di ritardo successivo al sessantesimo		

Il calendario delle prove di DR è unico per le varie infrastrutture, quindi la penale verrà applicata una sola volta.

5.2.2 Storage

La Conduzione centrale – Storage riguarda la conduzione tecnico operativa e sistemistica del componente DISK STORAGE (inclusi Backup-Restore dei dati ed archiviazioni a medio lungo termine) per gli ambienti OPEN, garantendo la massima disponibilità, anche mediante tecnologia RAID.

Nella gestione delle banche dati vengono utilizzate tecnologie, architetture e modalità operative per assicurare la

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 51 di 95
costante disponibilità dei dati e del servizio, anche in caso di possibili eventi disastrosi.

Accanto alla copia on-line su disco viene resa disponibile anche una copia su nastro o su disco specializzato - Backup. Il servizio mette a disposizione sia l'infrastruttura che l'esercizio e la conduzione della stessa.

Il servizio **Disaster Recovery Storage** mette a disposizione una copia dei dati considerati vitali presso un sito alternativo a quello primario. Questa copia in caso di disastro è la base per poter ripristinare nel sito alternativo le attività dell'Amministrazione. Per disporre di questa copia sempre aggiornata, la copia stessa viene effettuata on-line in modalità asincrona con quella esistente nel sito primario. La verifica della correttezza della copia effettuata avviene ogni 6 mesi con l'esecuzione di specifiche procedure di ripartenza delle applicazioni su basi dati scelte a campione; per l'esecuzione di queste prove senza interrompere l'attività di copia on-line, si usa una seconda copia di dati eseguita "Point in Time". Lo Storage Disaster Recovery riguarda la parte dati e banche dati memorizzata su disco in SAN e se non specificamente rifiutato da parte dell'Amministrazione, è attivato di norma, a garanzia della costante disponibilità del dato.

L'orario del servizio è H24.

5.2.2.1 Livelli di Servizio

Servizio	Storage		
	Soglia	Penale	Orario di osservazione
Livelli di Servizio			
Disponibilità del	vedi tabella 5.2 "Gestione e conduzione		H24

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 52 di 95

Servizio	Storage		
	Soglia	Penale	Orario di osservazione
Livelli di Servizio			
servizio erogato dall'infrastruttura sottostante (GB)		infrastruttura"	
Disponibilità del servizio di DR	98%	€ 50,00 per ogni decimo di punto percentuale di diminuzione rispetto al valore prefissato (in caso di più Amministrazioni aderenti alla medesima piattaforma, la penale si intende relativa ad ogni Amministrazione)	
Esito positivo della prova di verifica periodica in data concordata (nel rispetto del calendario concordato)	10 giorni di ritardo concordata	€ 250,00 per ogni giorno di ritardo dall'undicesimo al trentesimo; € 500,00 per ogni giorno di ritardo dal trentunesimo al sessantesimo; € 750,00 per ogni	

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 53 di 95

Servizio		Storage	
Livelli di Servizio	Soglia	Penale	Orario di osservazione
		giorno di ritardo successivo al sessantesimo	

5.2.3 *Appliance*

La Conduzione centrale – Appliance riguarda la conduzione tecnico operativa e sistemistica del componente Appliance e Sistemi Integrati a supporto del Sistema informativo.

Gli apparati che garantiscano migliori prestazioni e semplicità gestionale sono:

- Apparati specializzati - Apparecchiature ingegnerizzate per particolari soluzioni applicative al fine di rendere maggiormente efficienti le elaborazioni rispetto alle piattaforme tradizionali.
- Converged infrastructure o Sistemi Integrati - che integrano diverse componenti quali server, storage e connettività ad alta banda per migliorarne le prestazioni.

Nel Data Center Sogei sono utilizzate in tre ambiti specifici:

1. **Apparati DB transazionali (Appliance T)** - Appliance di categoria Enterprise con funzionalità di gestione delle basi dati transazionali in ambito open.
2. **Apparati DB Analytics (Appliance-A)** - Appliance di categoria Enterprise con funzionalità di gestione delle basi dati di back-end per datawarehouse ed Advanced Analytics in ambito open.

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 54 di 95

3. Piattaforma per la gestione di code QUEUE-Management (Appliance Q)

- Il servizio rende disponibile alle componenti applicative un sistema di gestione code (queue management) e offre l'accesso a una piattaforma di gestione altamente performante, di alta affidabilità e elevate prestazioni. Le caratteristiche tecniche e prestazionali del servizio reso dalla piattaforma sono funzione dei seguenti parametri operativi:

- Dimensione media dei messaggi (KB inviati o ricevuti);
- Numero di messaggi nell'unità di tempo (msg/sec)
- Numero di code;
- Architettura di affidabilità della soluzione.

In relazione alla combinazione di questi elementi (i primi due, dimensionali) il servizio è erogato in tre fasce (Tier).

Servizio AQ	Tier1	Tier2	Tier3
Piattaforma	Dimensione msg <=5 KB	Dimensione msg >5KB e =>20 KB	Dimensione msg >20 KB e <=200 KB
Queue	N.ro msg/min <= 2000 msg/sec	N.ro msg/sec <= 1500	N.ro msg/sec <= 350
Management			

Il throughput dell'appliance dipende fortemente dalla dimensione media del messaggio trattato per cui il numero di messaggi trattati nell'unità di tempo da un apparato diminuisce con l'aumento della dimensione media.

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 55 di 95

Nel dimensionamento dell'apparato quindi il valore da prendere come riferimento è la dimensione media dei messaggi che la componente applicativa invia o riceve.

Nel caso quindi che a parità di dimensione media del messaggio l'applicazione richieda un throughput maggiore vanno incrementati il numero di Tier necessari.

Disaster recovery Servizi ICT e dati

Le caratteristiche del servizio sono le medesime già illustrate per la componente SERVER e STORAGE per le banche dati.

Continuità Operativa – Disaster recovery Servizi ICT

Ad oggi non esiste l'infrastruttura di DR per gli Appliance-A; nell'ambito della Conduzione centrale Appliance-T ed Appliance-Q si inquadra il servizio Disaster Recovery della componente di business che ha come fine quello di permettere agli utenti la ripresa delle attività produttive in caso di disastro che colpisca il sito primario che si trova a Roma. Il servizio ha come presupposto la disponibilità della copia dei dati effettuata con il servizio di Disaster Recovery delle banche dati (storage), che se non specificamente rifiutato da parte dell'Amministrazione, è attivato di norma, a garanzia della costante disponibilità del dato. La verifica della correttezza delle azioni di predisposizione viene effettuata ogni 6 mesi con la ripartenza sul sito di recovery delle applicazioni di backup. Con cadenza annuale viene effettuata una prova di ripartenza con la partecipazione di un selezionato numero di utenti finali.

Continuità Operativa – Disaster recovery Storage

Il servizio mette a disposizione una copia dei dati considerati vitali presso un sito alternativo a quello primario. Questa

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 56 di 95

copia in caso di disastro è la base per poter ripristinare nel sito alternativo le attività dell'Amministrazione. Per disporre di questa copia sempre aggiornata, la copia stessa viene effettuata on-line in modalità asincrona con quella esistente nel sito primario. La verifica della correttezza della copia effettuata avviene ogni 6 mesi con l'esecuzione di specifiche procedure di ripartenza delle applicazioni su basi dati scelte a campione; per l'esecuzione di queste prove senza interrompere l'attività di copia on-line, si usa una seconda copia di dati eseguita "Point in Time". Lo Storage Disaster Recovery riguarda la parte dati e banche dati memorizzata su disco in SAN e se non specificamente rifiutato da parte dell'Amministrazione, è attivato di norma, a garanzia della costante disponibilità del dato.

L'orario del servizio è H24

5.2.3.1 Livelli di Servizio

In caso in cui l'Amministrazione richieda un orario H24 senza possibilità di prevedere fermi concordati, ne verrà valutata la fattibilità e attivato un apposito servizio PLATINUM remunerato sulla base delle risorse aggiuntive necessarie.

Servizio	Appliance		
	Soglia	Penale	Orario di osservazione
Livelli di Servizio			
Disponibilità del servizio erogato dall'infrastruttura sottostante (GB)	vedi tabella 5.2 "Gestione e conduzione infrastruttura"		H24
Disponibilità del	98%	€ 50,00 per ogni	

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 57 di 95

Servizio		Appliance	
Livelli di Servizio	Soglia	Penale	Orario di osservazione
servizio di DR (solo per GBT)		decimo di punto percentuale di diminuzione rispetto al valore prefissato (in caso di più Amministrazioni aderenti alla medesima piattaforma, la penale si intende relativa ad ogni Amministrazione)	
Esito positivo della prova di verifica periodica in data concordata(solo per GBT) (nel rispetto del calendario concordato)	10 giorni di ritardo rispetto alla data concordata	€ 250,00 per ogni giorno di ritardo dall'undicesimo al trentesimo; € 500,00 per ogni giorno di ritardo dal trentunesimo al sessantesimo; € 750,00 per ogni giorno di ritardo successivo al sessantesimo	

5.2.4 Piattaforma Big Data

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 58 di 95

Il servizio offre l'accesso a una piattaforma di Big Data altamente performante, di alta affidabilità e elevate prestazioni. Le Piattaforme “Big Data” sono quelle deputate alla raccolta di dati estesa in termini di volume, velocità e varietà tali da richiedere strumenti non convenzionali per estrapolare, gestire e processare informazioni entro un tempo ragionevole.

Il Servizio prevede l'utilizzo di un Cluster Hadoop, infrastruttura distribuita open source sviluppata sotto l'egida della Apache Software Foundation per l'elaborazione di Big Data, ovvero un cluster di macchine su cui è installata una distribuzione Hadoop (Cloudera, Hortonworks).

In tale servizio rientrano anche i servizi di streaming distribuito per operazioni di publish & subscribe (es. prodotto Apache Kafka).

Tecnicamente la piattaforma si basa su una collezione di server fisici o virtuali in grado di operare in alta affidabilità e fornendo capacità computazionale in grado di scalare al crescere dei dati e delle operazioni da eseguire su di essi consentendo elaborazioni di tipo batch, puntuali e real time.

Il servizio non prevede un DR né dei dati né del servizio ICT che li utilizza.

Le piattaforme Big Data hanno insito nell'infrastruttura una salvaguardia del dato, per cui non necessitano (e la mole dei dati, lo renderebbe di fatto poco praticabile) di backup su nastro.

A salvaguardia dei dati in caso di disastro nel sito principale si prevedrà, comunque un servizio di backup con replica

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 59 di 95
 remota su sito di DR dei dati, senza ripartenza del servizio
 ICT.

In caso di richiesta esplicita, Sogei, potrà attivare un servizio di DR del servizio ICT anche in ambito Big Data, con i limiti e le possibilità delle tecnologie adottate.

L'orario del servizio è H24.

5.2.4.1 Livelli di Servizio

Servizio		Piattaforma bigdata	
Livelli di Servizio	Soglia	Penale	Orario di osservazione
Disponibilità del servizio erogato dall'infrastruttura sottostante (GB)	vedi tabella 5.2 “Gestione e conduzione infrastruttura”		H24

Di seguito alcune precisazioni:

Il DR non è fornito di default, in alternativa può essere effettuato, su richiesta, un servizio di backup su sistemi VLT, con replica su sito di Recovery.

5.2.5 Piattaforma NOSQL

Le Piattaforme “NOSQL”, in analogia a quelle BIG DATA sono quelle deputate alla raccolta di dati che utilizzano una varietà di modelli di dati per accedere e gestirli. Questi tipi di Database sono ottimizzati specificatamente per applicazioni che necessitano di grandi volumi di dati, latenza bassa e modelli di dati flessibili, ottenuti snellendo alcuni dei criteri di coerenza tipici dei database relazionali.

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 60 di 95

Le piattaforme per “NOSQL” sono costituite da un sistema di calcolo distribuito realizzato da una collezione di computer indipendenti che, dal punto di vista dell’utente, risultano essere un unico sistema coerente. Un esempio di database NOSQL è MongoDB, db che si allontana dalla struttura tradizionale basata su tabelle dei database relazionali in favore di documenti in stile JSON con schema.

L’offerta prevede l’utilizzo di un Cluster ossia un cluster di macchine su cui è installata un DB di tipo NOSQL (es. MongoDB, Couchbase etc).

Nel driver ‘NOSQL’ rientrano anche le piattaforme che erogano servizi in memory distribuiti che utilizzano gli stessi principi in termini di infrastruttura: Sistemi Distribuiti con enorme quantità di ram e capacità di calcolo, che di fatto rispondono alla stessa tipologia di architettura (normalmente massiva nelle quantità di dischi, utilizzo di server fisici/virtuali, dato replicato tra più nodi).

Il servizio offre l’accesso a una piattaforma altamente performante, di alta affidabilità ed elevate prestazioni. Tecnicamente la piattaforma si basa su una collezione di server fisici o virtuali in grado di operare in alta affidabilità e fornendo capacità computazionale in grado di scalare al crescere dei dati e delle operazioni da eseguire su di essi consentendo elaborazioni di tipo batch, puntuali e real time.

Il servizio, non prevede, considerando la tipologia e l’onerosità del servizio, un DR né dei dati né del servizio di business che li utilizza.

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 61 di 95

La piattaforma ha infatti nell’infrastruttura una salvaguardia del dato, per cui non necessitano (e la mole dei dati, lo renderebbe di fatto poco praticabile) di backup su nastro.

A salvaguardia dei dati in caso di disastro nel Sito Principale si prevedrà, comunque un servizio di backup con replica remota su sito di DR dei dati, senza ripartenza del servizio di business.

In caso di richiesta esplicita, Sogei, potrà attivare un servizio di DR del servizio ICT anche in ambito “NOSQL”, con i limiti e le possibilità delle tecnologie adottate.

L’orario del servizio è H24.

5.2.5.1 Livelli di Servizio

Servizio	Piattaforma NOSQL			
	Livelli di Servizio	Soglia	Penale	Orario di osservazione
Disponibilità del servizio erogato dall'infrastruttura sottostante (GB)		vedi tabella 5.2 “Gestione e conduzione infrastruttura”		H24

Di seguito alcune precisazioni:

Analogamente all’ambito hadoop, anche i sistemi NOSQL offrono una salvaguardia del dato attraverso la replica dello stesso su copie distribuite, di conseguenza, considerando anche le moli dei dati, il DR non è fornito di default. Su richiesta può essere realizzato e per la tipologia di sistema, il costo è il medesimo di quello di produzione.

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 62 di 95

In alternativa può essere effettuato, su richiesta, un servizio di backup su sistemi VLT, con replica su sito di Recovery. Il costo per tale servizio è quello determinato in ambito Storage per il backup.

5.3 **SERVIZI DI COLLABORATION E COMMUNICATION**

I servizi di collaboration and communication services, descritti di seguito, forniscono una serie completa di strumenti finalizzati a garantire l'efficienza e l'operatività dell'utente e a favorire la comunicazione e lo scambio delle informazioni in un contesto affidabile e sicuro.

5.3.1 ***Servizi navigation Internet***

Il servizio comprende la gestione della navigazione sulla rete Internet con protocollo standard http e protocollo sicuro https utilizzando un proxy, cioè un sistema informatico che funge da intermediario per le richieste da parte dei client alla ricerca di risorse web disaccoppiando in tal modo l'accesso alle risorse dalla postazione dell'utente.

Il servizio viene offerto secondo i seguenti profili di utenza:

- Utente Base: tale utenza può accedere con regole di filtraggio comuni basate su white list secondo le indicazioni dell'Amministrazione (max 300 regole di filtraggio).
- Utente Esteso: tale utenza può accedere con regole dinamiche di filtraggio dei contenuti personalizzate per garantire che l'utilizzo di Internet sia conforme ad una politica di utilizzo definita dall'Amministrazione; viene inoltre effettuata una scansione in tempo reale dei contenuti in entrata per garantirne la sicurezza contro virus e altro malware.

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 63 di 95

- Utente Avanzato: tale utenza funzionalmente è simile alla categoria precedente “Utente Esteso” ma è caratterizzata dall’utilizzo “aziendale” di soluzioni Cloud per servizi di tipo Intranet. Tale servizio deve essere dichiarato dall’Amministrazione. Il servizio è attivabile solo se tutti gli utenti di una Amministrazione aderiscono al servizio.
- Sicurezza PLUS: su richiesta è possibile attivare anche un servizio avanzato di sicurezza che prevede un controllo approfondito sulla navigazione degli utenti al fine di evidenziare online eventuale codice malevolo all’interno della navigazione web dell’utenza (sandbox, minacce zero-day).

Orario del servizio H24.

5.3.1.1 Livelli di Servizio

Servizio		Servizio navigation Internet	
Livelli di Servizio	Soglia	Penale	Orario di osservazione
Disponibilità del servizio	Indisponibilità del servizio nel quadri mestre < 1h	€ 516,00 per ogni ora di mancata disponibilità del servizio	H24

5.3.2 Virtual Private Network utente

Con il termine Virtual Private Network Utente si intende la realizzazione di connessioni private tra una singola postazione e un terminatore che consente l’accesso a risorse private tipicamente servizi erogati dall’infrastruttura PSN attraverso una rete pubblica Internet.

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 64 di 95

La soluzione di Virtual Private Network utente adottata in Sogei è basata sullo standard TLS.

Gli utenti abilitati accedono ad un portale dal quale sarà consentito l'accesso all'infrastruttura privata previa autenticazione a 2 fattori di cui uno con token OTP.

L'accesso alle risorse interne seguirà le politiche di sicurezza definite per l'ente o per il gruppo di utenti previa una fase di verifica di fattibilità tecnica per evitare che minacce software siano introdotte all'interno del perimetro aziendale.

Il servizio prevede accesso con utente e password con Token acquisite dall'Amministrazione secondo indicazioni fornite da Sogei e registrate sui sistemi (qualora il Token venga erogato via SMS l'invio SMS è a carico dell'Amministrazione).

Orario del servizio: H24

5.3.2.1 Livelli di Servizio

Virtual Private Network utente			
Livelli di Servizio	Soglia	Penale	Orario di osservazione
Disponibilità del servizio	99,0%	€ 1.250,00 per ogni decimo di punto percentuale di diminuzione rispetto al valore prefissato	H24

5.3.3 Servizi di Digital WorkSpace

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 65 di 95

La soluzione di Digital WorkSpace è in grado di distribuire in modo rapido e sicuro applicazioni e desktop agli utenti. La piattaforma consente di erogare un ambiente di lavoro di ufficio privo di qualsiasi tipo di vincolo fisico e, di conseguenza, promuovere iniziative di Telelavoro e di Smart Working. La piattaforma di Digital WorkSpace offre una reale alternativa al Desktop Computing ed eroga le seguenti quattro tipologie di servizi per ognuna delle quali sono previsti due pacchetti di funzionalità: “Standard”, ovvero le funzionalità minime del singolo servizio, “Plus” ovvero funzionalità aggiuntive a quanto previsto nel pacchetto “Standard”:

- **Virtual Desktop pooled:** servizio di desktop virtuali

Funzionalità Standard:

- Distribuzione Software,
- Patching,
- Compliance,
- Antivirus.

Funzionalità Plus:

- Quota disco Dati utente aggiuntiva (fornita con servizio storage),
- Accesso da rete pubblica,
- Reporting accesso utenti,
- Configurazioni personalizzate.

- **Bundle di vApp:** servizio di Virtual APP in bundle che prevede la configurazione di alcuni server (Session Host) per la distribuzione delle applicazioni sia ai desktop

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 66 di 95
tradizionali che virtuali. L’utente può utilizzare le vAPP attraverso una sessione remota sui Session Host caratterizzata da un “look and feel” identico all’applicativo erogato. Il Bundle prevede l’erogazione di un massimo di n° 10 vAPP ed uno spazio dati per il profilo utente pari a 25 GB. Le funzionalità aggiuntive previste nel pacchetto “Plus” possono essere selezionate singolarmente.

Funzionalità Standard:

- Streaming delle vAPP.

Funzionalità Plus:

- Reporting accesso utenti,
 - Accesso da rete pubblica,
 - Quota disco dati aggiuntiva (fornita con servizio storage).
- **Singola vApp:** servizio per una singola Virtual APP; il servizio è identico in termini di funzionalità al servizio Bundle vAPP e prevede l’erogazione di un massimo di n° 1 vAPP ed uno spazio dati per il profilo utenti pari a 500 MB. Le funzionalità aggiuntive previste nel pacchetto “Plus” possono essere selezionate singolarmente.

Funzionalità Standard:

- Streaming della vAPP.

Funzionalità Plus:

- Reporting accesso utenti,
- Accesso da rete pubblica,
- vApp personalizzate,

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 67 di 95

- Quota disco dati aggiuntiva (fornita con servizio storage).

- **Singola vAPP “capped”:** servizio del tutto analogo a quello non ‘bloccato’ con le seguenti specificazioni:

Funzionalità Standard:

È stato calcolato con una concorrenza di utenze molto bassa e pari al 40% al fine di coprire esigenze specifiche di rotazione del personale, piuttosto che di Smartworking.

Essendo l'AC bloccata da questo basso livello di concorrenza, decisamente inferiore a quello osservato usualmente nell'uso del servizio, per garantire i livelli di servizio del servizio stesso e la qualità dello stesso, raggiunta la quota del 40% degli utenti definiti (il driver è sempre computato sul numero di utenti definiti), l'utente successivo sarà respinto dall'infrastruttura;

Essendo poi un driver ad hoc, considerando la pesante incidenza sull'infrastruttura data dalla concorrenza, ogni anno, in sede di Piano Operativo dovrà essere definito il massimo numero di utenti aderenti a questo driver. Eventuali necessità ulteriori per driver diversi, saranno aggiuntive rispetto al medesimo, ossia non si potranno azzerare/diminuire gli utenti qui definiti per sostituirli con utenti di tipologia diversa, se non previa verifica con Sogei.

Orario di Servizio: H24

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 68 di 95

5.3.3.1 Livelli di Servizio

Servizio	Digital workspace		
	Livelli di Servizio	Soglia	Penale
Disponibilità Portale Digital Workspace	99,0%	€250,00 per ogni decimo di punto percentuale di diminuzione rispetto al valore prefissato	H24
Uptime Infrastruttura Piattaforma Virtuale	99,0%	€500,00 per ogni decimo di punto percentuale di diminuzione rispetto al valore prefissato	

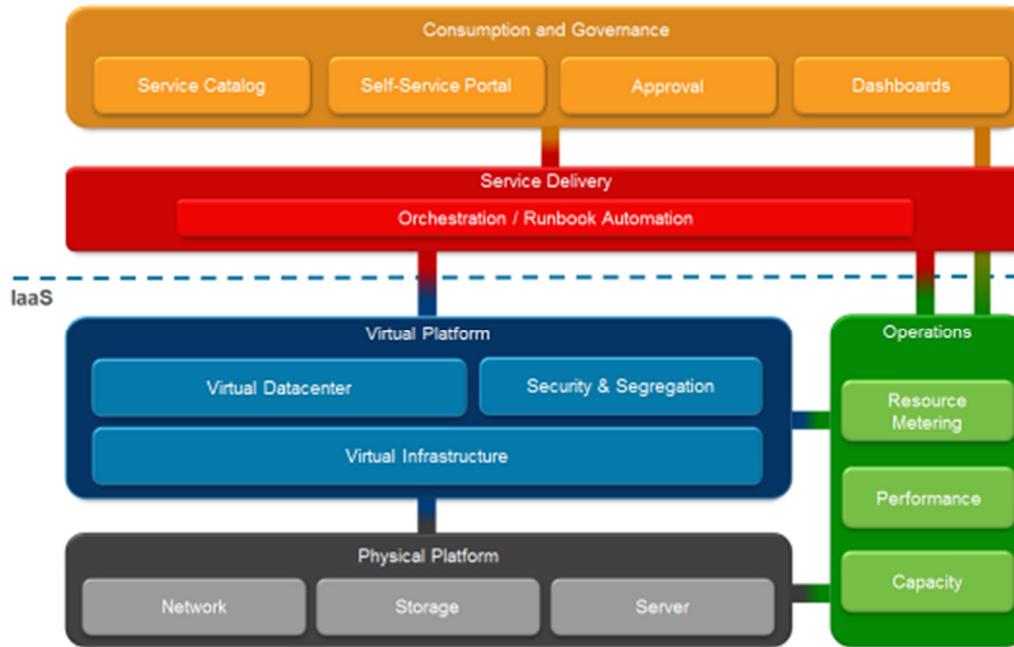
5.4 SERVIZI DI TIPOLOGIA CLOUD**5.4.1 Piattaforma IaaS**

Sogei mette a disposizione una Piattaforma Cloud per l'offerta di un servizio di Infrastructure as a Service (IaaS) On-Demand in cui ogni utente abilitato al servizio può crearsi in autonomia i propri Cloud Server Virtuali, di seguito CSV, scegliendoli da un catalogo. La Piattaforma interagisce con una infrastruttura virtuale sfruttandone tutte le potenzialità per la gestione dei CSV, dello Storage e del Networking.

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 69 di 95

Dal punto di vista logico, la soluzione è rappresentata dal seguente schema:



In linea generale:

- gli utenti, compatibilmente con il ruolo loro assegnato, hanno accesso al blocco logico superiore (“Consumption and Governance”), potendo quindi inserire richieste di servizi esposti su un catalogo, operare in modalità self-service sulle istanze CSV, accedere a dashboard che riportano informazioni sulla configurazione delle proprie istanze CSV e sulle risorse consumate;
- il team IT di Sogei ha invece accesso sia al blocco logico superiore che a quelli sottostanti per predisporre, gestire e manutenere il servizio di Cloud Computing di tipo IaaS.

La Piattaforma Cloud Sogei include tutti gli elementi per abilitare un Cloud Environment:

- portale di Self Service e Service Catalog Cloud - fornisce agli utenti del Tenant la possibilità di richiedere il deploy di servizi e di tracciarne il ciclo di vita;

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 70 di 95

- service Delivery Automation - automatizza il provisioning dei servizi richiesti.

La disponibilità delle istanze CSV pubblicate (Template pre-configurati da Sogei) può variare in base a nuove esigenze o secondo le caratteristiche dell'Hypervisor.

Il service catalog cloud, da cui l'utente può configurare il proprio sistema, offre la possibilità di richiedere dei CSV preconfigurati con i seguenti sistemi operativi:

- Microsoft Windows Server;
- Red Hat Enterprise Linux;
- Ubuntu Linux.

La configurazione standard del CSV prevede:

- una quota disco da 200GB, di cui 100GB preallocati sul CSV esposto nel catalogo dei servizi ed altri 100GB da richiedere in fase di prima allocazione o in alternativa come action di post-deploy del CSV;
- il backup dell'immagine virtuale di sistema in configurazione standard;
- una replica locale dell'immagine virtuale (Alta Affidabilità Estesa);
- una replica dell'immagine virtuale sul sito di Disaster.

In fase di richiesta l'utente, oltre alla configurazione del CSV in termini di vCPU e vRam, può specificare il network di destinazione ed eventuali dischi aggiuntivi.

Completata la creazione del CSV, l'utente potrà richiederne la modifica della sua configurazione in termini di risorse computazionali e spazio disco.

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 71 di 95

È possibile richiedere uno spazio disco aggiuntivo rispetto alle quote previste contrattualmente e/o previste a catalogo, richiedibile sia in fase di prima allocazione per le varie tipologie di CSV esposte sia in fase successiva come modifica al CSV.

Tramite opzioni aggiuntive è prevista, inoltre, la possibilità di richiedere il Servizio di Backup e selezionarne la relativa tipologia.

Il servizio di backup è opzionabile su più Tipologie, ognuna delle quali presenta diversi parametri di frequenza, retention e numero di restore possibili. Per default il singolo CSV è associato al livello Bronze (backup CSV) e a nessun tipo di backup per quanto riguarda il Backup Autonomo.

A richiesta possono essere effettuati dei WAPT su:

- Web Application
- Web Service

dell'Amministrazione, anche ai fini dell'esposizione del servizio su internet.

Il servizio di Web Application Penetration Test consente all'Amministrazione di eseguire un'analisi di sicurezza delle applicazioni Web individuando le vulnerabilità presenti ed esaminando l'esposizione al rischio di attacchi informatici nei confronti dei servizi e dell'infrastruttura.

L'attività è eseguita da personale specializzato secondo le due principali metodologie internazionali in materia di test di sicurezza informatica: OWASP e OSSTMM.

Le aree di analisi esaminate nel corso del test comprendono almeno le seguenti:

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 72 di 95

- Logica dell'applicazione: identificazione delle problematiche legate alla logica dell'applicazione;
- Autenticazione: analisi delle procedure di autenticazione per verificarne la robustezza;
- Autorizzazione: verifica della gestione dei ruoli delle utenze applicative e identificazione di eventuali problematiche che possano portare ad una privilege escalation oppure all'accesso a dati e/o risorse di competenza di altri utenti;
- Sicurezza della comunicazione: analisi del canale di comunicazione utilizzato;
- Algoritmi di cifratura: verifica della robustezza degli algoritmi di cifratura utilizzati;
- Validazione dei dati: analisi di tutti i campi di input presenti mediante diversi tipologie di payload allo scopo di verificarne la sicurezza e scongiurare l'eventuale presenza di vulnerabilità di tipo injection;
- Configurazione e deployment: analisi della configurazione del server, delle eventuali risorse di default presenti e degli header http;
- Gestione Errori: verifica della corretta gestione degli errori con eventuale segnalazione;
- Privacy: analisi del flusso applicativo al fine di individuare eventuali esposizioni di dati identificativi, personali o sensibili dell'utente;
- Gestione della sessione;
- Dipendenze di terze parti: analisi delle componenti software utilizzate dall'applicazione individuate nel corso

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 73 di 95
del test e segnalazione della presenza di eventuali vulnerabilità note.

L’attività di test prevede:

- Identificazione delle vulnerabilità per via manuale o con il supporto di strumenti automatici;
- Raccolta delle evidenze necessarie per consentire a terzi di ripercorrere i passaggi necessari alla sua individuazione;
- Analisi delle vulnerabilità e assegnazione di un livello di severità (ALTA, MEDIA, BASSA, INFORMATIVA) sulla base di metriche standard internazionali quali il CVSSv2;
- Indirizzamento delle attività per il rientro delle vulnerabilità identificate indicando per ciascuna di esse le best practice da adottare;
- Produzione di reportistica di dettaglio (technical report) sulle analisi eseguite con le evidenze raccolte per ciascuna delle vulnerabilità identificate.

Il servizio viene erogato ai clienti su richiesta previa accettazione di un incarico ufficiale denominato Rules of Engagement (RoE) mediante il quale saranno fornite tutte le informazioni necessarie allo svolgimento dell’attività. In fase di avvio, previa raggiungibilità degli ambienti target, sarà fornita una stima dell’effort necessario sulla base di una valutazione dimensionale.

Il servizio prevede, infatti, tre diversi profili di erogazione, a seconda della tipologia di applicazione sottoposta al test, come specificato nella seguente tabella

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 74 di 95

PROFILO	TIPOLOGIA DI APPLICAZIONE
SMALL	Applicazioni web dal contenuto informativo (siti web statici)
MEDIUM	Applicazioni web dinamiche, con uno o più profili di utenza e costituite da più funzionalità/form di inserimento dati.
BIG	Applicazioni web dinamiche e complesse con un numero di funzionalità/form maggiore di 20 (portali web).

Sono inoltre inclusi i seguenti servizi:

- *Security Operation Center Centrale*: il servizio sarà assicurato a protezione dell’infrastruttura cloud nei termini e nei modi già descritti nell’ambito SERVER.
- *Continuità Operativa*: Disaster recovery Servizi ICT: il servizio sarà assicurato a protezione dell’infrastruttura cloud nei termini e nei modi, già descritti nell’ambito SERVER ma senza assicurare la ripartenza dei servizi, dipendente dalle configurazioni delle VM e dei software in esse installati (responsabilità dell’Amministrazione). Sogei assicurerà la ripartenza delle singole VM nella configurazione del sito principale. Non assicurerà eventuali configurazioni, comprese quelle di rete, spesso necessarie per garantire la continuità operativa del business.

Sulla base degli indicatori di seguito descritti (Disponibilità e Accessibilità), saranno messi a disposizione i seguenti strumenti di reporting e visualizzazione:

- un report inviato via e-mail, contenente l’andamento dei due indicatori nelle ultime 24/48 ore, a partire dalla mezzanotte passata;

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 75 di 95

- un report a richiesta che fornisce l'andamento dei due indicatori dal giorno prima fino all'ora precedente.

Disponibilità dell'Infrastruttura Cloud: viene controllato lo stato di salute delle Virtual Machine in termini di vCpu, memoria, connettività e file system, ecc. I dati di monitoraggio a cadenza regolare (ogni 5 minuti) vengono trasferiti sul Datawarehouse della piattaforma centrale Sogei.

Accessibilità alla Infrastruttura Cloud: il controllo viene effettuato mediante accesso ogni 5 minuti ad una pagina https esposta su internet dalle Virtual Machine di servizio per verificare il corretto funzionamento di tutte le componenti dell'infrastruttura Cloud: internet, sicurezza perimetrale, connettività, piattaforma cloud. Modalità di reporting ed accesso alle informazioni di controllo.

Orario di Servizio: H24

5.4.1.1 Livelli di Servizio

Servizio	IaaS			
	Livelli di Servizio	Soglia	Penale	Orario di osservazione
Disponibilità online della piattaforma	99,8%	La penale è pari al 2‰ (due per mille) del corrispettivo quadrimestrale per ogni scostamento di 0,1% (zero virgola uno per cento) rispetto al valore prefissato	H24	

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 76 di 95

SERVIZI DI BASE DIVERSI DA QUELLI DI CONDUZIONE

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 77 di 95

6. PIATTAFORME ASP

Si tratta di servizi ICT offerti da Sogei ed erogati su proprie Piattaforme dotate di strumenti necessari alla loro erogazione, come servizi per la gestione documentale, soluzioni e-learning e servizi di sicurezza, offerti in modalità ASP (Application Service Provider). Tali servizi, erogati attraverso infrastrutture remote condivise da più clienti e ubicate presso il Data Center Sogei, sono proposti attraverso un modello di pricing a canone basato sugli effettivi consumi.

6.1 *SERVIZI DI SICUREZZA*

6.1.1 *Piattaforme di sicurezza IAM (Identity Access Management)*

Il servizio prevede l’identificazione, l’autenticazione e l’autorizzazione degli utenti interni ed esterni mediante sistemi di directory, di controllo delle autorizzazioni, PKI (Public Key Infrastructure) e sistemi per la gestione integrata delle componenti al fine di consentire all’Amministrazione una gestione autonoma delle autorizzazioni ai propri servizi. Il Disaster Recovery è incluso in modalità “full” per l’ambito CAST e Certification Authority e in modalità “base” (sole funzioni in lettura) per l’ambito CAU.

Orario di Servizio: H24

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 78 di 95

6.1.1.1 Livelli di Servizio

Servizio	Piattaforme di sicurezza – identity access management			
	Livelli di Servizio	Soglia	Penale	Orario di osservazione
Disponibilità del servizio	99,0%	€ 1.250,00 per ogni decimo di punto percentuale di diminuzione rispetto al valore prefissato	H24	

6.1.2 Piattaforme di sicurezza SOC (Security Operation Center)

Il SOC Sogei ha una struttura logica centralizzata con i seguenti obiettivi:

- raccogliere e analizzare gli eventi di sicurezza rilevati dalle varie componenti infrastrutturali, le altre tecnologie (hardware e software) di sicurezza presenti anche negli asset periferici dell’Amministrazione che ha sottoscritto il servizio;
- gestire e monitorare tutti i Sistemi di Sicurezza, al fine di identificare, contenere e bloccare eventuali “Minacce Informatiche” rilevate;
- contribuire alla gestione e all’analisi degli incidenti informatici in collaborazione con la struttura del CERT Sogei ed i riferimenti dell’Amministrazione;
- supportare le attività di Governo della Sicurezza verso l’Amministrazione.

Il servizio SOC è svolto principalmente attraverso la

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 79 di 95

centralizzazione di tutti i log di evento provenienti dai dispositivi infrastrutturali di sicurezza.

I suddetti log sono analizzati e correlati in tempo reale, attraverso tecnologia di tipo SIEM (Security Incident and Event Management), per dare evidenza degli eventi più significativi ai fini della sicurezza e funzionali alla gestione degli incidenti informatici.

I servizi del SOC sono differenziati tra servizi endpoint e dispositivi. Per dispositivi si intendono apparati di sicurezza fisici o virtuali gestiti.

Il servizio include le seguenti attività:

- Monitoraggio delle sorgenti e notifica di vulnerabilità e minacce, con suggerimenti per la loro mitigazione;
- Definizione, validazione e verifica delle configurazioni tecniche dei sistemi di sicurezza, aggiornamento della documentazione inerente l'infrastruttura di sicurezza IT;
- Configurazione degli apparati di sicurezza in base alle politiche stabilite e attività di manutenzione sugli stessi, compreso il Patch Management;
- Definizione, autorizzazione, implementazione, modifica (change) ed “enforcement”, delle regole di sicurezza da implementare; valutazione del rischio associato a tali attività, laddove acquisiti i servizi corrispondenti;
- Monitoraggio in tempo reale dei sistemi di sicurezza (Real Time Security Monitoring), al fine di rilevare eventuali incidenti, attività sospette e violazioni delle politiche di sicurezza, anomalie e/o disservizi sull'infrastruttura di sicurezza;

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 80 di 95

- Validazione dei sistemi attraverso scansioni periodiche (o su richiesta), per rilevare ed analizzare vulnerabilità applicative e di sistema operativo con notifica alle strutture responsabili del Patch Management, evidenziando eventuali attività di adeguamento non effettuate/posticipate (scansioni successive) laddove acquisiti i servizi corrispondenti;
- Produzione di reportistica di livello tecnico ed executive;
- Gestione degli eventi significativi rilevati (Incident Response, Incident Containment e Incident Recovery) coordinata anche attraverso la struttura del CERT Sogei con l’Amministrazione, di risposta e contenimento degli impatti derivanti dagli incidenti identificati e successivo ripristino delle normali attività operative.
- Identificazione di possibili incidenti (Incident Identification, Classification e Notification) tramite l’analisi delle informazioni raccolte e correlate dai sistemi del SOC, loro classificazione e notifica anche attraverso la struttura del CERT Sogei nel caso di incidenti con caratteristiche significative e rilevanti;
- Attività di supporto specialistico (Troubleshooting, Architectural, LabTest) per l’analisi delle anomalie applicative sui segmenti di rete dove insistono dispositivi di sicurezza perimetrale.

Orario di Servizio: H24

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 81 di 95

6.1.2.1 Livelli di Servizio

Servizio	Piattaforme di sicurezza – SOC		
Livelli di Servizio	Soglia	Penale	Orario di osservazione
Tempo di presa in carico della segnalazione (*)	<= 1 ora nel 95% dei casi	€ 0,5 per ogni richiesta che non rispetta il LdS	8.00-20.00 lun- ven 8.00-14.00 sabato
	<= 4 ore nel 100% dei casi	€ 0,7 per ogni richiesta che non rispetta il LdS	
Disponibilità del servizio SIEM	99,0%	€ 1.250,00 per ogni decimo di punto percentuale di diminuzione rispetto al valore prefissato	H24

(*) Tempo di presa in carico di segnalazioni provenienti da segnalazioni degli utenti raccolte da Sogei.

7. SERVIZIO SITO/PORTALE WEB E COMPONENTI ACCESSORI

Il Servizio si riferisce alle attività di sviluppo e conduzione (manutenzione) di siti/portali Internet o Intranet per la condivisione di informazioni e/o servizi corredati delle necessarie personalizzazioni e degli eventuali “servizi accessori” modulari laddove richiesti. In particolare:

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 82 di 95

- Sviluppo sito: si tratta di uno sviluppo a corpo che prevede l'attività di analisi, progettazione, sviluppo, test e messa in esercizio di un nuovo sito/portale composto dalla home page e dai template delle pagine standard (es. pagina news, pagina di approfondimento etc.), realizzato su una delle piattaforme standard Sogei, la cui complessità è definita Extra, Alta, Media e Bassa in relazione alla quantificazione dei parametri di seguiti definiti. È ricompresa nel primo anno l'attività di manutenzione applicativa.
- Conduzione sito: si tratta di un servizio a canone che comprende la gestione dell'infrastruttura, le attività di manutenzione ordinaria del sito/portale, la gestione delle versioni di software di base, i piccoli interventi di manutenzione evolutiva necessari a garantire l'attualità della struttura e dei contenuti. Sono inoltre ricomprese le attività di web analytics.

I Servizi accessori sono:

- Redazione ordinaria: si tratta di un servizio a canone che comprende l'attività di pubblicazione, modifica e movimentazione di contenuti informativi e file, compreso l'aggiornamento delle pagine del sito, effettuata su precisa indicazione del committente sia relativamente al contenuto informativo che al posizionamento dello stesso all'interno del sito. Le attività sono eseguite secondo le modalità operative concordate. Questo servizio viene erogato dal lunedì al venerdì, escluso festivi, in orario 8-18.
- Migrazione da altro sito: si tratta di un servizio a corpo che prevede l'attività di trasferimento di contenuti

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 83 di 95

editoriali e relativi allegati, dalla piattaforma sorgente alla piattaforma target individuata da Sogei. In dipendenza della specificità della piattaforma sorgente, è facoltà di Sogei individuare meccanismi automatici di trasferimento ovvero procedere all'inserimento manuale dei contenuti.

- Ulteriori servizi opzionali come di seguito dettagliato:

- Pagine con servizi applicativi: si tratta di uno sviluppo a corpo che comprende l'attività di implementazione di pagine web per l'inserimento di dati, successiva chiamata a un servizio esterno e presentazione dei dati di risposta opportunamente formattati (per esempio: form di accesso alla rubrica, pagina di ricerca, survey, form di prenotazione appuntamenti, ecc.).
- Canali Social: si tratta di un servizio a canone che comprende l'attività relativa alla gestione (apertura, configurazione e monitoraggio) dei canali social richiesti dall'organizzazione anche attraverso piattaforme di social media management. Nell'attività di monitoraggio è inclusa la fase di assessment iniziale, l'individuazione dei keyword di ricerca, l'individuazione dei topic di analisi, pubblicazione di notizie (post), la moderazione dei commenti, la sentiment analysis e la produzione di reportistica ad hoc. Questo servizio viene erogato dal lunedì al venerdì, escluso festivi, in orario 8-18.
- Redazione speciale: si tratta di un servizio a canone

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 84 di 95

che comprende l'attività di redazione come definita precedentemente ed erogata, su specifica richiesta del committente, dal lunedì al venerdì, in orario 18-22 e nei giorni festivi in orario 8-14.

- Sezione “area trasparenza” richiesta da ANAC: si tratta di uno sviluppo a corpo che comprende l'attività di predisposizione e aggiornamento periodico della sezione “trasparenza” in conformità con quanto stabilito dall'Autorità Nazionale AntiCorruzione. E’ inclusa l'attività di verifica periodica di rispondenza e conformità della pagina ai requisiti dell'ANAC.

La complessità di un sito è definita Extra, Alta, Media e Bassa in relazione alla quantificazione dei seguenti parametri:

- Numero di pagine;
- Platea di utenti visitatori;
- N. visite medie;
- N. linee redazionali.

Servizio	Bassa	Media	Alta	Extra (*)
Sito/Portale informativo	Pagine < di 100 Platea < 1.000 visitatori unici/gg visite medie < 10.000/gg linee redazionali (**) =1	Pagine < di 1.000 Platea < 10.000 visitatori unici/gg visite medie < 30000/gg linee redazionali < 5	Pagine < di 5.000 Platea < 50.000 visitatori unici/gg visite medie < 70000/gg linee redazionali < 10	Pagine > di 5.000 Platea > 50.000 visitatori unici/gg visite medie > 70000/gg linee redazionali > 10

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 85 di 95

--	--	--	--	--

(*) la classe di complessità “Extra” è prevista anche per quei siti/portali per i quali è stato necessario predisporre un’infrastruttura ad hoc per la particolare criticità del servizio collegato.

(**) la singola linea redazionale rappresenta il gruppo di redattori che opera continuativamente su una determinata sezione del sito ovvero rappresenta l’attività eseguita dai gruppi redazionali distribuiti sul territorio (redazioni periferiche per Amministrazioni con sedi delocalizzate). I servizi accessori opzionali presentano invece un costo puntuale mediato.

Orario di Servizio: H24

7.1 *LIVELLI DI SERVIZIO*

Allo sviluppo dei siti si applicano i Livelli di servizio del servizio “Personalizzazione del software di mercato”

Servizio	Servizio sito/portale web e componenti accessori			
	Livelli di Servizio	Soglia	Penale	Orario di osservazione
Disponibilità del servizio		99,50%	€ 1.250,00 per ogni decimo di punto percentuale di diminuzione rispetto al valore prefissato	7.00 - 23.00

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 86 di 95

Servizio	Servizio sito/portale web e componenti accessori		
Livelli di Servizio	Soglia	Penale	Orario di osservazione
Tempi di risposta	2 sec. nel 98% dei casi	€ 100,00 per ogni decimo di punto percentuale di diminuzione rispetto al valore prefissato	

Gli indicatori sono rilevati sulle sole pagine del sito stesso (pagine html, contenuti, grafica, portlet) e non agli eventuali servizi richiamati.

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 87 di 95

ASPETTI GESTIONALI

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 88 di 95

8. CORRISPETTIVI

SERVIZI PROFESSIONAL E ACCESSORI		
Servizio	CORRISPETTIVI	Euro/giorno
Professional (Supporto e Governance)	Servizio di Coordinamento	800
	Servizio Specialistico	502
	Servizio Operativo	362
Servizio	CORRISPETTIVI	Euro
Servizi accessori	Viaggio (a/r)	376,54
	Indennità di trasferta giornaliera	160,29

Il Servizio può essere remunerato secondo due modalità:

- se le attività di supporto richieste rivestano natura progettuale e sono identificabili output concreti oggetto di consegna, l’obiettivo sarà dimensionato secondo le tariffe della tablla precedente e l’importo complessivo derivante sarà remunerato a fronte della consegna degli output definiti.
- se le attività di supporto rivestano natura occasionale verranno remunerate a Tempo e Spesa secondo le tariffe della tablla precedente.

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 89 di 95

SERVIZI DI SVILUPPO		
Servizio	CORRISPETTIVI	Euro
Sviluppo e manutenzione evolutiva del software ad hoc	Unità di sviluppo	197,42
	Unità non funzionali (gg)	432,00
	Unità progettuale/di ambito (gg)	651,00
Servizio	CORRISPETTIVI	Euro/giorno
Personalizzazione prodotti di mercato	Personalizzazione prodotti di mercato	341,00

Il Servizio è dimensionato attraverso i corrispettivi di cui sopra applicati alle quantità stimate e remunerato secondo quanto riportato all'Allegato C, paragrafo 2.1 alla presente Convenzione.

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 90 di 95

SERVIZI DI BASE DI CONDUZIONE		
GESTIONE E CONDUZIONE SERVIZI ICT		
Servizio	CORRISPETTIVI	Euro
Manutenzione servizi ICT	Unità di manutenzione – mese	1,64
	Manutenzione a giorni persona	341,00
Servizio di Customer Care	Canone annuale per disponibilità del servizio	30.000,00
	Richieste risolte da Customer Support	7,15
	Richieste risolte dal Supporto Specialistico	35,52
	Numero pacchetti per 100 conversazioni in chatbot	26,58
	Attivazione servizio canali aggiuntivi (UT)	82.790,00
	Canone annuale per disponibilità canali	8.333,33
	Costo per invio di SMS	1,30
	Attivazione servizio per campagne outbound (UT)	55.066,67
	Canone annuale per disponibilità servizio campagne outbound	46.100,00
	Costo per invio di SMS (pacchetti da 30) per campagne outbound	1,30
	Costo per invio mail (pacchetti da 1000) per campagne outbound	2,80
	Canone annuale per Community per Amministrazione richiedente	212.440,00
	Canone annuale Dashboard ad utente	280,00
	Canone annuale per disponibilità Dashboard	3.000,00

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 91 di 95

GESTIONE E CONDUZIONE INFRASTRUTTURA		
Servizio	CORRISPETTIVI	Euro/mese
Server	Immagini	558,32
	vCPU	98,68
	vRAM	15,86
	Immagini DR	449,00
	vCPU DR	67,68
	vRAM DR	17,25
Storage	GB allocati	0,395
Appliance	GBA allocati in esercizio	3,9
	GBT allocati in esercizio	2,15
	GBT DR allocati in DR	0,97
	Canone Appliance Q Tier1	2.855,00
	Canone Appliance Q Tier2	1.192,00
	Canone Appliance Q Tier3	2.451,00
Piattaforma Big Data	GB BIG DATA allocato	3,26
Piattaforma NOSQL	GB NOSQL (o IN-MEMORY) allocato	2,26
SERVIZI DI COLLABORATION E COMMUNICATION		
Servizio	CORRISPETTIVI	Euro/mese
Servizio navigation Internet	utente base	0,61
	utente esteso	2,62
	utente avanzato	3,16
	Plus Sicurezza	0,96
Virtual Private Network utente	Utente con token OTP	2,55
Virtual desktop pooled	Virtual Desktop – Standard	26,86
Bundle vAPP	Bundle vApp – Standard	24,25
Singola vAPP	Singola vApp – Standard	9,84
Singola vAPP C	Singola vAPP Capped 40%	7,56
Plus	Reporting accesso utenti - Plus	802,15
	Accesso da rete pubblica – Plus	1
SERVIZI DI TIPOLOGIA CLOUD		
PIATTAFORMA IAAS		
Servizio	CORRISPETTIVI	Euro/mese

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 92 di 95

IaaS	canone mensile - VM 1 CPU 2 GB RAM (200 GB HD, backup VM, DR base)	92,11
	canone mensile - VM 2 CPU 4 GB RAM (200 GB HD, backup VM, DR base)	118,44
	canone mensile - VM 4 CPU 8 GB RAM (200 GB HD, backup VM, DR base)	171,1
	canone mensile - VM 4 CPU 16 GB RAM (200 GB HD, backup VM, DR base)	257,28
	canone mensile - VM 8 CPU 32 GB RAM (200 GB HD, backup VM, DR base)	448,77
	canone mensile - Licenza Red Hat Enterprise Linux , Standard	1,21
	canone mensile - Licenza Windows server	0,65
	canone mensile - STORAGE AGGIUNTIVO 1GB in HA, con Backup e DR base	0,29
	canone mensile - Storage NAS 1GB in HA, con backup e DR base	0,23
	canone mensile - Backup e Restore CSV Costo aggiuntivo per 1GB Profilo di backup Silver	0,031
	canone mensile - Backup e Restore CSV Costo aggiuntivo per 1GB Profilo di backup Silver_Plus	0,048
	canone mensile - Backup e Restore CSV Costo aggiuntivo per 1GB Profilo di backup Gold	0,069
	canone mensile - Backup e Restore CSV Costo aggiuntivo per 1GB Profilo di backup Gold_Plus	0,082
	canone mensile - Backup e Restore CSV Costo aggiuntivo per 1GB Profilo di backup Gold_Plus 6 mesi	0,095
	canone mensile - Backup e Restore CSV Costo aggiuntivo per 1GB Profilo di backup Platinum	0,12
	canone mensile - Backup e Restore CSV Costo aggiuntivo per 1GB Profilo di backup Platinum_Plus	0,16
	canone mensile - Backup e Restore CSV Costo aggiuntivo per 1GB Profilo di backup Platinum_Plus 6 mesi	0,18

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 93 di 95

	canone mensile - Backup e Restore dei dati strutturati e non strutturati, tramite agent per 1 GB Silver	0,036
	canone mensile - Backup e Restore dei dati strutturati e non strutturati, tramite agent per 1 GB Silver_Plus	0,039
	canone mensile - Backup e Restore dei dati strutturati e non strutturati, tramite agent per 1 GB Gold	0,031
	canone mensile - Backup e Restore dei dati strutturati e non strutturati, tramite agent per 1 GB Gold_Plus	0,070
	canone mensile - Backup e Restore dei dati strutturati e non strutturati, tramite agent per 1 GB Gold_Plus 6 mesi	0,081
	canone mensile - Backup e Restore dei dati strutturati e non strutturati, tramite agent per 1 GB Platinum	0,15
	canone mensile - Backup e Restore dei dati strutturati e non strutturati, tramite agent per 1 GB Platinum_Plus 6 mesi	0,17

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi – pag. 94 di 95

SERVIZI DI BASE DIVERSI DA QUELLI DI CONDUZIONE		
PIATTAFORME ASP		
SERVIZI DI SICUREZZA		
Servizio	CORRISPETTIVI	Euro/mese
Piattaforme di sicurezza - Identity Access Management	utente base	0,014
	utente gestito	0,229
	utente certificato	0,131
Piattaforme di sicurezza - SOC	Servizio SOC base - Fascia A da 15.001 a 50.000 endpoint	33.997,49
	Servizio SOC base - Fascia B da 5.001 a 15.000 endpoint	16.517,00
	Servizio SOC base - Fascia C da 1 a 5.000 endpoint	6.882,08
	Dispositivi gestiti	215,25
SERVIZIO SITO/PORTALE WEB E COMPONENTI ACCESSORI		
Servizio	CORRISPETTIVI	Euro UT
Servizio sito/portale web e componenti accessori	Sviluppo Fascia Bassa	62.850,00
	Sviluppo Fascia Media	92.860,00
	Sviluppo Fascia Alta	151.710,00
	Sviluppo Fascia Extra	170.510,00
	Migrazione Fascia Bassa	17.690,00
	Migrazione Fascia Media	27.440,00
	Migrazione Fascia Alta	39.000,00
	Migrazione Fascia Extra	51.670,00
	Pagine con servizi applicativi max 3 (Servizi Opzionali)	24.516
	Area trasparenza (Servizi Opzionali)	12.264
	CORRISPETTIVI	Euro/mese
	conduzione Fascia Bassa	15.068,00
	conduzione Fascia Media	24.044,00
	conduzione Fascia Alta	35.041,00

Allegato A

Descrizione dei Servizi, Livelli di servizio e Corrispettivi– pag. 95 di 95

conduzione Fascia Extra	52.765,00
Social (Servizi Opzionali)	5.008,00
Redazione speciale (Servizi Opzionali)	963,00
Redazione Fascia Bassa	4.816,00
Redazione Fascia Media	6.442,00
Redazione Fascia Alta	7.916,00
Redazione Fascia Extra	9.575,00

PNRR

Missione – Componente – Asse

Investimento 1.3.1

Allegato B - Piano Operativo

TITOLO: PNRR – Investimento M6C2 - 1.3.1 - Fascicolo Sanitario Elettronico

Sommario

1. Introduzione	3
2. Descrizione del Progetto	5
3. Modalità Operative	10
4. Piano Progettuale di Dettaglio	14
5. Articolazione Temporale del Progetto	17
6. Costi del Progetto	18
7. Interrelazione con altri interventi del PNRR	19

1. Introduzione

L'investimento 1.3.1 della Missione 6 Componente 2 del Piano Nazionale di Rilancio e Resilienza stanzia 1,38 miliardi di euro per il potenziamento del Fascicolo Sanitario Elettronico (FSE) al fine di garantirne la diffusione, l'omogeneità e l'accessibilità su tutto il territorio nazionale da parte degli assistiti e operatori sanitari. Di questi fondi, 811 milioni di euro circa sono stanziati per il potenziamento del Fascicolo anche tramite nuove componenti architetturali e di change management, mentre i restanti 569 milioni circa vanno a finanziare progetti in essere, complementari al Fascicolo Sanitario Elettronico e funzionali al suo potenziamento.

Per l'erogazione dei 811 milioni da parte della Commissione Europea associati a tale investimento, sono stati definiti due obiettivi:

- **Q4-2025 – l'85% dei medici di base alimentano il Fascicolo sanitario elettronico,**
- **Q2-2026 - tutte le Regioni e Province Autonome hanno adottato e utilizzano il FSE,**

per raggiungere i quali sono state fissate le seguenti milestones:

- **Q2 2024 – completamento dell'implementazione dell'EDS e del Gateway,**
- **Q4 2024 – tutti i documenti clinici devono essere digitalmente nativi ed integrati nel FSE, ovvero nell'EDS e nel Gateway.**

Il FSE, come indicato nelle Linee Guida per l'Attuazione del Fascicolo Sanitario Elettronico (d'ora in avanti denominate anche LLGG o Linee Guida) definite dal Ministero della Salute (MdS) e dal Ministero per l'Innovazione Tecnologica e la Transizione digitale (MITD) di concerto con il Ministero dell'Economia e delle Finanze, deve diventare:

- Il punto unico ed esclusivo di accesso per i cittadini ai servizi del SSN,
- L'ecosistema di servizi basati sui dati per i professionisti sanitari per la diagnosi e cura dei propri assistiti e per una assistenza sempre più personalizzata sul paziente,
- Strumento per le strutture ed istituzioni sanitarie che potranno utilizzare le informazioni cliniche del FSE per effettuare analisi di dati clinici e migliorare la erogazione dei servizi sanitari.

Per farlo, sono state definite 4 direttive di azione per potenziare il FSE:

- (i) Garantire servizi di sanità digitale omogenei ed uniformi,
- (ii) Uniformare i contenuti in termini di dati e codifiche adottate,
- (iii) Rafforzare l'architettura per migliorare l'interoperabilità del FSE,
- (iv) Potenziare la governance delle regole di attuazione del nuovo FSE.

Tali direttive di azione mirano a superare i limiti che connotano l'attuale contesto nazionale, consistenti in:

- Una concezione del FSE che prevede (i) un fascicolo prevalentemente orientato ai documenti, in termini di servizi, contenuti ed architettura, (ii) una governance focalizzata sulla standardizzazione di un nucleo minimo di documenti e non estesa ai documenti clinici integrativi comunque esistenti,
- Una attuazione del FSE caratterizzata da (i) servizi previsti dalla norma parzialmente diffusi sul territorio nazionale, (ii) implementazione non completa del nucleo minimo di documenti del fascicolo ed obbligatori per norma, (iii) documenti prodotti prevalentemente in forma non strutturata ed omogenea sul territorio nazionale, (iv) carenza di sistemi di codifica esaustivi per valorizzare tutte le informazioni cliniche, (v) alimentazione del fascicolo non uniforme, (vi) interoperabilità tra gli FSE Regionali limitata dalle loro disomogeneità oltre che

dalla carenza di un sistema anagrafico autoritativo di livello nazionale, (vii) governance basata su un coinvolgimento non sistematico ed istituzionalizzato delle amministrazioni interessate e degli enti di standardizzazione, con processi di messa a norma degli standard non tempestivi.

A tal fine, esse agiscono sulle 4 dimensioni del FSE, ovvero servizi, contenuti, architettura e governance, per ciascuna delle quali le Linee Guida definiscono i requisiti obbligatori e raccomandati da attuare nel breve, medio e lungo periodo. In particolare:

- Requisiti obbligatori da attuare nel breve termine, per (i) uniformare a livello nazionale i servizi del FSE già esistenti per cittadini ed operatori sanitari, (ii) estendere il nucleo minimo di documenti obbligatori del FSE e perfezionare la loro standardizzazione unitamente a quella dei documenti integrativi già implementati dalle Regioni, (iii) evolvere il modello di interoperabilità del FSE attraverso la realizzazione di una componente per l'acquisizione dei dati e documenti dai loro sistemi produttori, (iv) adottare un sistema per il controllo ed il monitoraggio della qualità delle informazioni cliniche che alimentano il FSE, (v) istituzionalizzare e governare processi di standardizzazione a livello nazionale delle diverse dimensioni del FSE;
- Requisiti obbligatori da attuare entro la durata del PNRR, per (i) evolvere verso servizi per l'accesso ai dati clinici (non più solo dei documenti) da parte di cittadini ed operatori sanitari, per il loro utilizzo nelle attività di prevenzione e cura svolte dai MMG/PLS e dai medici specialisti, per il loro impiego da parte dei farmacisti per svolgere le rispettive funzioni di verifica dell'aderenza alle terapie e delle possibili reazioni avverse, per il loro uso da parte delle istituzioni sanitarie per la programmazione sanitaria e la prevenzione, (ii) alimentare il FSE con dati clinici standardizzati attraverso l'uso di sistemi di codifica e dizionari, acquisiti nelle attività di prevenzione, diagnosi e cura condotte dai professionisti sanitari sugli assistiti, ivi compresi patient summary prodotti da MMG/PLS secondo target PNRR, dati di telemedicina, dati generati autonomamente dai pazienti ed imaging, (iii) attuare una nuova architettura del FSE, completa di un repository di dati clinici centrale in standard HL7 FHIR (opzionalmente riusabile anche a livello locale) e potenziata da nuove componenti di interoperabilità in grado di raggiungere e collegare tutte le strutture sanitarie produttrici di informazioni, (iv) adottare strumenti di Advanced Analytics, anche basati su tecniche di Intelligenza Artificiale per l'elaborazione dei dati clinici del FSE, (v) mettere a disposizione i dati clinici per la ricerca, (vi) istituzionalizzare a livello nazionale un processo continuo e sistematico di verifica delle esigenze informative e di standardizzazione dei documenti e dati clinici da far confluire nel FSE in aggiunta a quelli inizialmente previsti;
- Requisiti raccomandati per (i) realizzare servizi basati sui dati clinici, ulteriormente estesi a dati omici, genetici ed epigenetici, per una cura sempre più personalizzata sull'assistito, (ii) mettere a disposizione delle Istituzioni Sanitarie per finalità di governo, (iii) estendere i dati disponibili per ricerca a dati omici, genetici ed epigenetici.

La realizzazione di tali requisiti produce per il cittadino:

- Benefici diretti, in termini di (i) facilitazione dell'accesso alle cure su tutto il territorio nazionale, (ii) aumentata consapevolezza sul proprio stato di salute grazie ai dati clinici ed utile ad intraprendere le azioni per prevenire l'insorgere delle patologie, (iii) cure personalizzate rispetto al suo quadro clinico
- Benefici indiretti, in termini di (i) miglioramento della qualità delle cure assicurate da professionisti e strutture sanitarie attraverso l'utilizzo dei dati clinici e la loro cooperazione, (ii) aumentata capacità del sistema sanitario di intercettare per tempo l'insorgere di

patologie e del diffondersi di epidemie, grazie all'uso dei dati clinici, (iii) programmazione dell'offerta di prestazioni sulla base delle caratteristiche della popolazione assistita, (iv) potenziamento della ricerca per l'individuazione di nuove cure e trattamenti.

Per attuare i requisiti definiti per il nuovo FSE, le Linee Guida saranno seguite da documenti di programmazione che:

- Fissano target sui tempi di implementazione, livello di alimentazione ed utilizzo, tenendo conto dello stato dell'arte da cui partono gli FSE delle singole Regioni e dunque dell'effettivo gap che dovranno colmare per attuare il FSE nella nuova concezione,
- Programmano risorse finanziarie per il periodo 2022-2026, tenendo conto delle azioni che dovranno essere attuate dalle singole amministrazioni, siano esse centrali che locali.

In conclusione, quindi, il nuovo FSE mira a realizzare un Ecosistema di Dati Sanitari (EDS) sulla base del quale sia possibile implementare ed erogare servizi evoluti basati sui dati atomici. A tale fine:

- Raccoglie i dati e documenti prodotti dalle strutture sanitarie pubbliche, private accreditate e non accreditate,
- Consente ai cittadini di accedere ai propri dati e documenti,
- Abilita i professionisti sanitari ad accedere ai dati e documenti dei cittadini per la loro cura,
- Mette a disposizione degli Enti di ricerca una fonte dati utile per le finalità di ricerca in ambito medico e biomedico
- Permette alle Direzioni Sanitarie Regionali di svolgere le proprie funzioni di prevenzione e di governo,
- Consente al Ministero della Salute di avere dati utili per finalità di prevenzione, sorveglianza epidemiologica, profilassi internazionale e governo.

2. Descrizione del Progetto

2.1 Architettura Generale

La nuova architettura del FSE deve realizzare meccanismi che, favorendo l'integrazione periferica, consentano l'alimentazione completa del Fascicolo Sanitario Elettronico mediante i dati ed i documenti sanitari e sociosanitari prodotti sul territorio nazionale secondo formati standard, come definiti dalle Linee Guida. Questa rappresenta una condizione necessaria affinché anche i meccanismi di interoperabilità possano essere efficacemente potenziati.

Un altro obiettivo che si vuole raggiungere è quello di garantire uniformità di accesso ai servizi sanitari on line sul territorio nazionale e rendere fruibile l'informazione sia attraverso i documenti nativamente digitali, sia attraverso i dati atomici che li compongono, assicurando le condizioni per lo sviluppo di servizi di presa in carico del paziente sempre più avanzati.

La nuova architettura del FSE nel suo complesso prevede (1) sia la **gestione dei documenti**, potenziando i meccanismi di interoperabilità tra gli FSE Regionali, (2) sia la **gestione dei dati atomici**, prodotti nell'ambito dei processi di prevenzione, cura e riabilitazione.

(1) Per quanto attiene la **gestione dei documenti**, essa mantiene una **struttura federata**, distribuita sulle singole Regioni per le componenti di indicizzazione (Registry Regionali, laddove presenti) e di archiviazione (Document Repository), ed introduce un elemento centrale nell'ambito dell'Infrastruttura Nazionale di Interoperabilità (INI), quale è il Registry Nazionale (Indice Nazionale), per rendere più efficienti ed efficaci i meccanismi di interoperabilità tra gli FSE Regionali. Nell'ambito

di tale struttura federata, i documenti oggetto di indicizzazione devono essere in formato standard HL7 CDA2 ed avere una rappresentazione “human readable” in formato PDF. Per questo motivo il CDA2 in cui sono contenuti i dati strutturati dell’evento clinico cui riferisce il documento, deve essere iniettato nel corrispondente PDF, quest’ultimo firmato in PaDES.

(2) Relativamente alla **gestione dei dati**, la nuova architettura prevede l’introduzione dell’**Ecosistema Dati Sanitari (EDS)**, come da DL 4/2022, che comprende un Data Repository Centrale in cui sono archiviati i dati in **standard FHIR** acquisiti dai sistemi produttori utilizzati dagli esercenti le professioni sanitarie che prendono in cura il paziente, sia nell’ambito del Servizio Sanitario Nazionale e dei servizi socio-sanitari regionali, sia al di fuori degli stessi. L’EDS implementa altresì API in standard FHIR per la costruzione di servizi basati sui dati di:

- Prevenzione, cura e riabilitazione, rivolti ai professionisti sanitari e alle strutture sanitarie abilitate, secondo le autorizzazioni al trattamento rilasciate dagli assistiti, oltre che ai cittadini al fine consultare le proprie informazioni cliniche,
- Prevenzione, sorveglianza epidemiologica e governo, di supporto alle Direzioni Sanitarie Regionali,
- Prevenzione e profilassi internazionale di supporto al Ministero della Salute.

I dati e i documenti clinici sono acquisiti dalle strutture sanitarie mediante una componente **Gateway**, collocata nelle reti aziendali o regionali, nel momento stesso in cui sono prodotti dai sistemi utilizzati nelle strutture sanitarie e prima che siano indicizzati nei FSE regionali. Una volta acquisiti i dati e i documenti, le istanze della componente Gateway hanno il compito di validare i dati/documenti, convertirli in formato FHIR, se non lo sono già in origine, e inviarli al Data Repository Centrale dell’EDS, che li memorizza in formato FHIR.

Il Gateway è l’elemento che consente di alimentare e mantenere allineate le componenti orientate alla gestione dei documenti (Registry) e quelle orientate alla gestione dei dati (EDS).

2.2 Le Componenti Oggetto di Realizzazione

Le macro-componenti della nuova architettura del FSE che sono oggetto del presente piano operativo, sono quelle inerenti la gestione dei dati, e precisamente:

Ecosistema Dati Sanitari (EDS)	<p>Si compone di:</p> <ul style="list-style-type: none"> ▪ Data Repository Centrale: implementa le funzioni per ricevere, memorizzare e rendere accessibili in modo granulare <i>i dati clinici, personali e amministrativi</i>, in formato <i>FHIR</i>, acquisiti dai sistemi utilizzati dai professionisti e dalle strutture sanitarie pubbliche e private (sia accreditati con il SSN sia non accreditati) per le finalità indicate nell’Articolo 12, Decreto Legge n. 179 del 18 ottobre 2012, nonché <i>i dati autonomamente generati / raccolti dall’assistito (PGHD)</i> ed <i>i dati provenienti da sistemi di telemedicina</i>. Il Data Repository Centrale consente anche di realizzare meccanismi di interoperabilità del dato tra Regioni (similmente al Registry Nazionale per i documenti). In particolare, esso implementa servizi di sottoscrizione per l’erogazione dei dati in esso contenuti che consentono eventualmente di distribuirli su data store FHIR gestiti anche a livello regionale / aziendale in base alla loro pertinenza e finalità. ▪ Servizi di Gestione di Dizionari e Codifiche (Servizi Terminologici): consentono di gestire, manutenere e mettere a disposizione <i>i dizionari e le codifiche</i> previsti dalle LLGG per la valorizzazione univoca dei dati prodotti dai professionisti e strutture sanitarie, acquisiti ed archiviati nell’ambito del Data Repository Centrale dell’EDS. I servizi
---------------------------------------	--

	<p>terminologici sono utilizzati dal Gateway per la validazione dei dati da esso acquisiti, e possono essere utilizzati dai sistemi produttori per la loro codifica e valorizzazione.</p> <ul style="list-style-type: none"> ▪ Layer dei Servizi: è l'elemento dell'EDS che ha l'obiettivo di implementare, secondo logica a micro-servizi (API), ed esporre servizi applicativi basati sui dati memorizzati nel Data Repository Centrale dell'EDS, che possono essere invocati da client di front-end, quali possono essere i Portali FSE Regionali / Nazionale ed app mobile destinati a cittadini ed operatori sanitari, piuttosto che applicazioni utilizzate dalle strutture e dai professionisti sanitari, comprese le cartelle dei MMG/PLS. Implementa altresì le funzioni per l'accesso ai servizi digitali operazionali / dispositivi (es. servizi di scelta e revoca MMG/PLS, prenotazione prestazioni sanitarie, accesso ai servizi di telemedicina, pagamento di prestazioni erogate in regime di SSN, ecc) erogati ed esposti da sistemi terzi, come ANA, sistemi CUP, sistemi di Telemedicina, PagoPA. Al fine di realizzare i servizi di business adotta componenti di API Gateway, API Management e di orchestrazione di API, che consentono di comporre e gestire API lungo workflow di lavoro e processi di interoperabilità che danno origine a servizi di business e/o a nuove API. Nell'ambito di tale layer sono esposti servizi dell'EDS trasversali, funzionali a: (1) Gestione di Dizionari e Codifiche, (2) Anonimizzazione e Pseudonimizzazione dei dati, (3) Definizione e distribuzione delle Regole di Validazione dei dati, (4) Definizione e distribuzione delle Regole di Mapping in FHIR di dati acquisiti in formato CDA2, (5) Policy Management per configurare, gestire e verificare l'applicazione delle politiche di autorizzazione, sicurezza e privacy per l'accesso al dato, (6) Autenticazione di utenti e sistemi. ▪ Funzioni Utente: costituiscono le funzioni che implementano la logica di business dei servizi previsti dalle LLGG e rivolti a cittadini, MMG/PLS, Medici Specialisti, Farmacisti, Direzioni Sanitarie Regionali ed altri Operatori Sanitari, esclusa la rispettiva UX/UI. Comprendono funzioni di dashboarding, data analytics e reporting. ▪ Sistema di Monitoraggio e Controllo: ha obiettivo di valutare l'effettiva alimentazione in termini di dati e documenti del FSE, il suo utilizzo da parte di cittadini, operatori ed enti sanitari. Prevede uno strato persistente nel Data Repository Centrale, dove sono memorizzati i dati di monitoraggio, ed un cruscotto direzionale per gli utenti autorizzati degli Enti centrali, Regioni e Aziende Sanitarie. ▪ Sistema di Amministrazione: realizza le funzioni di monitoraggio e console di amministrazione del sistema in tutte le sue componenti, a partire da quelle infrastrutturali e di rete, fino alle componenti applicative.
Gateway	Elemento che estende l'EDS implementando le funzionalità utili ad acquisire i dati clinici dai sistemi produttori. In particolare, ha il compito di verificare che i dati clinici, prodotti dai sistemi utilizzati dai professionisti e dalle strutture sanitarie di prevenzione e cura, rispettino le regole sintattiche e semantiche di composizione previste dalla norma e, una volta validati, di tradurli nel formato HL7 FHIR, laddove non generati alla fonte in tale standard, per essere inviati al Data Repository Centrale dell'EDS. A valle della validazione dei dati, qualora estratti a partire da un documento, il Gateway interviene anche nel processo di indicizzazione del documento sul Registry Nazionale e Regionale, per garantire che venga mantenuta la correlazione fra il documento ed i dati FHIR da esso acquisiti. Esso inoltre provvede alla raccolta dei dati di log delle transazioni eseguite ed al loro invio al Sistema di Monitoraggio e Controllo dell'EDS.

Agli elementi architetturali anzi indicati si aggiungono l'insieme dei **servizi di integrazione** con:

- *Anagrafe Nazionale Assistiti (ANA)*, per quanto attiene i dati anagrafici degli assistiti ed identificazione dei MMG/PLS ad essi associati; le posizioni anagrafiche di ANA sono

utilizzate direttamente dal Gateway (per l'eventuale applicazione di controlli sulla esistenza delle posizioni anagrafiche cui riferiscono i dati acquisiti) e dal Data Repository Centrale dell'EDS, indirettamente dai sistemi produttori e dai FSE Regionali che le adottano nei sistemi anagrafici regionali / aziendali.

- *Sistema Tessera Sanitaria (Sistema TS)*, per quanto attiene l'acquisizione dei dati amministrativi di prescrizione e certificazione, nonché l'utilizzo dei dati dei medici ed operatori sanitari iscritti agli ordini professionali.
- *INI-Anagrafe Consensi Nazionale*, per verificare il consenso alla consultazione del fascicolo in fase di richiesta accesso ad esso da parte del personale sanitario.
- *INI-Anagrafe Nazionale delle Deleghe*, per quanto riguarda la verifica dei soggetti terzi che sono stati delegati dagli assistiti per l'accesso ai servizi offerti dal FSE.
- *Document Repository* delle strutture sanitarie, per le fasi di pubblicazione di un documento validato, acquisizione del suo riferimento e dei suoi metadati.
- *Registry Nazionale* per la comunicazione dei metadati dei documenti che devono essere su di esso indicizzati.
- *Portale FSE Nazionale*, che dovrà implementare i servizi utente previsti dalle LLGG secondo il modello di UI/UX che sarà definito a livello nazionale (FSE Best in Class), per il tramite delle API esposte dal Livello dei Servizi dell'EDS.
- *Sistemi di Cartella MMG/PLS*, che alimentano con i dati e documenti nativi digitali da essi prodotti il Data Repository Centrale dell'EDS, per il tramite del Gateway, e consumano i servizi basati sui dati esposti dal Layer dei Servizi dell'EDS.
- *Sistemi delle Strutture Sanitarie*, che alimentano con i dati e documenti nativi digitali da essi prodotti il Data Repository Centrale dell'EDS, per il tramite del Gateway, e consumano i servizi basati sui dati esposti dal Layer dei Servizi dell'EDS.
- *Servizi di Telemedicina*, che alimentano il Data Repository Centrale dell'EDS con i dati acquisiti per il tramite delle piattaforme di telemedicina, e lo consulteranno per accedere ai dati clinici degli assistiti da essi presi in carico.
- *NSIS* per quanto attiene le previsioni del Regolamento Interconnessione.

In termini di **deployment** delle componenti ivi delineate si prevede:

- **Deployment dell'EDS e di tutte le sue componenti su ambiente infrastrutturale centrale.**
Tale ambiente potrà essere inizialmente implementato su infrastrutture on-premises di SOGEI per essere successivamente (eventualmente) migrato in cloud, sul PSN nazionale.
- **Disponibilità potenziale del Gateway**
 1. **sia in modalità a servizio**, ospitato su una infrastruttura gestita a livello nazionale quale è quella di SOGEI piuttosto che del PSN,
 2. **sia installato su una infrastruttura regionale**, per essere assicurato da questa in modalità a servizio alle strutture sanitarie,
 3. **sia installato all'interno della singola struttura sanitaria**, in modalità on-premises, su una infrastruttura che si colloca nel perimetro della ASL/AO medesima.

Gli ambienti infrastrutturali che saranno assicurati per lo sviluppo, il test ed il deployment delle componenti progettuali sono:

- **Ambienti di sviluppo e test**, per l'esecuzione delle attività di rilascio del codice sorgente e verifica del suo corretto funzionamento, propedeutico al packaging della release software.
- **Ambiente di pre-produzione**, allineato in termini di dati all'ambiente di produzione ed in termini software all'ultima versione disponibile, utile sia per effettuare test propedeutici alla messa in produzione di nuove release software, sia per simulare eventuali bug rilevati in produzione e verificare l'efficacia di patch realizzate per la loro risoluzione, sia per finalità di formazione e training.
- **Ambiente di produzione**, in cui sono in esecuzione le componenti del progetto.
- **Ambiente di qualificazione delle soluzioni di mercato e/o custom** che producono dati / documenti e che devono integrarsi con il Gateway, e/o che devono accedere ai servizi dell'EDS, attraverso il quale saranno condotte le attività per la verifica e certificazione di dette soluzioni.
- **Ambienti di integrazione configurati** rispetto al contesto delle singole Regioni ed utili a testare il corretto funzionamento dell'interoperabilità delle istanze aziendali / regionali delle soluzioni qualificate con il Gateway – laddove produttrici di dati - piuttosto che con l'EDS – laddove consumatrici di servizi e dati.

Sono altresì inclusi gli ambienti infrastrutturali di diaster & recovery utili ad assicurare continuità operativa anche in caso di disastro.

Nel seguito si riepilogano le componenti oggetto di realizzazione e fornitura nell'ambito del presente piano operativo, con indicazione del fatto che si tratti di software applicativo o di servizio infrastrutturale, nonché della tipologia di deliverables documentali previsti.

Macro-Componente	Componente	Tipologia Componente (SW/Infrastrutturale)	Tipologia Deliverables Documentali (*)
C1 – EDS: Ecosistema Dati Sanitari	C1.1 - EDS - Data Repository	Software	Progettazione Software
	C1.2 - EDS - Servizi di Gestione Dizionari e Codifiche (Servizi Terminologici)	Software	Progettazione Software
	C1.3 - EDS - Sistema di Monitoraggio e Controllo	Software	Progettazione Software
	C1.4 - EDS - Layer dei Servizi	Software	Progettazione Software
	C1.5 - EDS - Funzioni Utente	Software	Progettazione Software
	C1.6 - EDS - Sistema di Amministrazione	Software	Progettazione Software
C2 – Gateway	C2.1 – Gateway	Software	Progettazione Software
C3 – Servizi di Integrazione	C3.1 - Integrazione con Sistemi MMG/PLS	Software	Specifiche Tecniche di Integrazione
	C3.2 - Integrazione con Sistemi delle Strutture Sanitarie	Software	Specifiche Tecniche di Integrazione
	C3.3 - Integrazione con Sistemi di Telemedicina	Software	Specifiche Tecniche di Integrazione
	C3.4 - Integrazione con Sistemi Nazionali: ANA, Sistema TS, INI, Registry Nazionale, Anagrafe Consensi, Anagrafe Deleghe, Portale Nazionale FSE (**)	Software	Specifiche Tecniche di Integrazione
C4 – Ambienti Infrastrutturali	C4.1 - Ambienti di Sviluppo, Test, Pre-Produzione, Produzione, Qualificazione, Integrazione	Servizi Infrastrutturali	Progettazione Tecnica Infrastruttura e Dimensionamento

(*) Tutte le componenti software dovranno essere altresì corredate della relativa manualistica di installazione e configurazione, oltre che utente. Per quanto attiene le specifiche tecniche di integrazione queste dovranno essere complete delle interfacce (swagger) allo scopo previste.

(**) La realizzazione di tali servizi di integrazione potrà essere avviata sulla base di un piano condiviso con il titolare del Sistema TS, ANA, ecc

I requisiti sulla base dei quali le componenti oggetto del presente piano operativo saranno implementate sono quelli definiti dal MITD, di concerto con il Ministero della Salute, e dettagliati nei seguenti documenti:

- Linee Guida di Attuazione (LLGG)
- Linee Guida Architetturali, che definiscono requisiti funzionali delle componenti architettoniche del progetto
- Specifiche tecniche funzionali di dettaglio del componente Gateway
- Specifiche tecniche funzionali di dettaglio del componente Ecosistema Dati Sanitari (EDS)
- Specifiche tecniche funzionali del Sistema di Monitoraggio e Controllo
- Requisiti in tema di Cybersecurity e Privacy
- Requisiti di Architettura, Infrastruttura e Gestione
- Documentazione specifiche di mapping documenti in formato HL7 CDA2 vs HL7 FHIR.

I requisiti di progettazione software, le scelte architettoniche e tecnologiche che potranno essere adottate in attuazione dei requisiti tecnico-funzionali definiti nei documenti anzi indicati dovranno essere proposti da SOGEI e approvati ed accettati da parte del MITD, propedeuticamente alla esecuzione delle attività implementative.

3. Modalità Operative

3.1 Modello di Governance della Convenzione

Il governo delle attività previste dalla Convenzione è da considerarsi pienamente integrato e sinergico con il governo di tutte le iniziative in ambito Sanità Digitale coordinate dal DTD/MITD.

A riguardo sono state identificate le seguenti strutture organizzative:

- **Comitato di attuazione**, con ruoli e responsabilità così come definiti all’articolo 3 della *Convenzione*
- **Program management office**, istituito all’interno del DTD/MITD con la responsabilità sulle seguenti attività:
 - esaminare e rendere un parere sotto il profilo tecnico operativo relativamente al Piano operativo annuale;
 - garantire il costante monitoraggio delle attività, anche al fine di proporre adeguate soluzioni ad eventuali criticità emergenti in corso di attuazione;
 - verificare, attraverso attività di monitoraggio, il grado di raggiungimento degli obiettivi definiti nel Piano operativo mediante riunioni di avanzamento;
 - mettere in atto le azioni necessarie per rimuovere le criticità che dovessero emergere con particolare riferimento a quelle che hanno un impatto sul rispetto dei tempi;

3.2 Modalità di Conduzione, Monitoraggio e Controllo Interno del Progetto

Il progetto prevede l’adozione di un approccio Agile (Scaled Agile Framework), ed una organizzazione in due tipologie di stream distinti:

- **stream realizzativi** (Agile Release Train - ART), uno per ognuna delle macro-componenti di cui al capitolo 2.2,
- **stream di servizi continuativi** funzionali alla qualificazione e validazione delle soluzioni e loro integrazioni con l’EDS ed il Gateway, nonché ad assicurare la loro continuità operativa per il completamento dell’interconnessione di tutte le Regioni e Strutture Sanitarie,

tutti coordinati attraverso un team di **Project Management** operativo che si interfaccia con il team di **Program Management**, quest’ultimo supportato a sua volta da una struttura di **Program Management Office**.

In particolare, **4 sono gli stream realizzativi**, inerenti la progettazione, implementazione, test e roll-out di **Ecosistema Dati Sanitari, Gateway, Servizi di Integrazione ed Ambienti Infrastrutturali**, ciascuno dei quali così organizzati:

- **Business Owner (BO)** – Definisce gli obiettivi di business che devono essere soddisfatti dalla soluzione oggetto di rilascio.
- **Product Manager (PRM)** – Definisce i requisiti di business e di architettura funzionale, nonché gli standard di riferimento, che devono essere implementati dalla soluzione oggetto di rilascio nell’ambito dello specifico stream, per soddisfare gli obiettivi fissati dai BO.
- **Release Train Engineer (RTE)** – Definisce e mantiene aggiornato il product backlog e la roadmap di rilascio della soluzione prevista nello specifico stream progettuale, nel rispetto dei requisiti espressi dal PRM. Stabilisce, di concerto con il PRM, gli sprint di realizzazione dei prodotti intermedi e finali che compongono la soluzione e gli Agile Team ad essi assegnati. Gestisce ed ottimizza l’esecuzione dei processi di lavoro dell’intero stream progettuale, sincronizzando i rilasci dei diversi Agile Team che operano negli sprint identificati per il rilascio della soluzione oggetto dello stream.

- **System Architect (SA)** – Disegna l'architettura tecnica della soluzione, progetta le sue componenti e sottosistemi primari, identifica le interfacce e le interazioni tra di esse, determina i requisiti non funzionali.
- **Agile Team** – *Progetta, implementa, effettua il test ed il roll-out dell'incremento di prodotto* della soluzione come previsto nell'ambito dello sprint ad esso assegnato. E' composto da: (1) *Product Owner (PRO)*, che stabilisce il perimetro dei requisiti che costituiscono l'incremento di prodotto da rilasciare nell'ambito dello sprint; (2) *Scrum Master (SM)*, che guida e supporta il lavoro dell'Agile Team affinché realizzi l'incremento di prodotto determinato dal PRO; (3) *Risorse preposte allo sviluppo* dei requisiti oggetto dello sprint assegnato all'Agile Team.
- **Test e Quality Assurance (TQA)** – Effettua i test per accertare la conformità ai requisiti ed il corretto funzionamento degli incrementi di prodotto definiti per i diversi sprint, nell'ambito dei rispettivi Agile Team.

Agli stream realizzativi si affiancano **2 stream di servizi continuativi** che assicurano rispettivamente:

- **Qualificazione e Validazione delle Soluzioni e delle Integrazioni**, avente obiettivo di
 1. Supportare gli Enti preposti alla certificazione e qualificazione della interoperabilità delle soluzioni di mercato e/o custom con l'EDS ed il Gateway, nella esecuzione dei test utili allo scopo,
 2. Supportare le Regioni e le Aziende Sanitarie nel verificare il corretto funzionamento delle integrazioni dei sistemi da esse utilizzati con l'EDS ed il Gateway, sia in fase di iniziale roll-out della nuova architettura, sia successivamente in virtù dell'adozione di nuovi sistemi / integrazioni.

Nell'ambito di tale stream opera il team di Test e Quality Assurance, le cui risorse operano anche nell'ambito degli Agile Team degli sprint di rilascio dei prodotti che compongono le macro-componenti del progetto.

- **Supporto post-roll-out** per il completamento del progetto, assicurando la continuità di funzionamento e l'uso delle componenti applicative e degli ambienti infrastrutturali da parte delle Regioni e delle Strutture Sanitarie, affinché queste possano alimentare il FSE (e dunque l'EDS per il tramite del Gateway) con tutti i dati e documenti nativi digitali previsti dalle LLGG.

In tale modello operativo, il team di Program Management del MITD, supportato dal Program Management Office, provvede ad effettuare:

- La definizione delle milestones intermedie e finali e degli output attesi per i diversi stream previsti dal progetto in fase di avviamento del progetto,
- Il monitoraggio continuo dell'avanzamento dei diversi stream e dei KPI temporali e qualitativi fissati per il progetto
- La verifica dei report di esecuzione e della rendicontazione delle attività ed output prodotti nei diversi stream di progetto.

A tale team si affianca il Project Management operativo di SOGEI che, sulla base delle milestones ed output attesi definiti dal team di Program Management, provvede a pianificare, organizzare e coordinare i team e le attività esecutive finalizzate a realizzare quanto oggetto del presente piano, nonché a rendicontarne il rispettivo avanzamento.

In generale, la realizzazione delle attività oggetto del presente piano dovranno avvenire nel rispetto dei principi e regole di gestione del progetto nel seguito riassunte:

- Le Linee Guida di Attuazione del FSE e gli allegati tecnico-funzionali (Linee Guida Architetturali, Specifiche tecniche funzionali di dettaglio delle componenti Gateway, Ecosistema Dati Sanitari (EDS), Sistema di Monitoraggio e Controllo, Requisiti in tema di Cybersecurity e Privacy, Requisiti di Architettura, Infrastruttura e Gestione) sono input per gli stream del piano operativo, che sono da intendersi ivi accettati da SOGEI nella loro versione condivisa sino al 31.03.2022.
- In fase di avviamento del progetto, sarà definito congiuntamente tra il MITD e SOGEI, sentito MdS, un piano esecutivo di massima delle attività progettuali nel rispetto dei vincoli temporali più avanti indicati, in cui saranno altresì indicati gli outcomes previsti intermedi e finali. Il piano esecutivo di massima dovrà altresì definire le regole e le modalità con cui saranno organizzate le attività implementative, e la loro validazione ed accettazione da parte del MITD. Tale piano esecutivo di massima sarà oggetto di approvazione da parte del MITD.

Le attività previste nell’ambito dei singoli stream e la loro articolazione temporale è definita nell’ambito del capitolo 5 cui si rinvia per i maggiori dettagli.

3.3 Rispetto dei PRINCIPI TRASVERSALI

Di seguito l’indicazione dell’impatto di Progetto sui principi trasversali del Piano Nazionale di Ripresa e Resilienza

Do No Significant Harm

In linea con il principio del “non arrecare danni significativi” all’ambiente (“do no significant harm” - DNSH) che ispira il Programma Next Generation EU (NGEU), il Progetto non solo minimizza gli impatti ambientali indiretti ma, come illustrato al punto seguente, avrà un impatto positivo sulla tutela dell’Ambiente.

Climate and Digital Tagging

Il **Progetto** contribuisce alla diffusione dei servizi digitali e al rafforzamento della comunicazione a distanza fra PA e cittadino. Ciò contribuirà alla **diminuzione dell’utilizzo di carta** (il fascicolo sanitario elettronico contiene centinaia di milioni di referti, in sostituzione di quelli cartacei) e alla **contrazione delle emissioni di CO₂** (riduzione degli spostamenti dei pazienti per recarsi fisicamente presso studi medici o altro operatore sanitario, per es. per consulto medico, in quanto il referto è già nelle disponibilità del medico).

La natura del **Progetto** potrà avere inoltre effetto positivo sul livello di digitalizzazione nazionale avendo un impatto diretto sui servizi e sulle funzionalità messe a disposizione dei cittadini.

Equità di Genere

Il Progetto, essendo rivolto a tutti i cittadini senza alcuna distinzione, sarà eseguito nel pieno rispetto del principio dell’equità di genere.

Valorizzazione e protezione dei giovani

L’iniziativa è orientata a sviluppare nuove e più efficienti modalità di comunicazione fra la Pubblica Amministrazione e il cittadino. Il carattere innovativo del Progetto lo rende di particolare interesse per le risorse giovani, rispetto alle quali l’utilizzo di canali di comunicazione digitale contribuiranno a colmare ulteriormente le distanze.

Riduzione divari territoriali

La disponibilità di servizi online su tutto il territorio nazionale contribuisce alla riduzione dei divari territoriali all'interno del Paese. Anche l'attività di comunicazione relativa all'iniziativa verrà modulata tenendo in considerazione tale obiettivo.

4. Piano Progettuale di Dettaglio

Di seguito si riporta la descrizione della struttura del progetto, la descrizione dei contenuti degli stream / Work Package in cui lo stesso è articolato e delle sottostanti attività.

WP – Work Package	Task	Descrizione	Prodotti (Deliverables)
Realizzazione EDS: Ecosistema Dati Sanitari	Progettazione Tecnica	<p>Disegno tecnico dell'architettura e dei servizi implementati dall'EDS, comprensiva della identificazione delle risorse ed API FHIR da utilizzare allo scopo, sulla base dei requisiti forniti dal MITD e definiti di concerto con MdS.</p> <p>Valutazione e selezione delle soluzioni tecnologiche con cui realizzare l'EDS.</p>	Documento di Progettazione Software, completo di schemi e diagrammi UML.
	Implementazione Test	<p>Sviluppo della soluzione.</p> <p>Test della soluzione rilasciata: unit test, integration test, performance test, acceptance test.</p>	<p>Software rilasciato: componenti dell'EDS (C1.x).</p> <p>Piano e Report di Esecuzione dei Test.</p>
	Roll-Out	<p>Parametrizzazione delle componenti dell'EDS, e di ogni suo servizio ed elemento utile al funzionamento dell'intera architettura, in particolare: Dizionari, Codifiche, Regole di Validazione, Regole di Mapping FHIR, Servizi di Sottoscrizione Dati, Algoritmi, Profili Utente, Processi Utente.</p> <p>Attivazione ed Avviamento in esercizio; comprende la formazione a personale tecnico IT del MITD, MdS, Agenas.</p>	<p>Software attivato in esercizio.</p> <p>Manuali di installazione e configurazione dell'EDS.</p>
Realizzazione Gateway	Progettazione Software dell'Architettura Deployment	<p>Progettazione software dell'architettura e dei servizi implementati dal Gateway, comprensiva della identificazione delle risorse ed API FHIR da utilizzare allo scopo, sulla base dei requisiti forniti dal MITD e definiti di concerto con MdS.</p> <p>Valutazione e selezione delle soluzioni tecnologiche con cui realizzare il Gateway.</p>	Documento di Progettazione Software, completo di schemi e diagrammi UML.
	Implementazione Test	<p>Sviluppo della soluzione.</p> <p>Test della soluzione rilasciata: unit test, integration test, performance test, acceptance test.</p>	<p>Software rilasciato: componente Gateway (C2).</p> <p>Piano e Report di Esecuzione dei Test.</p>
	Roll-Out	<p>Deployment del Gateway, sia distribuito sulle Aziende Sanitarie e/o Regioni, sia assicurato mediante servizio centralizzato, secondo policy definite dal MITD di concerto con MdS e con le Regioni.</p> <p>Parametrizzazione delle funzioni e servizi del Gateway.</p> <p>Attivazione ed Avviamento in esercizio del Gateway; comprende la formazione a personale tecnico IT del MITD, MdS, Agenas.</p>	<p>Software attivato in esercizio.</p> <p>Manuali di installazione e configurazione del Gateway.</p>
Realizzazione Servizi di Integrazione	Progettazione Specifiche Integrazione	<p>Definizione specifiche tecniche di integrazione del Gateway e dell'EDS, rispettivamente con sistemi produttori di dati e documenti e con sistemi consumatori di dati: sistemi cartella MMG/PLS, sistemi delle strutture sanitarie, sistemi di telemedicina.</p> <p>Definizione delle specifiche tecniche di integrazione dell'EDS e del Gateway con i sistemi nazionali: ANA, Sistema TS, INI, Registry Nazionale, Anagrafe Consensi, Anagrafe Deleghe, Portale Nazionale FSE.</p>	<p>Documento Specifiche Tecniche delle Integrazioni del Gateway con Sistemi Produttori di Dati e Documenti (interfacce swagger) e con INI.</p> <p>Documento Specifiche Tecniche delle Integrazioni del Layer dei Servizi con Sistemi Consumatori di Dati.</p> <p>Documento Specifiche Tecniche delle Integrazioni dell'EDS e del Gateway con i Sistemi Nazionali.</p>

WP – Work Package	Task	Descrizione	Prodotti (Deliverables)
Qualificazione e Validazione Soluzioni ed Integrazioni	Implementazione e Test	Realizzazione e test delle integrazioni dell'EDS e del Gateway con sistemi produttori/consumatori di dati e con i sistemi nazionali.	Software rilasciato: servizi di integrazione (C3.x). Piano e Report di Esecuzione dei Test.
	Roll-Out	Configurazione ed attivazione delle integrazioni con sistemi produttori/consumatori di dati e con i sistemi nazionali.	Manuali di installazione e configurazione delle integrazioni.
Attivazione Ambienti Infrastrutturali	Qualificazione Soluzioni	Supporto agli Enti preposti (Agenas) alla esecuzione delle attività di test e certificazione del corretto funzionamento della interoperabilità con il Gateway e l'EDS da parte delle soluzioni di mercato e/o custom, per la loro qualificazione.	Documento dei Casi d'Uso / di Test per la Qualificazione delle Soluzioni. Report di esecuzione dei casi di test.
	Validazione Integrazioni	Supporto alle Regioni ed alle singole Aziende Sanitarie nell'effettuare le attività di configurazione, testing, validazione ed attivazione delle integrazioni dei rispettivi sistemi con il Gateway ed il Layer dei Servizi dell'EDS.	Documento dei Casi d'Uso / di Test per la Validazione dei sistemi configurati ed utilizzati dalle Regioni e dalle singole Aziende Sanitarie. Report di esecuzione dei casi di test.
Supporto Post Roll-Out per il Completamento del Progetto	Progettazione Tecnica e Dimensionamento	Progettazione tecnica e dimensionamento degli ambienti infrastrutturali di esecuzione dell'EDS e del Gateway.	Documento di Progettazione Tecnica e Dimensionamento degli ambienti infrastrutturali.
	Configurazione ed Attivazione	Configurazione ed attivazione degli ambienti di sviluppo, test, pre-produzione, produzione, qualificazione ed integrazione, su infrastruttura centrale.	Servizi infrastrutturali attivati.
	Porting su PSN (Eventuale)	Migrazione in cloud, su PSN, delle componenti architettoniche laddove valutato dal MITD di concerto con MdS.	Documento studio di fattibilità per la migrazione al PSN. Software applicativo EDS e Gateway migrato su PSN.
	Supporto Applicativo	Supporto tecnico-specialistico all'uso del software applicativo e delle sue integrazioni da parte delle Regioni e delle Strutture Sanitarie in esercizio, ed alla risoluzione di eventuali problematiche da questi rilevati. Supporto tecnico-specialistico per l'adeguamento ed aggiornamento delle configurazioni dell'EDS e del Gateway e loro servizi di integrazione. Supporto tecnico-specialistico per l'adeguamento ed aggiornamento dei Dizionari e Codifiche (sulla base di quanto stabilito dall'Ente di standardizzazione nazionale, Agenas), Regole di Validazione dei dati, Regole di Mapping FHIR, Algoritmi, ecc. Supporto tecnico-specialistico per il rilascio di nuove versioni del software applicativo. Supporto tecnico-specialistico per la verifica ed il monitoraggio delle performance del software applicativo e per effettuare eventuali azioni di fine tuning sui parametri di sistema e sull'architettura applicativa. Supposto tecnico-specialistico finalizzato alla distribuzione, aggiornamento e verifica del funzionamento delle release, delle configurazioni e policy di sicurezza applicate alle istanze containerizzate del Gateway e del middleware per la sua esecuzione, siano esse centrali, siano esse distribuite su Regioni e/o Aziende Sanitarie. Per le istanze del Gateway installate su infrastrutture tecnologiche regionali e/o aziendali rimane responsabilità di SOGEI assicurare tale supporto su tutto lo stack software e servizi contenuti nei container in cui sono in esecuzione,	Reporting periodico (bimestrale) sui servizi erogati e relativi livelli di servizio (SLA) assicurati.

WP – Work Package	Task	Descrizione	Prodotti (Deliverables)
		dal middleware alle componenti applicative, e sulla loro distribuzione.	
	Supporto per il Data Quality	Supporto tecnico-specialistico per l'analisi della qualità e completezza dei dati acquisiti, definizione degli interventi volti alla loro completa e corretta valorizzazione, ovvero diversa gestione ed utilizzo.	Reporting periodico (bimestrale) sui servizi erogati e relativi livelli di servizio (SLA) assicurati.
	Manutenzione Correttiva Adeguativa ed	Manutenzione correttiva del software applicativo per la risoluzione di anomalie e problemi segnalati da utenti o rilevati proattivamente da SOGEI. Manutenzione adeguativa del software applicativo per mantenerlo allineato ai cambiamenti dell'ambiente tecnologico.	Reporting periodico (bimestrale) sui servizi erogati e relativi livelli di servizio (SLA) assicurati.
	Supporto Sistemistico Ambienti Infrastrutturali	Supporto sistemistico sui servizi infrastrutturali che compongono gli ambienti di esecuzione del software applicativo, quali: piattaforma di Big Data, piattaforma NO SQL, Server, Storage, Blob Storage, ecc. Sono altresì compresi i servizi sistemistici per l'attuazione della business continuity e del disaster & recovery finalizzata ad assicurare la continuità operativa di ogni elemento infrastrutturale anche in caso di disastro.	Reporting periodico (bimestrale) sui servizi erogati e relativi livelli di servizio (SLA) assicurati. Reporting periodico sulle risorse infrastrutturali effettivamente utilizzate.
	Estensione dei Servizi fino a 24 ore 7 x 7	Estensione dei servizi di supporto applicativo, manutenzione correttiva del software applicativo e supporto sistemistico sugli ambienti infrastrutturali oltre la fascia oraria ordinaria di copertura di detti servizi sino a coprire 24 ore 7 giorni su 7. Tale estensione varrà per l'EDS, il Gateway ed i loro servizi di integrazione con sistemi produttori / consumatori di dati utilizzati dalle strutture sanitarie, con particolare riferimento a quelli di ambito ospedaliero e diagnostico.	Reporting periodico (bimestrale) sui servizi erogati e relativi livelli di servizio (SLA) assicurati.

Al fine di assicurare la presa in carico e la risoluzione da parte di SOGEI delle problematiche che potranno eventualmente emergere nell'uso ed integrazione delle componenti ivi previste, da parte delle Regioni e delle Strutture Sanitarie, si prevedono i seguenti canali e modalità di attivazione:

- Sistema di trouble ticketing, web-based, per la segnalazione delle problematiche rilevate da personale tecnico di Regioni e Strutture Sanitarie, piuttosto che dai produttori di soluzioni software che interoperano con le componenti oggetto del progetto.
- In considerazione del fatto che la tempestiva presa in carico di problematiche rientranti nel perimetro Sogei è assicurata dalla gestione H24 e dalla relativa control room, si prevede un canale web mail dedicato al personale tecnico delle Regioni, Strutture ed Enti Sanitari dislocati sul territorio, per la risoluzione delle problematiche rilevate in esercizio,

5. Articolazione Temporale del Progetto

In relazione alla pianificazione temporale del rilascio dei prodotti intermedi e finali previsti per il progetto, questa segue le milestones ed i target fissati dall'investimento 1.3.1 del PNRR per il potenziamento del FSE, ed in particolare:

- **Q2 2024 – completamento dell'implementazione dell'EDS e del Gateway,**
- **Q4 2024 – tutti i documenti clinici devono essere digitalmente nativi ed integrati nel FSE, ovvero nell'EDS e Gateway,**
- **Q4-2025 – l'85% dei medici di base alimentano il Fascicolo sanitario elettronico,**
- **Q2-2026 - tutte le Regioni e Province Autonome hanno adottato e utilizzano il FSE.**

Al fine di assicurare il rispetto di tali tempistiche il piano operativo fissa le seguenti principali milestones di progetto:

Milestones	Tempistica
Ambienti Infrastrutturali	
Rilascio Documento di Progettazione Tecnica e Dimensionamento dell'Infrastruttura per EDS e Gateway ¹ .	30/06/2022
Rilascio Piano Esecutivo di Massima	30/06/2022
Rilascio Ambienti Infrastrutturali (sviluppo e validazione, rilascio successivo per produzione)	30/06/2022
Gateway	
Consegna Specifiche Tecniche delle Interfacce di Integrazione del Gateway (swagger), comprensive dei servizi di indicizzazione verso INI	30/07/2022
Rilascio Prima Release in ambiente di pre-produzione, contenente le seguenti funzioni: • Validazione Sintattica e Semantica dei documenti previsti nei primi 12 mesi dalle LLGG, sulla base di un primo subset di controlli che si basino sugli attuali dizionari e schemi di codifica vigenti (definiti da implementation guide CDA2). • Collezione dei log di validazione.	30/06/2022
Rilascio Prima Release in ambiente di produzione, contenente le seguenti funzioni: • Validazione Sintattica e Semantica dei documenti previsti nei primi 12 mesi dalle LLGG, sulla base di un primo subset di controlli che si basino sugli attuali dizionari e schemi di codifica vigenti (definiti da implementation guide CDA2). • Collezione dei log di validazione.	30/09/2022
Rilascio Seconda Release in ambiente di pre-produzione, contenente tutte le funzionalità previste dalle "Specifiche tecniche di dettaglio del Gateway".	30/11/2022
Rilascio Seconda Release in ambiente di produzione, contenente tutte le funzionalità previste dalle "Specifiche tecniche di dettaglio del Gateway".	31/12/2022
Ecosistema Dati Sanitari	
Rilascio Prima Release in ambiente di pre-produzione, contenente le seguenti componenti funzionali: • Completamento Sistema di Monitoraggio e Controllo • Servizi di acquisizione dati e prima versione del Data Repository Centrale in standard FHIR.	30/11/2022
Rilascio Prima Release in ambiente di produzione, contenente le seguenti componenti funzionali: • Completamento Sistema di Monitoraggio e Controllo • Servizi di acquisizione dati e prima versione del Data Repository Centrale in standard FHIR.	31/12/2022
Rilascio Seconda Release in ambiente di pre-produzione, contenente le seguenti componenti funzionali: • Servizi e funzioni complete del Data Repository Centrale in standard FHIR • Funzioni di Policy Manager del Layer dei Servizi.	30/04/2023
Rilascio Seconda Release in ambiente di produzione, contenente le seguenti componenti funzionali: • Servizi e funzioni complete del Data Repository Centrale in standard FHIR • Funzioni di Policy Manager del Layer dei Servizi.	30/06/2023
Rilascio Terza Release in ambiente di pre-produzione, contenente le seguenti componenti funzionali: • Servizi e funzioni complete del Layer dei Servizi.	31/07/2023
Rilascio Terza Release in ambiente di produzione, contenente le seguenti componenti funzionali: • Servizi e funzioni complete del Layer dei Servizi.	30/09/2023
Completamento del Roll-Out del Sistema Complessivo e sue Integrazioni	30/06/2024

¹ Prima versione del documento di Progettazione Tecnica e Dimensionamento dell'Infrastruttura per EDS e Gateway che potrà essere aggiornata con eventuali successive modifiche ed integrazioni in corso di progettazione delle componenti applicative.

Nell'Allegato 1 al presente documento sono riportate le tempistiche previste per i primi rilasci delle singole componenti e prodotti previsti dal progetto, fermo restando il rispetto delle milestones anzi indicate.

6. Costi del Progetto

Riepilogo Generale Costi 2022-2026

	2022	2023	2024	2025	2026	Tot. senza IVA	Tot. con IVA
Supporto x Governance e Progettazione	807.792,68	3.635.067,08	3.069.612,20	323.117,07	242.337,81	8.077.926,84	9.855.070,75
Sviluppo: Implement. e Test	1.723.708,35	7.756.687,56	6.550.091,72	689.483,34	517.112,50	17.237.083,46	21.029.241,83
Supporto x Roll-Out	2.014.772,17	9.066.474,76	7.656.134,24	805.908,87	604.431,65	20.147.721,68	24.580.220,45
Supporto x Qualificazione e Validazione	302.870,16	1.362.915,74	1.150.906,62	121.148,07	90.861,05	3.028.701,64	3.695.016,00
Conduzione: Applicazioni e Ambienti Infrastrutturali (**)	-	7.161.600,97	11.473.668,88	15.705.566,22	20.705.627,72	55.046.463,79	67.156.685,82
Totale (*)	4.849.143,36	28.982.746,10	29.900.413,66	17.645.223,57	22.160.370,73	103.537.897,42	126.316.234,85

(*) Gli importi previsti nelle varie annualità posso essere rivisti all'interno del massimale riportato nella Convenzione.

(**) costo della conduzione in itinere, crescente, da tenere in considerazione in termini di copertura economica dopo il termine della presente convenzione

Nell'Allegato 1 al presente documento è riportato il dettaglio delle voci di costo per singolo componente e servizio necessario per la sua progettazione, implementazione, test e roll-out, e supporto specialistico post roll-out per l'uso del software applicativo e sue integrazioni da parte delle Regioni e delle Strutture Sanitarie sino a completamento del progetto.

7. Interrelazione con altri interventi del PNRR

Esistono dipendenze con il seguente investimento PNRR:

- Investimento 1.2 “Casa come primo luogo di cura e telemedicina” della Componente 1 “Reti di prossimità, strutture intermedie e telemedicina per l'assistenza sanitaria territoriale”, Missione 6 del PNRR, che ha come obiettivo principale il potenziamento dei servizi domiciliari, anche attraverso soluzioni di telemedicina per supportare al meglio i pazienti con malattie croniche.
- Investimento 1.1.1 “Ammodernamento del parco tecnologico e digitale ospedaliero (Digitalizzazione)” della Componente 2, Missione 6 del PNRR, per l'adozione di soluzioni innovative e tecnologicamente avanzate e il potenziamento del patrimonio digitale delle strutture sanitarie pubbliche.



CONVENZIONE PER L'AFFIDAMENTO DELLE ATTIVITÀ DI
REALIZZAZIONE E GESTIONE DELL'ECOSISTEMA DATI SANITARI (EDS)
PREVISTO DALL'INVESTIMENTO M6C2 - 1.3.1 DEL PNRR - FASCICOLO
SANITARIO ELETTRONICO – EX ART. 12 COMMA 15-QUATER DEL
DECRETO-LEGGE N. 179 DEL 2012

ALLEGATO C

PROCESSO DI PIANIFICAZIONE, RENDICONTAZIONE E
FATTURAZIONE

Allegato C – Processo di pianificazione, rendicontazione e fatturazione

pag. 2 di 16

INDICE

1.	PREMESSA	3
2.	PIANIFICAZIONE	3
2.1	CRITERI DI DEFINIZIONE PRODOTTO SERVIZIO SPECIFICO DI PERTINENZA	5
3.	RENDICONTAZIONE FUNZIONALE (RAPPORTO PERIODICO ECONOMICO FUNZIONALE)	6
4.	RENDICONTAZIONE ECONOMICO CONTABILE (RAPPORTO PERIODICO CONTABILE)	8
5.	FATTURAZIONE	9
6.	ESEMPI DI REPORTISTICA PRODOTTA DA SISTEMA	11

Allegato C - Processo di pianificazione, rendicontazione e fatturazione

pag. 3 di 16

1. PREMESSA

Il presente allegato, parte integrante e sostanziale alla presente Convenzione stipulata tra Sogei e la Presidenza del Consiglio dei Ministri, Dipartimento per la trasformazione digitale, il Ministero della Salute e l’Agenzia Nazionale per i Servizi Sanitari Regionali, definisce il processo che governa le fasi di:

- Pianificazione delle esigenze del Cliente così come definito all’articolo 9 della Convenzione, strutturate secondo le tipologie di servizio definite nei Piani operativi annuali;
- Rendicontazione periodica dello stato di avanzamento economico/funzionale delle attività svolte così come definito all’articolo 10, comma 1 lettera b) della Convenzione e strutturata secondo la Pianificazione di cui al punto precedente;
- Rendicontazione periodica contabile delle attività svolte come definito all’articolo 10, comma 1, lettera a) della Convenzione e strutturata secondo la Pianificazione di cui al primo punto;
- Fatturazione dei servizi erogati nel periodo come definito nell’articolo 18 della Convenzione e strutturata secondo la Pianificazione di cui al primo punto.

2. PIANIFICAZIONE

Le esigenze dell’Amministrazione sono raccolte nel Piano Operativo, documento in cui vengono individuati annualmente gli obiettivi da perseguire.

Il Piano Operativo è il risultato di un processo che prevede la produzione di vari output:

1. Descrizione delle attività dell’anno - contiene un testo descrittivo degli

Allegato C – Processo di pianificazione, rendicontazione e fatturazione

pag. 4 di 16

obiettivi da raggiungere nell'anno ed in particolare:

- Prodotti/Servizi Specifici di pertinenza costruiti secondo i criteri delineati nel successivo paragrafo 2.1 comprensivi di tutti i Servizi, ed eventuali beni da acquisire;
- Servizi Professional;
- Beni e servizi a rimborso da acquisire;
- Servizi base di conduzione e non, in termini di volumi attesi.

2. Analisi dei costi per la determinazione degli importi relativi ai PSS di pertinenza.
3. Riepilogo degli impegni economici di dettaglio dell'anno per singoli obiettivi a corredo della parte testuale del Piano Operativo.
4. Tabella riepilogativa del massimale annuale ripartito per natura di remunerazione.
5. Documento di definizione dei Livelli di Servizio specifici del Cliente.

L'approvazione da parte dell'Amministrazione di tale documentazione rappresenta la formalizzazione degli impegni contrattuali e trova corrispondenza nei sistemi gestionali Sogei, da cui viene prodotta anche tutta la successiva documentazione, nonché nei corrispondenti sistemi gestionali dell'Amministrazione nei quali dovrà essere acquisita e corredata con tutte le informazioni per le relative attività di monitoraggio, riscontro e liquidazione nonché per la redazione dell'allegato al decreto giuridico di impegno alla spesa per ciascun esercizio finanziario.

Elemento chiave dell'organizzazione del Piano Operativo e di tutti i documenti fondamentali del processo in esame, è l'attribuzione di un codice univoco effettuata dal sistema Sogei a:

- PSS di pertinenza ed agli oggetti di pagamento in esso contenuti,

Allegato C - Processo di pianificazione, rendicontazione e fatturazione

pag. 5 di 16

- cosiddetti Punti di piano (tutte le attività non organizzate in PSS ed agli obiettivi in cui questi sono declinati),
- Servizi di base,
- obiettivi di acquisizione di Beni e servizi a rimborso.

Rispetto alla prima versione di Piano Operativo oggetto di approvazione, possono essere gestite delle varianti il cui iter approvativo farà riferimento ai codici di cui sopra per una determinazione chiara della richiesta.

2.1 CRITERI DI DEFINIZIONE PRODOTTO SERVIZIO SPECIFICO DI PERTINENZA

I Prodotti/Servizi Specifici di pertinenza rappresentano una vista progettuale delle attività da svolgere per raggiungere un obiettivo e presentano una serie di vantaggi:

- consentono una maggior condivisione degli obiettivi fra le parti coinvolte;
- richiedono una pianificazione attenta da parte del cliente;
- consentono a Sogei una miglior organizzazione del lavoro.

I passi per la definizione dei PSS di pertinenza sono:

- delineare gli obiettivi attesi anche al fine della determinazione degli specifici livelli di servizio per la misurazione delle performance del PSS stesso;
- esprimere requisiti progettuali, funzionali e non funzionali, qualitativi e temporali chiari;
- dimensionare l'impegno anche economico relativamente ai Servizi necessari per raggiungere l'obiettivo sulla base dei corrispettivi previsti e degli eventuali beni necessari;

Allegato C – Processo di pianificazione, rendicontazione e fatturazione

pag. 6 di 16

- fissare un prezzo corrispondente agli elementi oggetto di pagamento individuati (un output concreto, un servizio mensile fisso, dei “pezzi” gestiti...).

La descrizione del contenuto del PSS è riportata nel Documento di cui al punto 1 del paragrafo 2 ed è corredata di tutte le informazioni utili ai fini di un’analisi economica del PSS che viene invece declinata nel documento di cui al punto 2 del medesimo paragrafo.

In fase di definizione del PSS possono essere individuati eventuali livelli di servizio specifici del PSS orientati alla misurazione delle performance del prodotto finale. I livelli di servizio definiti potranno richiedere un periodo permettere a punto la modalità di rilevazione nonché un periodo di sperimentazione.

L’attuazione del PSS di pertinenza è oggetto di continuo monitoraggio sia da parte della Società che dell’Amministrazione; il sopravvenire di elementi di variazione delle esigenze che hanno portato alla definizione del PSS di pertinenza richiedono una nuova valutazione dello stesso in tutti i suoi aspetti ed una eventuale sua rimodulazione.

Si specifica che i progetti basati interamente sul Servizio di Sviluppo software verranno erogati come PSS di pertinenza.

3. RENDICONTAZIONE FUNZIONALE (RAPPORTO PERIODICO ECONOMICO FUNZIONALE)

Sulla base della periodicità concordata tra Società e Amministrazione, verrà predisposto un prospetto analitico sullo stato di avanzamento economico-

Allegato C - Processo di pianificazione, rendicontazione e fatturazione

pag. 7 di 16

funzionale e le eventuali variazioni in termini di obiettivi, volumi, date e/o di impegni economici concordati. Il prospetto è strutturato e riporta i codici identificativi secondo lo schema già descritto nel paragrafo precedente e conterrà la situazione alla “data” dello stato avanzamento lavori e dello stato avanzamento economico; un esempio di schema prodotto da sistema viene riportato in Tabella A.

Il rendiconto funzionale dovrà essere trasmesso periodicamente secondo la tempistica condivisa tra le Parti.

Resta inteso che, qualora il termine ultimo previsto per la trasmissione dei dati di interesse cada in concomitanza di giorni non lavorativi o festività infrasettimanali, tale termine dovrà intendersi automaticamente posticipato al primo giorno lavorativo utile.

Di seguito si riportano le principali informazioni:

- Area,
- Codice Progetto (da Piano Triennale dell’Amministrazione),
- Codice e nome punto di piano – codice univoco dell’intervento del Piano Operativo che potrà essere di tipo PSS di pertinenza, Servizio di base, Servizi professional a TS o BS etc.,
- Codice e nome elemento di dettaglio:
 - identificativo del singolo rilascio, se si tratta di PSS di pertinenza e di Servizi di base,
 - identificativo del codice obiettivo se si tratta di Servizi professional remunerati a TS,
 - BS per beni e servizi,

Allegato C – Processo di pianificazione, rendicontazione e fatturazione

pag. 8 di 16

- NS per note spese di missione,
- Quantità/volumi pianificati per i PSS di pertinenza e per i Servizi di base e giorni per le attività che ricadono nell’ambito dei Servizi professionali,
- Importi corrispondenti,
- SAL rilascio % - percentuale di avanzamento,
- Note - per evidenziare eventuali dati di dettaglio o criticità,
- Stato dell’obiettivo o del rilascio - bozza, in corso, annullato.

Le informazioni, riversate nel sistema gestionale dell’amministrazione, saranno correlate con la Tipologia di spesa/Capitolo/impegno/.

4. RENDICONTAZIONE ECONOMICO CONTABILE (RAPPORTO PERIODICO CONTABILE)

Al termine di ciascun quadri mestre vengono rilevati dai sistemi di rendicontazione propri di Sogei i consuntivi del periodo per le diverse tipologie di remunerazione:

- timesheet per il Tempo e Spesa;
- consuntivo di volumi, pezzi prodotti o canoni per PSS di pertinenza e per Servizi di base;
- beni e servizi effettivamente installati nel periodo;
- beni e servizi a rimborso contabilizzati;

da cui viene predisposto il Riepilogo.

La rendicontazione economico contabile, di cui le Tabelle B, C, D, E ed F rappresentano un esempio, è composta dai seguenti prospetti:

Allegato C - Processo di pianificazione, rendicontazione e fatturazione

pag. 9 di 16

- a) "Ordini di vendita dei Servizi" di avanzamento economico per Servizi professional remunerati a TS, PSS di pertinenza e Servizi di base,
- b) "Ordini di vendita dei B&S" relativa ai beni già consegnati o installati ed ai servizi già prestati o in corso di prestazione,
- c) Collaudo B&S a rimborso contiene l'esito dei collaudi eseguiti sui fornitori terzi,
- d) Penali fornitori è il prospetto che riporta eventuali penali applicate a fornitori terzi per inadempienze contrattuali. Tale importo viene accreditato con l'emissione di una apposita nota di credito per riversamento penali applicate a fornitori e relativa documentazione a corredo,
- e) Dettaglio beni ad installazione è il prospetto che elenca le apparecchiature hardware acquistate da Sogei per nome e per conto dell'Amministrazione installate nel periodo presso i loro uffici.

Il Cliente ha tempo 30 giorni per verificarne, mediante sistema gestionale che consenta tale riscontro, il contenuto e richiedere chiarimenti o eventuali rettifiche, che comporteranno un'interruzione dei termini e, all'esito positivo, procedere all'approvazione. Allo scadere dei 30 giorni o ad approvazione del Rapporto quadrimestrale la Società potrà procedere alla fatturazione in coerenza con gli OdV inviati.

5. FATTURAZIONE

L'acconto viene calcolato secondo quanto specificato all'articolo 18 comma 1 della Convenzione.

Allegato C – Processo di pianificazione, rendicontazione e fatturazione

pag. 10 di 16

La fatturazione dei servizi erogati avviene attraverso l'emissione delle fatture di conguaglio quadrimestrali sulla base dei consuntivi del periodo.

Al termine di ciascun quadri mestre la Sogei predispone ed invia gli OdV di consuntivo del periodo così come descritto nel paragrafo precedente per le diverse tipologie di remunerazione:

- timesheet per i Servizi professionali remunerati a TS;
- consuntivo di volumi o pezzi prodotti per PSS di pertinenza e per Servizi di base;
- beni e servizi effettivamente installati nel periodo;
- beni e servizi a rimborso contabilizzati.

Le fatture di conguaglio verranno emesse sulla base del consuntivo quadri mestrale approvato e dell'acconto; l'Amministrazione provvederà alla loro liquidazione entro 30 giorni dall'emissione delle fatture.

Le fatture inviate al cliente sono conservate digitalmente secondo la normativa vigente.

Tutti i documenti contabili a supporto delle fatture stesse vengono conservati e resi disponibili al cliente per eventuali verifiche.

Si fa presente che nel caso di progetti a finanziamento europeo, identificabili in modo specifico in fase di Pianificazione, verrà emessa apposita fatturazione.

Allegato C - Processo di pianificazione, rendicontazione e fatturazione

pag. 11 di 16

6. ESEMPI DI REPORTISTICA PRODOTTA DA SISTEMA

Tabella A – Esempio di Rapporto periodico economico funzionale

Contratto.....e Sogei – Periodo di riferimento gg/mm/aaaa – gg/mm/aaaa

Area	Codice progetto	Descrizione progetto	Codice sottoprogetto	Descrizione sottoprogetto	Codice PPT	Descrizione PPT	Prog ressi vo rilas cio / Codi ce obiettivo	Descrizione rilascio / obiettivo	Data inizio rilascio	Data inizio rilascio effettiva	Data disponibilità al collaudo	Data disponibilità al collaudo effettiva	Data rilascio prevista	Data rilascio effettiva
XXXXXX	Condizione	SERVER	01	IMMAGINI							
XXXXXX	Condizione	ASSISTENZA CENTRALE AGLI UTENTI	01	RICHIESTE RISOLTE DAL SUPPORTO SPECIALISTICO							
XXXXXX	Supporto xxxx	Supporto xxxx	INTERVENTO DI SUPPORTO	01	INTERVENTO DI SUPPORTO XXXXXXXX	01/01/2020			31/12/2020			
XXXXXX	Supporto xxxx	Supporto xxxx	INTERVENTO DI SUPPORTO	01	INTERVENTO DI SUPPORTO XXXXXXXX	01/01/2020			31/12/2020			
XXXXXX	Condizione	Condizione	ASSISTENZA CENTRALE AGLI UTENTI	02	RICHIESTE RISOLTE DA CUSTOMER SUPPORT							
XXXXXX	EVOLUZIONE DEL SISTEMA XXXXXX		07		04/03/2020	29/09/2020		14/10/2020			
XXXXXX	NUOVO SISTEMA YYYY		08		08/01/2020	18/02/2020	28/02/2020	13/03/2020	11/03/2020		

Allegato C – Processo di pianificazione, rendicontazione e fatturazione

pag. 12 di 16

Tabella B: Ordine di Vendita Servizi

Tipo rilascio / obiettivo	Capitolo	Quantità / Volumi pianificati	Baseline importo rilascio	Importo rilascio	Importo maturato	SAL rilascio	Note	Stato
---------------------------	----------	-------------------------------	---------------------------	------------------	------------------	--------------	------	-------

Contrattoe Sogei - Periodo di riferimento gg/mm/aaaa - gg/mm/aaaa

SEZIONE : ODV Servizi

Tipologia	MESE	PERIODO	ANNO	PERIODO COMP	ANNO COMP	Codice Servizio/Intervento	ARTICOLO	DESC ARTICOLO	UDM	QUANTITA	PREZZO	IMPORTO	Obiettivo	Attività	NUM ODV	NUM LINEA
Server	DIC	3Q	AAAA	3Q	AAAA	XXXXXX	OS consuntivo	Immagini	num	nnnnnn	€	€				
Server	DIC	3Q	AAAA	3Q	AAAA	XXXXXX	OS consuntivo	vRAM	num	nnnnnn	€	€				
Professional	DIC	3Q	AAAA	3Q	AAAA	XXXXXX	OS consuntivo	Servizio di Coordinamento	gg	nnnnnn	€	€				
Sviluppo e manutenzione evolutiva del software ad hoc	DIC	3Q	AAAA	3Q	AAAA	XXXXXX	OS consuntivo	Unità di sviluppo	FP	nnnnnn	€	€				
Sviluppo e manutenzione evolutiva del software ad hoc	DIC	3Q	AAAA	3Q	AAAA	XXXXXX	OS consuntivo	Unità non funzionali	GG	nnnnnn	€	€				
				
				

Allegato C - Processo di pianificazione, rendicontazione e fatturazione

pag. 13 di 16

Tabella C: Ordine di Vendita beni e servizi

Contratto e Sogei - Periodo di riferimento gg/mm/aaaa - gg/mm/aaaa

Sezione: ODV beni e servizi

CONT RATT O ESEC UTIV O	CAPITOLO	TIPOLOGI A	MES E	PERIOD O	ANNO	PERIODO COMP	ANNO COMP	PPT	ARTIC OLO	DESC ARTICOLO	UDM	Q.tà	Costo unitario	Totale	Repertorio	Num ODA ODL	Num ODA Linea	DESC ARTICOLO ODA	Marca	Modello	Ragione Sociale	Sede Consegnna	Voce di Spesa	Num ODV	Num Linea ODV
QC	Corrente	B&S	SET	3Q	2017	3Q	2017	600M01	A.4	SERVIZI DI MANUTENZIONE DEI BENI	Num	nn	€	€	x	Manutenzione Licenze	-	-	AAAAA S.R.L.	-	BA801	1
QC	Corrente	B&S	SET	3Q	2017	3Q	2017	600M01	A.4	SERVIZI DI MANUTENZIONE DEI BENI	Num	nn	€	€	x	Manutenz Apparecchiature periferiche	-	-	BBBBB S.R.L.	-	BB303	2
QC	Investimento	B&S	OTT	3Q	2017	3Q	2017	600M01	A.2	PRODOTTI SOFTWARE DI MERCATO	Num	nn	€	€	x	Licenza sw "....."	-	-	CCCCC S.R.L.	-	BA816	3
QC	Investimento	B&S	OTT	3Q	2017	3Q	2017	600M01	A.1	SISTEMI DI ELAB. PERIFERICI, SOFTWARE DI BASE E DI SISTEMA	Num	nn	€	€	x	STAMPANTE	fffff	hhhhh	xxxxxx		BA802	3
QC	Corrente	B&S	SET	3Q	2017	3Q	2017	600M01	A.4	

Allegato C – Processo di pianificazione, rendicontazione e fatturazione

pag. 14 di 16

Tabella D: collaudi effettuati nel periodo

Contratto e Sogei - Periodo di riferimento gg/mm/aaaa - gg/mm/aaaa

SEZIONE : collaudi effettuati nel periodo

Fornitore	Contratto	Data stipula	Descrizione	Data collaudo	Data Accettazione Certificato di Collaudo	Esito
Ragione sociale fornitore	Codice Contratto	gg/mm/aaaa	gg/mm/aaaa	gg/mm/aaaa	Positivo/Negativo

Allegato C - Processo di pianificazione, rendicontazione e fatturazione

pag. 15 di 16

Tabella E: penali fornitori

Contratto tra ..e Sogei Periodo di riferimento xx/xx/yyyy - xx/xx/yyyy			SEZIONE: penali applicate ai fornitori	
N°	DATA	SOCIETA'	CONTRATTO	IMPORTO
189	gg/mm/aaaa	XXXXXX	€ xxxx,xx
190	gg/mm/aaaa	YYYYYY	€ xxxx,xx
191	gg/mm/aaaa	ZZZZZZ	€ xxxx,xx
198	gg/mm/aaaa	AAAAAA	€ xxxx,xx

TOTALE -

Allegato C – Processo di pianificazione, rendicontazione e fatturazione

pag. 16 di 16

Tabella F: beni installati nel periodo

Contratto trae Sogei Periodo di riferimento xx/xx/xxxx - xx/xx/xxxx									SEZIONE: beni installati	
Matricola	Repertorio	VDS	Tipologia	Modello	Prezzo	Codice Ufficio	Ufficio	Località	Data Installazione	
XX76AGX06S	BA802	STAMPANTE xxxxxx	€ xxx	A-37	ROMA	gg/mm/aaaa	
....	BA802	STAMPANTE yyyy	€ xxx	gg/mm/aaaa	
....	BA802	€ xxx	gg/mm/aaaa	
....	BA802	€ xxx	gg/mm/aaaa	
....	BA802	€ xxx	gg/mm/aaaa	



CONVENZIONE PER L'AFFIDAMENTO DELLE ATTIVITÀ DI REALIZZAZIONE E
GESTIONE DELL'ECOSISTEMA DATI SANITARI (EDS) PREVISTO
DALL'INVESTIMENTO M6C2 - 1.3.1 DEL PNRR - FASCICOLO SANITARIO
ELETTRONICO – EX ART. 12 COMMA 15-QUATER DEL DECRETO-LEGGE N. 179
DEL 2012

ALLEGATO D

PROCESSO E FLUSSO DI COMUNICAZIONE PER I SERVIZI DI SVILUPPO E
PROFESSIONAL

INDICE

1.	PREMESSA	3
2.	SVILUPPO SOFTWARE.....	3
2.1	STANDARD INTERNI DI QUALITÀ	8
2.2	FASI DEL PROCESSO DI SVILUPPO	9
2.2.1	Analisi preliminare o analisi intraiterazione	10
2.2.2	Analisi dei requisiti	12
2.2.3	Progettazione	15
2.2.4	Realizzazione.....	15
2.2.5	Test	16
2.2.6	Rilascio.....	16
2.3	VERIFICA DI CONFORMITÀ.....	17
2.4	ESTENSIONE.....	18
2.5	FLUSSO DI COMUNICAZIONE E DOCUMENTAZIONE PER SVILUPPO SOFTWARE.....	18
3.	SERVIZI PROFESSIONAL	20

1. PREMESSA

Il presente allegato è parte integrante e sostanziale della Convenzione stipulata tra Sogei e la Presidenza del Consiglio dei Ministri, Dipartimento per la trasformazione digitale, il Ministero della Salute e l'Agenzia Nazionale per i Servizi Sanitari Regionali.

Di seguito vengono descritti:

- il processo messo in atto nell'ambito del Servizio di sviluppo ed evoluzione del Sistema Informativo e del Servizio Professional;
- la documentazione ed i processi di comunicazione per tali Servizi.

2. SVILUPPO SOFTWARE

Lo sviluppo di soluzioni software è correlato all'esigenza dell'Amministrazione di nuove applicazioni, mentre le manutenzioni evolutive sono connesse all'esigenza di far evolvere le applicazioni già in esercizio, anche a seguito di variazioni normative e regolamentari.

L'applicazione è una collezione integrata di procedure automatizzate e dati che forniscono supporto ad un obiettivo applicativo ed è formata da uno o più componenti, moduli, o sottosistemi.

L'applicazione viene realizzata con uno sviluppo ad hoc oppure mediante la parametrizzazione e personalizzazione di pacchetti software acquistati dal mercato.

In entrambi i casi le attività di sviluppo e manutenzione evolutiva vengono condotte adottando le metodologie così come descritto nell'Allegato A; qualsiasi sia la metodologia messa in campo, individuata in funzione della maggior adeguatezza al contesto da trattare, il processo logicamente seguito risulta il medesimo.

Il processo di sviluppo descritto di seguito si adatta alla naturale evoluzione dei requisiti che si sperimenta nel contesto dell'ingegneria del software e all'esigenza di far emergere questa natura evolutiva il prima possibile nel ciclo di sviluppo per abbattere i costi delle modifiche sul prodotto. L'instabilità dei requisiti, insita nello sviluppo del software, è presente anche nel particolare contesto in cui la Società opera, caratterizzato da requisiti che possono variare o si aggiungono nel corso della realizzazione dell'obiettivo. Un esempio di contesto con requisiti non ben definiti all'inizio della realizzazione è l'attuazione di normative i cui

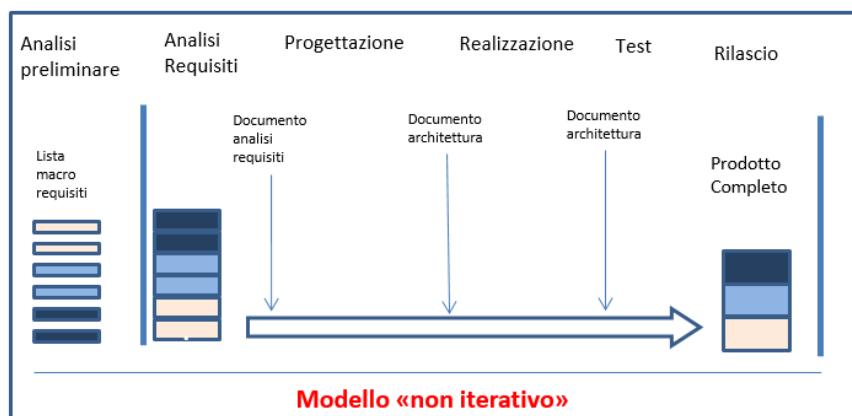
dettagli attuativi vengono definiti attraverso decreti, circolari etc. a ridosso della data di disponibilità del servizio stesso.

Per venire incontro a tale esigenza si è definito un processo software flessibile in cui le fasi sono sostanzialmente quelle definite nei paragrafi successivi, eseguite in modo ciclico man mano che i requisiti si chiariscono e, in alcuni casi, anche in sovrapposizione.

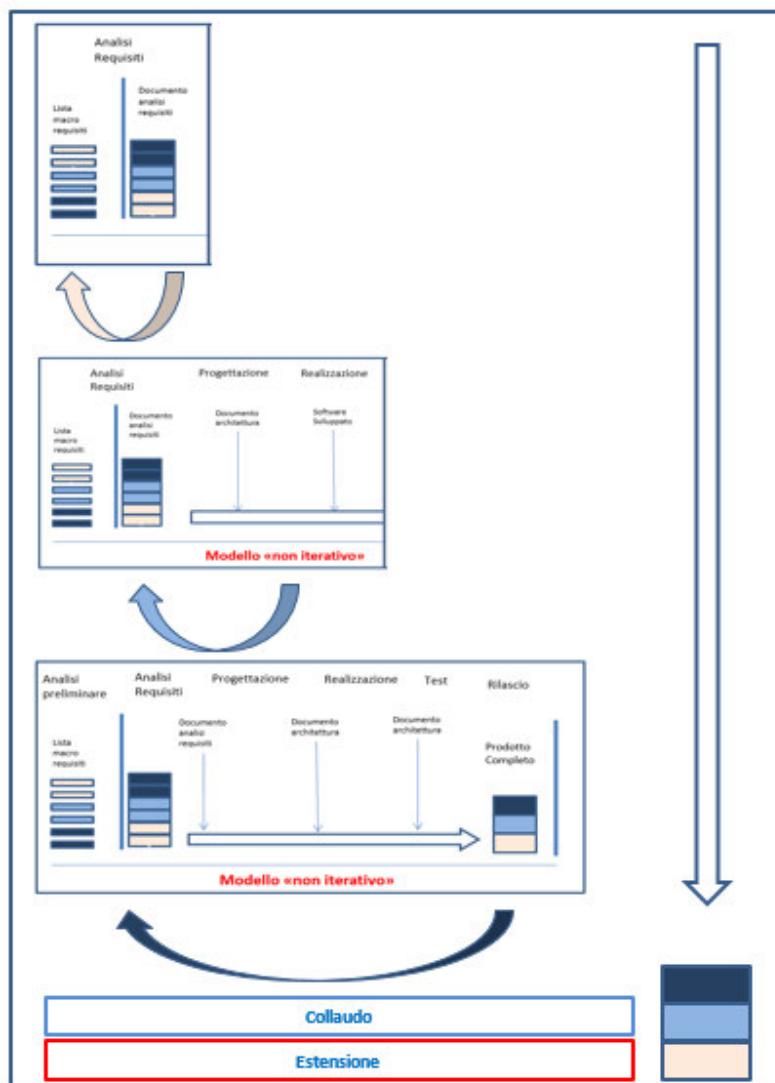
Lo sviluppo si può sostanziare in un unico rilascio dell'applicazione oppure in rilasci intermedi di software, nel primo caso le attività si sostanziano in un unico passaggio attraverso le diverse fasi (con eventuali ricicli tra fasi) mentre nel secondo in più “iterazioni” per cui ciascuna “iterazione” corrisponde ad un sottoinsieme di requisiti rilasciabili in maniera indipendente e valutabili dall'Amministrazione. Nel caso di sviluppo a modello “iterativo”, il rilascio dell'ultima “iterazione” corrisponde ovviamente al rilascio dell'applicazione. Nel caso di sviluppo a modello “non iterativo” l'Amministrazione viene coinvolta dalla fase iniziale di definizione dei requisiti fino a loro completa approvazione e quindi ad una situazione di sostanziale stabilità. Tale modalità di sviluppo è caratterizzata comunque dalla possibilità di effettuare ricicli tra fasi o nell'ambito della stessa fase; i ricicli sono attivati da verifiche di qualità degli output (quality checkpoint) della fase stessa. Ad esempio in fase di analisi dei requisiti un checkpoint può essere il prototipo dell'interfaccia che innasca un riciclo all'interno della fase stessa; oppure in fase di sviluppo il prototipo funzionante evidenzia un nuovo requisito che implica un riciclo partendo dalla fase di analisi.

Questo modello, pur avendo il vantaggio di avere dei requisiti stabili fin dall'inizio del ciclo di sviluppo espone al rischio che emergano alcune modifiche ai requisiti in una fase avanzata del ciclo di sviluppo e quindi la relativa gestione comporta dei costi significativi.

In figura 1 si riporta in modo schematico il modello appena descritto:

Figura 1: modello “non iterativo””

L’evoluzione del processo stesso è descritta invece in figura 2 dove si evidenzia il riciclo tra fasi e il costo sempre maggiore a seconda della tardività in cui emerge il cambiamento richiesto:

Figura 2 : richiesta di modifica nel modello "non iterativo"

Nel caso di sviluppo a modello “iterativo” (adatto all’utilizzo con alcuni framework di tipo “agile”) la particolarità è data da un rapporto continuativo con l’Amministrazione per definire in itinere i macrorequisiti e le loro priorità e fare una valutazione immediata della parte di prodotto relativa alla singola “iterazione”. Ogni “iterazione” è caratterizzata dal passaggio di ciascuna fase del processo così come descritto successivamente. Per ogni “iterazione” viene individuato un sottoinsieme di requisiti da implementare con un livello di qualità paragonabile a quello di un rilascio in esercizio. Il modello “iterativo” permette di affrontare in modo più immediato i requisiti ed eventuali integrazioni/variazioni degli stessi man mano che emergono minimizzandone i relativi costi; ciò è determinato anche dal costante coinvolgimento dell’Amministrazione che, fornendo alla *Società* feedback costanti, permette un migliore allineamento con le sue esigenze di business.

In figura 3 si riporta il processo per quanto riguarda l’evoluzione di una singola “iterazione”:

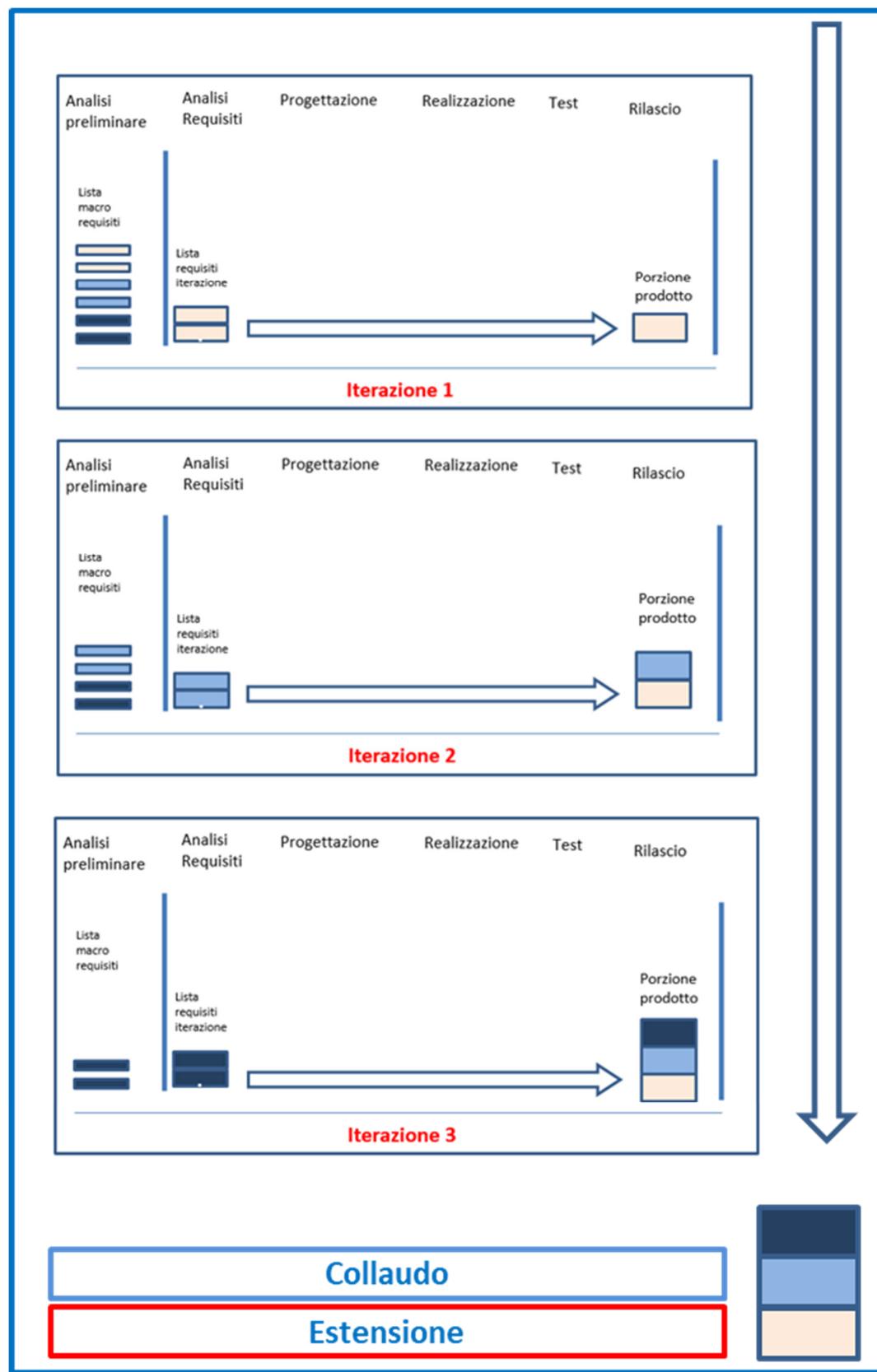
Figura 3: singola “iterazione” in un modello “iterativo”



In questo modello, come detto, per ogni “iterazione” viene gestito un sottoinsieme dei requisiti e questo sottoinsieme passa per tutte le fasi del processo produttivo.

L’evoluzione del processo di sviluppo stesso è descritta invece in figura 4 dove si evidenzia la gestione delle modifiche nel modello a “iterazioni”.

Figura 4: evoluzione modifiche in un modello "iterativo"



In questo caso le modifiche vengono esaminate alla fine di ogni “iterazione” ed eventualmente, se ritenute prioritarie, lavorate nell’“iterazione” successiva mitigando il

rischio di modifiche emergenti in fase molto avanzata del processo di sviluppo.

2.1 STANDARD INTERNI DI QUALITÀ

Indipendentemente dal processo di sviluppo attuato, la *Società* adotta standard interni ad alto livello per la verifica della rispondenza ai requisiti non funzionali di qualità:

Caratteristica ISO 25010	Sottocaratteristiche associate
Idoneità funzionale	Completezza Funzionale
	Correttezza Funzionale
Efficienza delle prestazioni	Comportamento Temporale
	Capacità
	Efficienza Strutturale
Compatibilità	Interoperabilità
Usabilità	Usabilità
	Accessibilità
Affidabilità	Tolleranza ai guasti
	Affidabilità Strutturale
Sicurezza	Riservatezza
	Autenticità
	Responsabilità
	Sicurezza
Manutenibilità	Modularità
	Riutilizzabilità
	Testabilità
	Manutenibilità
Portabilità	Adattabilità front end
	Adattabilità back end

Tali standard sono espressi in forma di procedure interne che determinano, a seconda della criticità del servizio o della tipologia di intervento, quale debba essere la copertura e la profondità di queste verifiche. In generale le verifiche che possono essere svolte su un servizio o intervento sono:

- verifiche di qualità dei dati,
- attività di analisi delle misure di sicurezza e privacy in materia di GDPR,
- verifiche dei requisiti di carico, dimensionamento e performance nel processo di capacity planning e nei successivi benchmark,
- verifica della qualità del codice, attraverso l’analisi statica condotta in modo sistematico su quanto prodotto,
- analisi del codice prodotto con test dinamici,
- test di sicurezza, tra cui i Web Application Penetration Test,
- test di integrazione delle componenti software e di sistema,
- test dei servizi di monitoraggio per verificare il funzionamento completo dei sistemi in cui verrà fatto il deploy.

Al fine di garantire le medesime performance anche lo sviluppo di siti nell’ambito del “Servizio sito/portale web e componenti accessori”, se pur venduto in diversa modalità, è soggetta agli stessi controlli di qualità e sicurezza nell’ambito del ciclo produttivo Sogei. Particolare interesse sarà riservato alla qualità in uso dei Servizi ICT messi a disposizione degli utenti finali; la Società e l’Amministrazione collaboreranno per individuare idonei indicatori da misurare e valutare anche attraverso indagini di Customer satisfaction rivolte ai medesimi utenti.

2.2 **FASI DEL PROCESSO DI SVILUPPO**

Le fasi del processo relative ad un obiettivo di sviluppo si articolano in:

- analisi preliminare o analisi intrainterazione;
- analisi dei requisiti;
- progettazione;

- realizzazione;
- test;
- rilascio.

2.2.1 ***Analisi preliminare o analisi intraiterazione***

Tale fase, richiesta in caso di uno sviluppo “iterativo”, nella prima “iterazione” ha lo scopo di identificare una lista completa dei macrorequisiti funzionali e non funzionali mentre, nelle “iterazioni” successive alla prima, comporta la revisione della lista in base a quanto prodotto nell’“iterazione” precedente.

Nell’analisi preliminare vengono messi in evidenza macro requisiti il cui dettaglio sia sufficientemente chiaro ad avere una comprensione completa sia per l’Amministrazione che per la *Società* e con un livello di granularità adeguato alle informazioni disponibili all’inizio del progetto. A tal fine potrebbe essere utile:

- effettuare interviste agli utenti;
- esaminare la documentazione eventualmente già disponibile in tale ambito;
- esaminare il contesto amministrativo e organizzativo in cui si inserisce l’automazione;
- esaminare gli aspetti relativi alla qualità, alla sicurezza e alla privacy.

Le attività da svolgere sono:

- individuazione requisiti di alto livello e ordinamento per priorità secondo logiche concordate con l’Amministrazione;
- definizione dell’architettura target che guiderà le scelte implementative;
- identificazione dei principali dati di business, della loro categoria privacy e del loro trattamento e finalità dello stesso;
- eventuale definizione e condivisione del piano di massima delle release in funzione dei requisiti di alto livello da rendere disponibili in ambiente di produzione; a tale livello il piano potrebbe non comprendere tutti i macrorequisiti; nel caso di software ad hoc la definizione del piano si avverrà del risultato di una stima della dimensione

del software fatta attraverso metriche compatibili con gli standard ISO di riferimento (quali ad esempio ISO/IEC 14143-1:2007 e ISO/IEC 25010);

- individuazione della durata delle singole “iterazioni” nell’ambito delle release con l’indicazione del sottoinsieme di requisiti relativi alle prime “iterazioni” individuati.

I principali output dell’analisi preliminare sono:

- la lista dei macrorequisiti e le loro priorità e le caratteristiche principali dell’architettura target su cui verranno implementati;
- l’eventuale piano delle release di produzione, se si tratta di un obiettivo che necessita di più rilasci in produzione;
- l’individuazione di almeno la prima “iterazione” di requisiti da avviare.

L’analisi preliminare necessita di un coinvolgimento forte dell’Amministrazione proprio per una piena condivisione dell’impianto e accettazione di quanto stabilito prima dell’avvio della fase successiva.

Per ciascuna “iterazione” successiva, l’analisi intraiterazione consiste nel riesame della lista dei macrorequisiti ed in ogni altro elemento analizzato e valutato in accordo con l’Amministrazione prendendo in considerazione anche i feedback emersi nel corso della verifica delle “iterazioni” di rilascio già consegnate.

Le attività da svolgere sono:

- la valutazione di eventuali cambiamenti alla lista dei requisiti (funzionali e non funzionali) e, nel caso ci siano requisiti modificati, aggiunti oppure cancellati, si rivede, in accordo con l’Amministrazione, l’ordine di priorità degli stessi;
- l’identificazione dell’insieme dei requisiti (funzionali e non funzionali) che andranno sviluppati nell’“iterazione” di riferimento;
- eventuale verifica dell’effort dell’obiettivo in caso di cambiamenti significativi dei requisiti (funzionali e non funzionali). Le modalità con le quali verrà stimato l’effort relativo saranno le stese descritte per l’analisi dei requisiti.

Gli output della revisione dei requisiti (funzionali e non funzionali) sono:

- la lista dei requisiti in ordine di priorità aggiornata;

- il sottoinsieme dei requisiti da implementare nell’”iterazione” di riferimento.

Anche questa fase prevede il coinvolgimento dell’Amministrazione che dovrà confermare la nuova lista dei requisiti e le relative priorità.

Nel caso di sviluppo nel modello “non iterativo”, molte delle attività previste dalla fase preliminare, vengono effettuate nella fase di analisi dei requisiti descritta successivamente; l’analisi intraiterazione è una attività che può scaturire da verifiche intermedie dell’obiettivo nel corso di qualsiasi fase del ciclo produttivo.

2.2.2 *Analisi dei requisiti*

La fase di analisi dei requisiti ha lo scopo di analizzare il dominio del problema per l’”iterazione” in considerazione, raccogliendo e dettagliando tutti i requisiti funzionali e non funzionali, che diventeranno elementi di qualità specifici per quel servizio, al fine di arrivare a condividere con l’Amministrazione la soluzione proposta.

Tale fase prende in input l’insieme di requisiti selezionati per l’”iterazione” corrente, li completa fino a raggiungere un livello di dettaglio adeguato ad avere l’approvazione dell’Amministrazione.

Le attività previste sono:

- analisi di dettaglio dei requisiti funzionali e non funzionali e dei dati di business, anche curando gli aspetti della qualità e della sicurezza;
- disegno del modello concettuale dei dati;
- eventuale prototipazione dell’interfaccia tenendo conto anche di aspetti di accessibilità e usabilità;
- progettazione del piano di test coerente con i requisiti identificati;
- classificazione del Servizio se trattasi di sviluppo;
- nel caso di sviluppo a modello “non iterativo”: identificazione dei principali dati di business, della loro categoria privacy e del loro trattamento e finalità dello stesso;
- nel caso di sviluppo a modello “iterativo”: eventuale revisione di quanto definito in fase di analisi preliminare riguardo il trattamento dei dati ai fini della privacy;

- nel caso di manutenzioni evolutive, le attività descritte sono accompagnate dall’individuazione delle applicazioni coinvolte, al fine di identificare le funzionalità da creare/modificare/cancellare in relazione alle esigenze espresse.

Gli output della fase di analisi dei requisiti sono:

- i requisiti funzionali e non funzionali e la loro fattibilità, gli impatti dell’automazione proposta sui processi tecnico-organizzativi preesistenti;
- il disegno del modello concettuale dei dati;
- la proposta di automazione, con la descrizione delle funzionalità individuate e i principali dati coinvolti;
- il piano di test da verificare e completare con i casi di test eseguiti ed il loro esito da utilizzare per la verifica del rilascio;
- nel caso di sviluppo a modello “non iterativo” eventuale predisposizione di prototipi finalizzati a migliorare la definizione dei requisiti ed a consentire la validazione della soluzione proposta.

I risultati delle attività svolte durante la fase di analisi dei requisiti di un “iterazione” vengono formalizzati nei documenti:

- ‘Analisi dei Requisiti’ se si tratta di sviluppo o ‘Specifiche di Intervento di MEV’ se si tratta di evolutiva in cui è ricompreso il Piano dei test;
- documento ‘Misure Sicurezza e Privacy del Servizio ICT’, se necessario in base alla natura dei dati trattati ai fini della riservatezza e privacy.

Nel caso di sviluppo a modello “non iterativo”, qualora si ritenga che i requisiti abbiano un livello di stabilità adatto ad un’approvazione formale, il documento di analisi può essere rilasciato in approvazione all’Amministrazione. Qualora invece, i requisiti non fossero ritenuti consolidati il documento sarà redatto in bozza e condiviso in diverse versioni con l’Amministrazione fino al raggiungimento del livello di stabilità sopra definito.

Il documento ‘Misure Sicurezza e Privacy del Servizio ICT’ seguirà lo stesso flusso di consegna descritto per il documento di Analisi dei requisiti.

Nell’ambito di sviluppo a modello “iterativo”, entrambi i documenti verranno condivisi con

l'Amministrazione in versioni diverse in coerenza con la consegna delle "iterazioni" e saranno adeguati ad ogni integrazione o variazione derivante dall'esito delle verifiche svolte sulle singole "iterazioni". La validazione dell'"iterazione" da parte dell'Amministrazione costituirà accettazione dell'"iterazione" stessa e della relativa documentazione. Al completamento dell'ultima "iterazione" i documenti saranno oggetto di invio formale e, in particolare, costituiranno il riferimento per la Verifica di Conformità.

Qualora, nell'ambito dello sviluppo a modello "non iterativo", intervenissero variazioni di requisiti successivamente alla formalizzazione e approvazione del documento di Analisi dei requisiti, sarà necessario rivalutare l'intervento in termini di effort e tempi e procedere alla modifica in corso d'opera riaprendo la fase di analisi dei requisiti.

2.2.2.1 Completezza dei requisiti

È importante sottolineare l'importanza che riveste il livello di dettaglio che hanno i requisiti in una determinate fase dello sviluppo dei requisiti, in particolare il relativo impatto sulla misurazione del software il cui dettaglio dipenderà dalla completezza del requisito in un dato momento e dalla natura del requisito che si intende misurare.

Nel caso di requisito funzionale, soprattutto in processi iterativi, saranno definiti inizialmente dei macrorequisiti poco dettagliati; in questa fase la misura sarà molto approssimata e, in alcuni casi, scarna di alcuni elementi di dettaglio che potranno essere definiti successivamente (ad es individuazione puntuale dei det di un processo elementare nel caso dei function point).

Nel caso del requisito non funzionale ciò è maggiormente accentuato: la natura tecnica dell'implementazione del requisito non funzionale comporta infatti una stabilità in un momento successivo rispetto al requisito funzionale soprattutto ove sia necessario un certo livello di dettaglio. Probabilmente, la maturità nella soluzione che risponde ad un requisito non funzionale, si avrà solo nella fase di progettazione, anche se già nell'analisi dei requisiti si potrà disporre di informazioni per farne una stima di alto livello.

Ad esempio e in particolare riferendosi alle sottocategorie SNAP, l'analisi di dettaglio potrà essere effettuata solo nel momento in cui il requisito non funzionale avrà definita una soluzione completa. Mentre nella fasi precedenti sarà possibile effettuare solo delle stime,

anche molto approssimative, ove solo alcune volte sarà possibile indicare almeno le relative sottocategorie che maggiormente contribuiscono alla stima stessa, senza poter disporre di una misurazione puntuale.

2.2.3 ***Progettazione***

Indipendentemente dal modello metodologico di riferimento adottato, i requisiti funzionali e non funzionali individuati sono trasformati in caratteristiche specifiche del software da realizzare; la progettazione definisce, infatti, il disegno del servizio e come esso debba essere realizzato.

La progettazione consiste in:

- nel caso di sviluppo a modello “non iterativo”, progettare l’architettura, se si tratta di uno sviluppo o evoluzione con impatto architettonico;
- nel caso di sviluppo a modello “iterativo”, adeguare la progettazione dell’architettura target con i dettagli emersi nell’analisi dei requisiti dell’”iterazione”;
- progettazione componenti applicative e, in caso di sviluppo, dell’infrastruttura di sistema e di sicurezza;
- progettazione interfaccia e del modello della base dati (logico e fisico);
- completamento del piano di test con la progettazione dei casi di test da effettuare per requisiti non funzionali.

L’output di tale fase è il documento di progettazione. Per progetti in cui la scelta tecnologica implica forti impatti economici organizzativi sull’Amministrazione, la documentazione sarà oggetto di approvazione da parte di quest’ultima.

2.2.4 ***Realizzazione***

La fase di realizzazione ha come scopo la produzione dei singoli componenti del software o la personalizzazione del software di mercato in rispondenza ai requisiti stabiliti nell’”iterazione”, specifica, in considerazione.

Le attività prevedono:

- realizzazione delle funzionalità, delle base dati e, ove necessario, bozza della documentazione utente a corredo;
- esecuzione del test applicativo o unit test ed eventuale verifica statica del codice.

L'output di tale fase è il completamento del software relativo all'"iterazione", specifica, in considerazione.

2.2.5 **Test**

La fase di test comprende le attività di verifica funzionale e non funzionale del software realizzato in ambiente di test e di validazione.

Il test viene attuato mediante gli strumenti più idonei e dipende dalla metodologia utilizzata per il processo di sviluppo.

In particolare in ambiente di test saranno eseguiti:

- test funzionali, non funzionali e di integrazione e in ogni caso tutti i test necessari applicabili in tale ambiente;
- verifiche di accessibilità e usabilità, se trattasi di sviluppo ad hoc.

In ambiente di validazione saranno eseguiti:

- test di carico, di sistema e di sicurezza, ed ogni altro test e verifica necessari in tale ambiente.

L'output di tale fase è il software relativo all'"iterazione", specifica, verificato.

2.2.6 **Rilascio**

La fase comprende tutte le attività necessarie per rilasciare il software realizzato e tutti i prodotti ad esso collegati; tale fase prevede attività diverse se si tratta del rilascio di un'"iterazione" intermedia oppure dell'ultima "iterazione" o dell'unica "iterazione" sviluppato.

Al termine della fase di test il software ha caratteristiche qualitative tali da poter essere trasferito in ambiente di produzione. Inizialmente verrà messo a disposizione dell'Amministrazione in ambiente di validazione per le opportune verifiche degli utenti.

Se si tratta di sviluppo a modello "iterativo" e l'"iterazione" rilasciata non è l'ultima,

l’Amministrazione potrà procedere alle verifiche in collaborazione con la *Società* e restituire alla *Società* i feedback utili al perfezionamento dell’applicazione. I feedback verranno utilizzati nella fase di revisione della lista requisiti dell’”iterazione” successiva.

Se si tratta di sviluppo a modello “non iterativo” oppure si tratta dell’ultima “iterazione” del modello precedente, la *Società* rilascia all’Amministrazione in ambiente di validazione l’applicazione e tutta la documentazione necessaria alla Verifica di Conformità. Contestualmente la *Società* si renderà disponibile per la Verifica di Conformità in contraddittorio.

Le attività previste sono:

- definizione del *Piano Operativo* del rilascio in validazione;
- completamento documentazione utente e di test.

Gli output di tale fase sono:

- disponibilità del risultato dell’”iterazione” o dell’applicazione completa;
- documentazione di test;
- eventuale documentazione utente se non disponibile online;
- misura delle funzionalità dell’”iterazione”.

2.3 ***VERIFICA DI CONFORMITÀ***

La Verifica di Conformità ha lo scopo di consentire all’Amministrazione di verificare la rispondenza del prodotto software realizzato ai requisiti concordati.

Nel caso di sviluppo a modello “iterativo”, la Verifica di Conformità dell’applicazione dovrà comunque tenere conto dell’esito della verifica svolta su tutte le “iterazioni” già validate.

Modalità di Verifica di Conformità del software

L’Amministrazione procederà alla Verifica di Conformità delle soluzioni in contraddittorio con la *Società* attraverso la verifica:

- della corrispondenza della documentazione prevista fornita dalla *Società*;
- della rispondenza dei moduli software alle funzionalità descritte nel documento di Analisi dei requisiti inviato formalmente;

- della rispondenza di quanto contenuto nel documento di test con il piano di test precedentemente concordato con la *Società*;
- della verifica degli output del piano di test.

2.4 ***ESTENSIONE***

Scopo della fase di Estensione è rendere disponibili a tutti gli Utenti del Sistema Informativo individuati dall’Amministrazione la soluzione software realizzata e le relative modalità di utilizzo.

Per il primo anno dalla data di inizio estensione della soluzione, non è previsto alcun onere per l’Amministrazione per le eventuali attività di manutenzione adeguativa e correttiva (periodo di manutenzione in garanzia).

L’Estensione prevede le seguenti attività:

- messa a punto dell’ambiente di produzione;
- trasferimento del software dall’ambiente di “validazione” all’ambiente di produzione;
- eventuale formazione per servizio di assistenza;
- aggiornamento patrimoniale e dimensionale dell’applicazione.

Nel caso di annualità, la consegna dell’applicazione conterrà l’evidenza della quota non conteggiata perchè proveniente da Sviluppi già presenti nelle annualità precedenti.

2.5 ***FLUSSO DI COMUNICAZIONE E DOCUMENTAZIONE PER SVILUPPO SOFTWARE***

La *Società* nel corso del ciclo produttivo predispone e mantiene aggiornato il documento di ‘Analisi dei Requisiti/Specifiche di intervento di MEV’ fino al consolidamento dei requisiti stessi e il documento di ‘Misure Sicurezza e Privacy del Servizio ICT’ fino alla sua completezza; aggiorna, se del caso, il piano dei test e verifiche.

Le parti potranno scambiarsi i documenti suddetti in bozza o qualsiasi altra documentazione necessaria (ad esempio prototipi, schemi architetturali etc...) fino a quando i requisiti e si riterranno consolidati, ovvero:

- nel caso di sviluppo a modello “non iterativo” la consegna formale sarà effettuata al termine della fase di analisi dei requisiti in funzione del consolidarsi dei requisiti stessi;
- nel caso di sviluppo “iterativo” la consegna formale avverrà al termine della fase di analisi dei requisiti dell’ultima “iterazione”.

Il documento ‘Analisi dei requisiti /Specifica di intervento di MEV’ dovrà contenere almeno:

- l’elenco dei macrorequisiti espressi dall’Amministrazione e gli eventuali riferimenti normativi;
- la descrizione del Sistema Informativo in cui si colloca l’intervento;
- il dettaglio dei requisiti funzionali e non funzionali e la proposta di automazione;
- piano di test;
- se si tratta di sviluppo, le misure di sicurezza e privacy adottate sul Servizio in base alla valutazione dell’Amministrazione; se si tratta di intervento evolutivo le misure verranno eventualmente adeguate in funzione dell’intervento effettuato.

Nel caso in cui si tratti di sviluppo a più “iterazioni”, il documento deve contenere anche:

- elenco macro requisiti e loro priorità con cui sono stati sviluppati;
- identificazione del sottoinsieme di requisiti inclusi nelle singole “iterazioni” rilasciate.

Il documento ‘Misure Sicurezza e Privacy del Servizio ICT’ dovrà contenere almeno:

- le misure di sicurezza e privacy in relazione ai dati personali trattati;
- la valutazione dei rischi intrinseci e residui dopo l’adozione delle misure di sicurezza già applicate e da applicare nell’intervento in corso.

In caso di sviluppo a modello “non iterativo”, all’insorgere di nuove o modificate esigenze, a fronte di documenti di output della fase Analisi dei requisiti già oggetto di approvazione formale da parte dell’Amministrazione, interviene la fase di Modifica in corso d’opera che consiste nella disamina della nuova esigenza e nella consegna di nuovi output contenenti le variazioni necessarie.

Al termine della fase di rilascio a modello “non iterativo” o dell’ultima “iterazione”, la *Società* invierà comunicazione all’Amministrazione che l’intervento è terminato e si è disponibili alla Verifica di Conformità; contestualmente verrà inviato:

- il documento di test contenente il piano di test, i casi di test ed il loro esito, nonché eventuali elementi utili per la valutazione della qualità;
- la bozza di documentazione utente, se non disponibile on-line.

L’Amministrazione entro 20 giorni dalla comunicazione formale della *Società* dovrà procedere alla Verifica di Conformità oppure alla richiesta di anticipata Estensione che avrà valore di Verifica di Conformità positiva.

In assenza di comunicazione dell’Amministrazione e trascorsi i termini, la *Società* è autorizzata a procedere alla fatturazione secondo quanto stabilito nella presente *Convenzione*.

In caso di prima Verifica di Conformità negativa, l’Amministrazione trascorsi almeno 10 giorni lavorativi convoca la *Società* per una seconda Verifica di Conformità. In caso di esito positivo della seconda Verifica di Conformità la *Società* può procedere alla fatturazione; altrimenti l’Amministrazione dovrà esprimersi in via definitiva sulla volontà di procedere ad una nuova verifica, ovvero di non accettare il prodotto, di annullare l’obiettivo e di non autorizzare la fatturazione.

Successivamente all’esito positivo della Verifica di Conformità, l’Amministrazione dovrà richiedere mediante comunicazione l’estensione dell’obiettivo; la *Società* procede all’estensione dell’applicazione secondo gli accordi con l’Amministrazione ed invia comunicazione dell’avvenuta conclusione della fase e la relativa documentazione:

- documentazione utente definitiva se prevista;
- misurazione del patrimonio software dell’applicazione rilasciata.

3. SERVIZI PROFESSIONALI

Nell’ambito del Servizio Professional vengono svolte attività di supporto e governance verso l’Amministrazione così come meglio descritte nell’Allegato A.

Il servizio viene erogato nei vari contesti descritti mettendo a disposizione competenze e

professionalità altamente specializzate secondo un mix professionale che dipende di volta in volta dalle necessità dell'Amministrazione e dal contesto specifico.

Nel caso in cui le attività di supporto siano volte ad obiettivi progettuali, il servizio dovrà prevedere la consegna di output specifici condivisi tra le parti e potrà essere remunerato a forfait.

Diversamente le attività di supporto che rivestano natura occasionale verrano remunerate a Tempo e Spesa secondo le tariffe di cui all'Allegato A.

Durante l'esecuzione delle attività, la *Società* e l'Amministrazione attuano un confronto continuo sulle attività da svolgere.

Fase "formulazione proposta"

- L'Amministrazione e la *Società* avvieranno le attività nei tempi e in coerenza con quanto previsto nel *Piano operativo*;
- la *Società* predisponde una proposta in cui vengono descritti i prodotti da realizzare, l'impegno delle risorse ed i tempi di consegna e lo sottopone all'approvazione dell'Amministrazione;
- in caso in cui l'Amministrazione formuli delle osservazioni, la *Società*, recependo dette osservazioni, risottomette una nuova proposta all'approvazione dell'Amministrazione prevedendo un eventuale riposizionamento nel tempo coerentemente con gli altri impegni previsti nel *Piano operativo*;
- l'approvazione da parte dell'Amministrazione documento ha valore di accettazione anche ai fini del dimensionamento economico e per l'avvio delle attività richieste.

Fase "Chiusura servizio"

- al termine del servizio la *Società* dovrà consegnare all'Amministrazione gli output previsti;
- l'Amministrazione dovrà procedere entro 10 giorni dalla ricezione dell'output alla sua approvazione;
- nel caso in cui i 10 giorni di cui al punto precedente trascorrano senza che vi sia alcuna osservazione da parte dell'Amministrazione l'output si intenderà approvato;

- in caso di osservazioni formulate dell’Amministrazione entro lo stesso termine massimo di 10 giorni, la *Società*, recependo dette osservazioni, potrà risottomettere l’output all’approvazione dell’Amministrazione o, in alternativa, proporre le proprie controdeduzioni, entro lo stesso termine massimo di 10 giorni;
- in tale ultimo caso, l’Amministrazione dovrà esprimersi in via definitiva, accettando o rigettando l’output prodotto, entro il limite massimo dei successivi 10 giorni;
- l’approvazione da parte dell’Amministrazione ha valore di accettazione anche ai fini della fatturazione e del pagamento.



Ministero della Salute

sogel

**CONVENZIONE PER L'AFFIDAMENTO DELLE ATTIVITA' DI
REALIZZAZIONE E GESTIONE DELL'ECOSISTEMA DATI SANITARI (EDS)
PREVISTO DALL'INVESTIMENTO M6C2 - 1.3.1 DEL PNRR**

- FASCICOLO SANITARIO ELETTRONICO –

EX ART. 12 COMMA 15-QUATER DEL DECRETO-LEGGE N. 179 DEL 2012

Allegato E

**ATTO DI ATTRIBUZIONE DEL RUOLO DI RESPONSABILE AI SENSI
DELL'ART 28 DEL REGOLAMENTO UE 2016/679 PER LA REALIZZAZIONE
DELL'ECOSISTEMA DATI SANITARI**

Sommario

1.	Definizioni	3
2.	Obblighi del Responsabile del trattamento nei confronti del Titolare	4
2.1	Limiti e termini del trattamento dei dati personali	4
2.2	Istruzioni del Titolare	4
2.3	Fornitura dei dati al Titolare.....	5
2.4	Registro dei trattamenti	5
2.5	Autorità di Controllo	5
2.6	Comunicazione e diffusione di dati.....	5
2.7	Ricorso a Sub-Responsabili del trattamento	5
2.8	Riservatezza e formazione delle persone autorizzate al trattamento.....	6
2.9	Obblighi del Responsabile nell'ambito dei diritti esercitati dagli Interessati...6	6
2.10	Misure di sicurezza.....	6
2.11	Cancellazione e distruzione dei dati	6
2.12	Ispezioni e revisione	6
2.13	Codici di condotta.....	7
2.14	Violazioni dei dati	7
2.15	Valutazione di impatto	7
2.16	Modifiche normative	7
3.	Rinvio.....	7

1. Definizioni

Nel presente documento si intende per:

- “Regolamento” o “GDPR” il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27.04.2016, relativo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati);
- “Norme in materia di protezione dei dati personali” il Regolamento, la normativa italiana in materia di trattamento dei dati personali, i provvedimenti e le linee guida del Comitato europeo per la protezione dei dati e del Garante per la protezione dei dati personali;
- “Contratto” la Convenzione per l'affidamento delle attività di realizzazione e gestione dell'ecosistema dati sanitari (EDS) previsto dall'investimento m6c2 - 1.3.1 del PNRR - Fascicolo Sanitario Elettronico – ex art. 12 comma 15-quater del decreto-legge n. 179 del 2012;
- “Titolare del trattamento” o “Titolare” il Ministero della Salute, il quale determina le finalità e i mezzi del trattamento di dati personali;
- “Responsabile iniziale del trattamento” o “Responsabile del trattamento” o “Responsabile” Sogei S.p.A. in quanto tratta dati personali per conto del Titolare o dell'eventuale Contitolare del trattamento;
- “Sub-Responsabile del trattamento” o “Sub-Responsabile” il fornitore o i suoi subappaltatori e subfornitori, individuati con procedura a evidenza pubblica, di cui Sogei S.p.A. si avvale per effettuare eventuali trattamenti di dati personali per conto del Titolare;
- “Persone autorizzate al trattamento” persone che in qualità di dipendenti, collaboratori, amministratori di sistema o consulenti del Responsabile del trattamento e/o del Sub-Responsabile del trattamento sono stati da questi autorizzati al trattamento dei dati personali sotto la loro diretta autorità;
- “Dati Personalni” qualsiasi informazione relativa a una persona fisica identificata o identificabile (interessato) - ivi inclusi i dati di cui agli artt. 9 e 10 del Regolamento - trattata dal Responsabile del trattamento per conto del Titolare del trattamento;
- “Trattamento” qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma messa a disposizione, il raffronto o l'interconnessione, la limitazione, allineamento o combinazione, la cancellazione o la distruzione;
- “Misure di Sicurezza” le misure di sicurezza tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio di cui all'art. 32 del Regolamento;
- “Registro delle attività di trattamento” o “Registro” il registro tenuto dal Responsabile del trattamento di tutte le categorie di attività relative al trattamento svolte per conto del Titolare del trattamento, di cui all'art. 30 del GDPR;
- “Violazione dei dati personali (*data breach*)” la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Premesso che:

- Il *Contratto* all'art. 25 indica la società Sogei S.p.A. quale Responsabile del trattamento dei dati ex art. 28 del Regolamento Europeo n. 2016/679;
- Sogei S.p.A. con la sottoscrizione del Contratto ha accettato la nomina di cui sopra e si è obbligata ad attenersi, nel trattamento dei dati personali, alle disposizioni del Regolamento (UE) 2016/679 ed alle ulteriori istruzioni per il trattamento dei dati personali contenute nel presente allegato.

Di seguito sono definite le istruzioni di carattere generale, che possono essere integrate e modificate per iscritto dal Titolare.

ISTRUZIONI

1. Elementi essenziali dei trattamenti che il Responsabile è autorizzato a svolgere

Il Responsabile è autorizzato a trattare per conto del Titolare tutti i dati personali necessari per la corretta esecuzione del *Contratto*.

La durata del trattamento è limitata e coincide con la durata del Contratto ovvero di sue eventuali proroghe, fatti salvi l'adempimento di specifici obblighi di legge o di documentate istruzioni impartite dal Titolare.

I dati trattati sono quelli personali comuni e quelli sensibili.

Le categorie di interessati sono coloro a cui si riferiscono i dati trattati attraverso l'Ecosistema Dati Sanitari così come definita nel Contratto nonché coloro che fruiscono dei servizi messi a disposizione dal Ministero della Salute.

Per l'esecuzione delle attività di cui al Contratto, il Responsabile del trattamento è autorizzato in via generale, ai sensi dell'art .28, paragrafo 2 del Regolamento, a ricorrere ove necessario ad altri responsabili del trattamento (Sub- Responsabili) individuati con procedure a evidenza pubblica, assumendo gli obblighi di cui all'art. 28, paragrafo 4 del Regolamento, come precisato nel successivo punto 2.7 del presente atto.

2. Obblighi del Responsabile del trattamento nei confronti del Titolare

2.1 Limiti e termini del trattamento dei dati personali

Il Responsabile è tenuto a trattare i dati personali solo e nei limiti in cui ciò sia necessario per l'esecuzione delle prestazioni contrattuali e le relative finalità.

Il Responsabile è tenuto a garantire che il trattamento dei dati personali sia effettuato in modo lecito e secondo correttezza, nel rispetto dei principi di cui all'art. 5 del Regolamento.

2.2 Istruzioni del Titolare

Il Responsabile è tenuto a trattare i dati personali soltanto su istruzione documentata del Titolare, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il Responsabile; in tal caso esso è tenuto ad informare il Titolare circa tale obbligo giuridico, prima del trattamento, a meno che il diritto vietи tale informazione per rilevanti motivi di interesse pubblico.

Il Responsabile non può trasferire i dati personali verso un paese terzo o un'organizzazione internazionale, salvo che non abbia preventivamente ottenuto autorizzazione scritta del Titolare.

Ove il Responsabile rilevi la sua impossibilità a rispettare le istruzioni impartite dal Titolare deve attuare comunque le possibili e ragionevoli misure di salvaguardia e deve avvertire immediatamente il Titolare e concordare eventuali ulteriori misure di protezione.

Qualora il Responsabile ritenga che una delle istruzioni violi il Regolamento o altre disposizioni nazionali o comunitarie deve informare immediatamente il Titolare.

2.3 Fornitura dei dati al Titolare

Qualora il Titolare o soggetto/funzione da esso incaricato/a abbia necessità, per lo svolgimento dei propri compiti istituzionali, di accedere a dati non disponibili attraverso i servizi applicativi, li richiede per iscritto, esplicitando tipologia dei dati, tempistica e modalità di fornitura, al Responsabile il quale è tenuto a renderli disponibili, secondo linee guida da concordare.

Le richieste di forniture di dati e le relative risposte sono scambiate mediante comunicazioni protocollate fra Titolare e Responsabile. Il Titolare informa il Responsabile circa il/i soggetto/i autorizzato/i a richiedere fornitura di dati, con eventuali limitazioni di ambito.

2.4 Registro dei trattamenti

Il Responsabile tiene un Registro di tutte le categorie di attività relative al trattamento (o ai trattamenti) svolti per conto del Titolare. Quest'ultimo deve assicurare la coerenza del proprio Registro con quello del Responsabile.

Il Responsabile mette a disposizione dell'Autorità di Controllo il Registro, ove richiesto, dandone al contempo informazione al Titolare.

2.5 Autorità di Controllo

Il Responsabile è tenuto in ogni caso a cooperare, su richiesta, con l'Autorità di Controllo nell'esecuzione dei suoi compiti.

Il Responsabile si obbliga a cooperare con il Titolare al fine di fornire tutte le informazioni, i dati e la documentazione necessaria affinché il Titolare possa adempiere alle richieste dell'Autorità di Controllo ovvero qualora si rendessero necessarie informazioni in caso di precontenzioso o contenzioso.

2.6 Comunicazione e diffusione di dati

Il Responsabile non può comunicare e/o diffondere dati senza l'esplicita autorizzazione del Titolare, fatte salve le particolari esigenze di riservatezza espressamente esplicitate dall'Autorità Giudiziaria.

2.7 Ricorso a Sub-Responsabili del trattamento

Il Sub-Responsabile del trattamento, individuato ai sensi del precedente punto 1, dovrà rispettare gli obblighi in materia di protezione dei dati personali imposti al Responsabile dalla Normativa in materia di protezione dei dati personali e dal Titolare con il presente atto e le eventuali ulteriori istruzioni documentate che lo stesso dovesse impartire. A tal fine il Responsabile è autorizzato dal Titolare a designare i fornitori quali Sub-Responsabili. Ai Sub-Responsabili verranno imposti, con l'atto di designazione - che può essere anche contenuto, ove possibile, nella documentazione della procedura ad evidenza pubblica - i medesimi obblighi e le medesime istruzioni ricevute dal Titolare.

Qualora il Sub-Responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile iniziale del trattamento conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del Sub- Responsabile.

Il Responsabile si impegna a informare preventivamente il Titolare di eventuali modifiche

riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al Titolare l'opportunità di opporsi a tali modifiche.

Il Responsabile si impegna comunque a rispettare le condizioni di cui ai paragrafi 2 e 4 dell'art.28 del Regolamento.

2.8 Riservatezza e formazione delle persone autorizzate al trattamento

Il Responsabile garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza e che siano adeguatamente formate in relazione alle Norme in materia di protezione dei dati personali e pienamente edotte rispetto alle istruzioni impartite dal Titolare.

2.9 Obblighi del Responsabile nell'ambito dei diritti esercitati dagli Interessati

Il Responsabile, ove richiesto, deve collaborare e supportare nel dare riscontro scritto, anche di mero diniego, alle istanze trasmesse dagli Interessati nell'esercizio dei diritti previsti dagli artt. 15-23 del GDPR, ovverosia alle istanze per l'esercizio del diritto di accesso, di rettifica, di integrazione, di cancellazione e di opposizione, diritto alla limitazione del trattamento, diritto alla portabilità dei dati, diritto a non essere oggetto di un processo decisionale automatizzato, compresa la profilazione.

Qualora gli interessati trasmettano la richiesta per l'esercizio dei loro diritti al Responsabile, questi deve inoltrarla tempestivamente al Titolare.

2.10 Misure di sicurezza

Il Responsabile, sulla base delle indicazioni del Titolare, adotta le misure richieste all'art.32 del Regolamento nonché le ulteriori misure di sicurezza di cui all'art. 3 del DPCM 10 novembre 2014 n. 194.

Nell'esecuzione del Contratto, il Responsabile supporta il Titolare nel tener conto dei principi della protezione dei dati fin dalla progettazione e protezione per impostazione predefinita.

Al fine di ridurre e mantenere per quanto più possibile al minimo i rischi e i pericoli derivanti dal trattamento dei dati personali, il Responsabile si impegna ad individuare le misure tecniche e organizzative più adeguate da mettere in atto nel rispetto dei vincoli del Contratto e sulla base delle indicazioni del Titolare, in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti degli interessati.

Il Responsabile dovrà operare attenendosi alle previsioni contenute nel documento condiviso di "Metodologia per la protezione dei dati e per la valutazione d'impatto", rendendo disponibile al Titolare ogni utile informazione per il corretto adempimento degli obblighi di cui agli articoli 25, 32 e 35 del Regolamento. Tale documento, allegato alle presenti istruzioni, sarà oggetto di revisione condivisa, secondo le modalità contenute nello stesso.

2.11 Cancellazione e distruzione dei dati

E' facoltà del Titolare, terminata la prestazione dei servizi relativi al trattamento, ottenere in qualunque momento la cancellazione o la restituzione di tutti i dati personali e la cancellazione totale di tutte le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati .

2.12 Ispezioni e revisione

Il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi a suo carico, consente e contribuisce alle attività di revisione, comprese le ispezioni, realizzate dal Titolare o da altro soggetto da questi incaricato, anche attraverso periodiche attività di *audit*, con modalità che saranno, di volta in

volta, concordate.

2.13 Codici di condotta

Ne caso in cui il Responsabile del trattamento aderisca a un codice di condotta approvato ai sensi dell'articolo 40 del Regolamento o a un meccanismo di certificazione approvato ai sensi dell'articolo 42 del Regolamento, tale adesione può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai paragrafi 1 e 4 dell'art. 28 del Regolamento.

2.14 Violazioni dei dati

Il Responsabile del trattamento si dichiara consapevole degli obblighi che incombono sul Titolare del trattamento, ai sensi dell'art.33 del Regolamento, in caso di violazione dei dati che sia tale da presentare un rischio per i diritti e le libertà fondamentali delle persone.

Il Responsabile si impegna a comunicare al Titolare la violazione dei dati personali “senza ingiustificato ritardo”, ai sensi e nei termini previsti dall'art.33 del Regolamento. Tale obbligo di cooperazione si impone anche nel caso in cui il Titolare debba comunicare la violazione all'interessato.

Il Responsabile si atterrà al “Flusso di notifica di *Data Breach* all'Autorità di controllo” allegato alla convenzione.

2.15 Valutazione di impatto

Per svolgere la valutazione d'impatto sulla protezione dei dati personali il Titolare può consultarsi con il proprio Responsabile della protezione dei dati, ai sensi dell'art. 35, comma 2, del Regolamento.

Il Responsabile del trattamento si impegna ad assistere il Titolare, a livello tecnico e organizzativo, nello svolgimento della valutazione d'impatto, così come disciplinata dall'art. 35 citato, in tutte le ipotesi in cui il trattamento preveda o necessiti della preliminare valutazione di impatto sulla protezione dei dati personali o del suo aggiornamento.

Il Responsabile dovrà operare attenendosi alle previsioni contenute nel documento condiviso di “Metodologia per la protezione dei dati e per la valutazione d'impatto”, rendendo disponibile al Titolare ogni utile informazione per il corretto adempimento degli obblighi di cui all'articolo 35 del Regolamento. Tale documento, allegato alle presenti istruzioni, sarà oggetto di revisione condivisa, secondo le modalità contenute nello stesso.

Il Responsabile del trattamento si impegna altresì ad assistere il Titolare nell'attività di consultazione preventiva dell'Autorità di Controllo prevista dall'articolo 36 del Regolamento.

2.16 Modifiche normative

Nell'eventualità di qualsivoglia modifica delle Norme in materia di protezione dei dati personali il Responsabile del trattamento supporta, nel rispetto dei vincoli del Contratto e nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse, il Titolare negli adeguamenti necessari.

3. Rinvio

Per tutto quanto non espressamente disciplinato nel presente atto, si richiamano gli obblighi previsti a carico del Responsabile del trattamento nel Contratto e dalle Norme in materia di protezione dei dati personali.

* * *

Allegati

- Metodologia per la protezione dei dati e per la valutazione d'impatto
- Flusso di notifica di *Data Breach* all'Autorità di controllo



Ministero della Salute



ALLEGATO F - PRIVACY

**ATTRIBUZIONE DEL RUOLO E DEGLI OBBLIGHI DI CUI ALL'ART. 28 DEL
REGOLAMENTO UE 2016/679**

INDICE

1.	DEFINIZIONI	4
2.	ATTRIBUZIONE DEL RUOLO DI RESPONSABILE	6
3.	ISTRUZIONI	8
3.1	ELEMENTI ESSENZIALI DEI TRATTAMENTI CHE IL RESPONSABILE È AUTORIZZATO A SVOLGERE	8
3.2	OBLIGHI DEL RESPONSABILE DEL TRATTAMENTO NEI CONFRONTI DEL TITOLARE	8
3.2.1	LIMITI E TERMINI DEL TRATTAMENTO DEI DATI PERSONALI	8
3.2.2	ISTRUZIONI DEL TITOLARE	9
3.2.3	FORNITURA DEI DATI AL TITOLARE	10
3.2.4	REGISTRO DEI TRATTAMENTI	10
3.2.5	AUTORITÀ DI CONTROLLO	10
3.2.6	COMUNICAZIONE E DIFFUSIONE DI DATI	10
3.2.7	RICORSO A SUB-RESPONSABILI DEL TRATTAMENTO	11
3.2.8	RISERVATEZZA E FORMAZIONE DELLE PERSONE AUTORIZZATE AL TRATTAMENTO	11
3.2.9	OBLIGHI DEL RESPONSABILE NELL'AMBITO DEI DIRITTI ESERCITATI DAGLI INTERESSATI	12
3.2.10	MISURE DI SICUREZZA	12
3.2.11	CANCELLAZIONE E DISTRUZIONE DEI DATI	12
3.2.12	ISPEZIONI E REVISIONE	13
3.2.13	CODICI DI CONDOTTA	13
3.2.14	VIOLAZIONI DEI DATI	13

ALLEGATO E PRIVACY

3.2.15	VALUTAZIONE DI IMPATTO	13
3.2.16	MODIFICHE NORMATIVE	14
3.3 RINVIO		14

ALLEGATI **ERRORE. IL SEGNALIBRO NON È DEFINITO.**

FLUSSO DI NOTIFICA DI DATA BREACH ALL'AUTORITÀ DI CONTROLLO **ERRORE. IL SEGNALIBRO NON È DEFINITO.**

1. DEFINIZIONI

Nel presente documento si intende per

- “*Amministrazione titolare o cliente*”, il Ministero della Salute quale Amministrazione destinataria dei servizi erogati da Agenas che riveste la qualifica di *Titolare del Trattamento* e per cui Agenas riveste la qualifica di *Responsabile del trattamento*;
- “*Dati Personal*” qualsiasi informazione relativa a una persona fisica identificata o identificabile (interessato) - ivi inclusi i dati di cui agli artt. 9 e 10 del Regolamento - trattata dal Responsabile del trattamento per conto del Titolare;
- “*Convenzione*”, si intende l’Accordo Esecutivo per sviluppo e conduzione della Ecosistema Dati Sanitari (EDS) di tutta la documentazione allo stesso afferente, stipulato tra Ministero della Salute, Sogei S.p.A. e il Dipartimento della trasformazione digitale della Presidenza del Consiglio dei Ministri e Agenas;
- “*Norme in materia di protezione dei dati personali*” il Regolamento, come di seguito definito, il D. Lgs. 196/2003 e s.m.i. e qualsiasi altra normativa o atto, comunitario o nazionale, avente forza normativa in materia di protezione dei dati personali, ivi compresi i provvedimenti del Garante per la protezione dei dati personali e del Comitato Europeo per la Protezione dei Dati;
- “*Misure di Sicurezza*” le misure di sicurezza tecniche e organizzative atte a garantire un livello di sicurezza adeguato al rischio di cui all’art. 32 del Regolamento;
- “*Persone autorizzate al trattamento*” persone che in qualità di dipendenti, collaboratori, amministratori di sistema o consulenti del Responsabile del trattamento e/o del Sub-Responsabile del trattamento sono stati da questi autorizzati al trattamento dei dati personali sotto la loro diretta autorità;
- “*Registro delle attività di trattamento*” o “*Registro*”, il registro tenuto dal Responsabile del trattamento di tutte le categorie di attività relative al trattamento svolte per conto del Titolare del trattamento, di cui all’art. 30, comma 2, del GDPR;
- “*Regolamento*” o “*GDPR*” il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27.04.2016, relativo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati);
- “*Responsabile del trattamento*” o “*Responsabile*” ai sensi dell’art. 4, n. 8 del Regolamento, la persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento, individuato in relazione alla Convenzione nell’Agenas e da quest’ultima nella società Sogei S.p.A. quale *Sub-Responsabile del trattamento*;.

ALLEGATO E PRIVACY

- “*Sub-Responsabile del trattamento*” o “*Sub-Responsabile*” il fornitore o i suoi subappaltatori e subfornitori, individuati con procedura a evidenza pubblica, di cui Sogei S.p.A. si potrà avvalere per effettuare eventuali trattamenti di dati personali per conto del Responsabile e del Titolare;
- “*Titolare del trattamento*” o “*Titolare*” ai sensi dell’art. 4, n. 7 del Regolamento, la persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali, individuato in relazione al Contratto nell’*Amministrazione Titolare*;
- “*Trattamento*” qualsiasi operazione o insieme di operazioni compiute con o senza l’ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, come la raccolta, la registrazione, l’organizzazione, la strutturazione, la conservazione, l’adattamento o la modifica, l’estrazione, la consultazione, l’uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma messa a disposizione, il raffronto o l’interconnessione, la limitazione, allineamento o combinazione, la cancellazione o la distruzione;
- “*Violazione dei dati personali (data breach)*” la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso ai dati personali trasmessi, conservati o comunque trattati;
- “*Autorità di controllo*” l’Autorità come definita all’art. 4, n. 21, del Regolamento.

2. ATTRIBUZIONE DEL RUOLO DI RESPONSABILE

Premesso che:

- Ministero della Salute svolge i compiti ad esso demandati dalla normativa europea ed italiana di riferimento;
- AGENAS riveste il ruolo Agenzia Nazionale per i Servizi Sanitari Regionali, in ragione delle disposizioni di legge e di Statuto che ne regolano l'attività;
- a tale riguardo è stato stipulato la Convenzione in relazione alla quale è necessario procedere alla sottoscrizione di apposito atto di attribuzione ad AGENAS del ruolo di Responsabile del trattamento dei dati personali ai sensi dell'art. 28 del Regolamento (cd. designazione);
- AGENAS presenta garanzie sufficienti in termini di conoscenza specialistica, affidabilità, esperienza e risorse per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del Regolamento, compreso il profilo relativo alla sicurezza del trattamento;
- le premesse formano parte integrante e sostanziale del presente atto,

tutto ciò premesso,

il Ministero della Salute (C.F 80242250589), con sede legale in Roma in Viale Giorgio Ribotta n.5, in persona del Segretario Generale, dott. Giovanni Leonardi, con incarico conferito con decreto del Presidente del Consiglio dei Ministri 14 maggio 2021, in qualità di legale rappresentante del Ministero e in qualità di Titolare del trattamento, (di seguito, anche il “**Ministero**”) ai sensi dell’art. 28 del Regolamento

ATTRIBUISCE A

all’Agenzia Nazionale per i Servizi Sanitari Regionali – AGENAS (C.F. 97113690586), con sede in Roma, Via delle Puglie, 23, rappresentata dal Presidente Prof. Enrico Coscioni, in qualità di legale rappresentante dell’Agenzia (di seguito, anche “**AGENAS**”), il ruolo di Responsabile del trattamento dei dati personali effettuato nell’esecuzione della Convenzione ai sensi dell’art. 28 del Regolamento.

A tale riguardo, il Responsabile del trattamento, sottoscrivendo il presente atto:

- conferma la sua diretta e approfondita conoscenza degli obblighi che si assume in relazione a quanto disposto dal Regolamento e, più in generale, dalle Norme in materia di protezione dei dati personali;
- si obbliga a procedere al trattamento dei dati – laddove questo sia necessario all’esecuzione delle prestazioni affidate – attenendosi in materia di sicurezza dei dati, oltre che al rispetto delle Norme in materia di protezione dei dati

PAG. 7 DI 14

ALLEGATO E PRIVACY

personalì, anche alle istruzioni di carattere generale nonché a ogni altra istruzione documentata concordate con il Titolare.

Di seguito sono definite le istruzioni di carattere generale che possono essere integrate e modificate nel tempo per iscritto dal Titolare.

3. ISTRUZIONI

3.1 ELEMENTI ESSENZIALI DEI TRATTAMENTI CHE IL RESPONSABILE È AUTORIZZATO A SVOLGERE

Il Responsabile è autorizzato a trattare per conto del Titolare i dati personali necessari per la corretta esecuzione della Convenzione.

La durata del trattamento è limitata e coincide con la durata dell'incarico conferito dal Titolare con la Convenzione ovvero di sue eventuali proroghe, fatto salvo l'adempimento di specifici obblighi di legge o di documentate istruzioni impartite dal Titolare.

Il tipo di dati personali trattati sono:

- i dati raccolti e generati dall'Ecosistema Dati Sanitari (EDS) di cui all'art. 12, comma 15-quater, del decreto-legge n. 179 del 2012 e s.m.i., la cui gestione operativa è affidata all'AGENAS.

Le categorie di interessati sono coloro a cui si riferiscono i dati trattati attraverso l'Ecosistema Dati Sanitari così come definita nel Contratto nonché coloro che fruiscono dei servizi messi a disposizione dal Ministero della Salute.

Qualora durante l'esecuzione contrattuale il tipo di dati personali trattati e le categorie di interessati dovessero subire modifiche sarà cura del Titolare comunicare formalmente a AGENAS le variazioni dell'ambito di trattamento alla stessa affidato.

Per l'esecuzione delle attività di cui alla Convenzione, il Responsabile del trattamento potrà ricorrere ove necessario ad altri responsabili del trattamento (Sub-Responsabili) individuati con procedure previste dalla normativa applicabile, come precisato nel successivo punto 3.2.7 del presente atto.

3.2 OBBLIGHI DEL RESPONSABILE DEL TRATTAMENTO NEI CONFRONTI DEL TITOLARE

3.2.1 LIMITI E TERMINI DEL TRATTAMENTO DEI DATI PERSONALI

Il Responsabile è tenuto a trattare i dati personali solo e nei limiti in cui ciò sia necessario per l'esecuzione delle prestazioni contrattuali e per le relative finalità.

3.2.2 ISTRUZIONI DEL TITOLARE

Il Responsabile è tenuto a trattare i dati personali soltanto su istruzione documentata del Titolare, anche in caso di trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il Responsabile; in tal caso esso è tenuto ad informare il Titolare circa tale obbligo giuridico prima del trattamento, a meno che il diritto vietи tale informazione per rilevanti motivi di interesse pubblico.

Il Responsabile – così come i suoi eventuali Sub-Responsabili nominati con la stipula della Convenzione – non può trasferire i dati personali verso un Paese terzo o un'organizzazione internazionale, salvo che non abbia preventivamente ottenuto un'autorizzazione scritta del Titolare. Tale autorizzazione, con la sottoscrizione del presente atto, viene concessa al Responsabile, e quindi ai suoi Sub-Responsabili, per tutti quei casi in cui questi ultimi ne abbiano necessità per il corretto funzionamento dei servizi e per l'erogazione degli stessi.

Qualora, per il corretto funzionamento dei servizi e per l'erogazione degli stessi si renda necessario trasferire i dati personali in paesi situati al di fuori dello SEE, il Responsabile si impegna a effettuare il trasferimento, anche tenendo in considerazione quanto previsto nei contratti stipulati con i sub responsabili, nel rispetto della normativa europea in materia di protezione dei dati personali - ivi incluso il GDPR, qualsiasi altra legge nazionale sulla protezione dei dati di uno degli Stati membri dell'Unione europea applicabile, nonché le linee guida e ordinanze emesse dalle autorità europee e nazionali competenti per la protezione dei dati e le sentenze delle autorità giudiziarie europee e nazionali competenti - e in presenza delle garanzie previste dal GDPR, assicurando un livello di protezione dei dati personali sostanzialmente equivalente a quello previsto dalla normativa privacy europea come suindicata.

A tal fine, il Responsabile si impegna a subordinare qualsiasi trasferimento dei dati personali verso paesi situati al di fuori dello SEE (che non siano stati destinatari di una decisione vincolante di adeguatezza da parte della Commissione europea) alla sottoscrizione delle clausole tipo adottate con decisione della Commissione europea 2010/87/EU ovvero delle diverse clausole tipo che saranno di volta in volta adottate dalla Commissione ai sensi del Regolamento ("Standard Contractual Clauses"), unitamente all'implementazione di ogni ulteriore misure tecnica, organizzativa e/o contrattuale finalizzata a garantire un livello di protezione sostanzialmente equivalente a quello garantito all'interno dello SEE. Il Responsabile riconosce e garantisce che le misure e gli impegni di cui sopra saranno debitamente e tempestivamente attuati e intrapresi anche dai relativi Sub-Responsabili.

Ove il Responsabile rilevi la sua impossibilità a rispettare le istruzioni impartite dal Titolare deve attuare comunque le possibili e ragionevoli misure di salvaguardia e

deve avvertire immediatamente il Titolare e concordare eventuali ulteriori misure di protezione.

Qualora il Responsabile ritenga che una delle istruzioni violi il Regolamento o altre disposizioni nazionali o comunitarie deve informare immediatamente il Titolare.

3.2.3 FORNITURA DEI DATI AL TITOLARE

Qualora il Titolare o soggetto/funzione da esso incaricato/a abbia necessità di accedere a dati non disponibili attraverso i servizi applicativi, li richiede per iscritto, esplicitando la tipologia dei dati, la tempistica e la modalità di fornitura, al Responsabile il quale è tenuto a renderli disponibili ove possibile entro 7 giorni o qualora vi sia urgenza anche in un tempo inferiore concordato con il Titolare.

3.2.4 REGISTRO DEI TRATTAMENTI

Il Responsabile tiene un Registro di tutte le categorie di attività relative al trattamento (o ai trattamenti) svolti per conto del Titolare.

Il Responsabile mette a disposizione dell'Autorità di controllo il Registro, ove richiesto, dandone al contempo informazione al Titolare.

3.2.5 AUTORITÀ DI CONTROLLO

Il Responsabile è tenuto in ogni caso a cooperare, su richiesta, con l'Autorità di controllo nell'esecuzione dei suoi compiti.

Il Responsabile si obbliga a cooperare con il Titolare al fine di fornire tutte le informazioni, i dati e la documentazione necessaria affinché il Titolare possa adempiere alle richieste dell'Autorità di controllo ovvero qualora si rendessero necessarie informazioni in caso di precontenzioso o contenzioso.

3.2.6 COMUNICAZIONE E DIFFUSIONE DI DATI

Il Responsabile non può comunicare e/o diffondere dati senza l'esplicita autorizzazione del Titolare, fatte salve le particolari esigenze di riservatezza espressamente esplicitate dall'Autorità Giudiziaria.

3.2.7 RICORSO A SUB-RESPONSABILI DEL TRATTAMENTO

Qualora nominati nel rispetto delle disposizioni che seguono, eventuali Sub-Responsabili del trattamento dovranno rispettare gli obblighi in materia di protezione dei dati personali imposti al Responsabile dalla normativa in materia di protezione dei dati personali e dal Titolare con il presente atto e le eventuali ulteriori istruzioni documentate che lo stesso dovesse impartire.

A tal fine, il Responsabile è autorizzato dal Titolare a designare, ai sensi dell'art. 28 del Regolamento, eventuali soggetti individuati a seguito delle procedure previste dalla normativa applicabile quali Sub-Responsabili.

Detti soggetti tratteranno i dati personali del Titolare in qualità di responsabili del trattamento in virtù di un accordo sul trattamento dei dati concluso con il Titolare medesimo o di un accordo concluso tra il Responsabile con Sogei ed eventuali suoi sub fornitori, ai sensi dell'art. 28, par. 4, del Regolamento, con il quale tali sub fornitori saranno nominati quali ulteriori responsabili per conto del Titolare e saranno vincolati al rispetto degli stessi obblighi in materia di protezione dei dati personali applicabili a Sogei in virtù del presente accordo e, ovviamente, della normativa di volta in volta vigente. In particolare, il sub fornitore dovrà fornire sufficienti garanzie circa l'implementazione di adeguate misure di sicurezza tecniche ed organizzative, in modo da rispettare i requisiti imposti dalle Norme in materia di protezione dei dati personali.

Resto inteso tra le Parti che, qualora il sub responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile conserva nei confronti del Titolare l'intera responsabilità degli obblighi del sub fornitore.

Il Responsabile dovrà informare il Titolare di ogni intenzione di modifica che abbia ad oggetto l'aggiunta, la sostituzione o la rimozione degli ulteriori responsabili di cui al paragrafo che precede, dando conseguentemente al Titolare l'opportunità di opporsi a tali modifiche.

3.2.8 RISERVATEZZA E FORMAZIONE DELLE PERSONE AUTORIZZATE AL TRATTAMENTO

Il Responsabile garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza e che siano adeguatamente formate in relazione alle Norme in materia di protezione dei dati personali e pienamente edotte rispetto alle istruzioni impartite dal Titolare.

3.2.9 OBBLIGHI DEL RESPONSABILE NELL'AMBITO DEI DIRITTI ESERCITATI DAGLI INTERESSATI

Il Responsabile, ove richiesto, deve collaborare e supportare nel dare riscontro scritto, anche di mero diniego, alle istanze trasmesse dagli Interessati nell'esercizio dei diritti previsti dagli artt. 15-23 del GDPR, vale a dire alle istanze per l'esercizio del diritto di accesso, di rettifica, di integrazione, di cancellazione e di opposizione, diritto alla limitazione del trattamento, diritto alla portabilità dei dati, diritto a non essere oggetto di un processo decisionale automatizzato, compresa la profilazione.

Qualora gli interessati trasmettano la richiesta per l'esercizio dei loro diritti al Responsabile, quest'ultimo deve inoltrarla tempestivamente al Titolare.

3.2.10 MISURE DI SICUREZZA

Il Responsabile, sulla base delle indicazioni del Titolare, adotta le misure richieste dall'art. 32 del Regolamento.

Nell'esecuzione del Contratto, il Responsabile supporta il Titolare nel tener conto dei principi della protezione dei dati fin dalla progettazione e protezione per impostazione predefinita.

Fatto salvo quanto previsto al par. 3.2.7, quarto paragrafo, il Responsabile dovrà operare, rendendo disponibile al Titolare ogni utile informazione per il corretto adempimento degli obblighi di cui agli articoli 25, 32 e 35 del Regolamento.

Il Responsabile adotta e rispetta le misure di sicurezza indicate dal Titolare e individua, sottponendole al Titolare, misure di sicurezza ulteriori a quelle già in uso, che dovesse ritenere necessarie per garantire un adeguato livello di protezione dei dati personali in relazione all'analisi dei rischi e alla valutazione d'impatto.

3.2.11 CANCELLAZIONE E DISTRUZIONE DEI DATI

E' facoltà del Titolare, terminata la prestazione dei servizi relativi al trattamento, ottenere in qualunque momento la cancellazione o la restituzione di tutti i dati personali e la cancellazione totale di tutte le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati.

3.2.12 ISPEZIONI E REVISIONE

Il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi a suo carico, consente e contribuisce alle attività di revisione, comprese le ispezioni, realizzate dal Titolare o da altro soggetto da questi incaricato, anche attraverso periodiche attività di audit, con modalità che saranno, di volta in volta, concordate.

3.2.13 CODICI DI CONDOTTA

Ne caso in cui il Responsabile del trattamento aderisca a un codice di condotta approvato ai sensi dell'articolo 40 del Regolamento o a un meccanismo di certificazione approvato ai sensi dell'articolo 42 del Regolamento, tale adesione può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai paragrafi 1 e 4 dell'art. 28 del Regolamento.

3.2.14 VIOLAZIONI DEI DATI

Il Responsabile del trattamento si dichiara consapevole degli obblighi che incombono sul Titolare del trattamento, ai sensi dell'art. 33 del Regolamento, in caso di violazione dei dati che sia tale da presentare un rischio per i diritti e le libertà fondamentali delle persone.

Il Responsabile si impegna a comunicare al Titolare la violazione dei dati personali "senza ingiustificato ritardo", ai sensi e nei termini previsti dall'art. 33 del Regolamento. Tale obbligo di cooperazione si impone anche nel caso in cui il Titolare debba comunicare la violazione all'interessato.

Il Responsabile si atterrà al "Flusso di notifica di Data Breach all'Autorità di controllo" allegato alle presenti istruzioni.

3.2.15 VALUTAZIONE DI IMPATTO

Per svolgere la valutazione d'impatto sulla protezione dei dati personali il Titolare può consultarsi con il proprio Responsabile della protezione dei dati, ai sensi dell'art. 35, comma 2, del Regolamento.

Il Responsabile del trattamento si impegna ad assistere il Titolare, a livello tecnico e organizzativo, nello svolgimento della valutazione d'impatto, così come

disciplinata dall'art. 35 citato, in tutte le ipotesi in cui il trattamento preveda o necessiti della preliminare valutazione di impatto sulla protezione dei dati personali o del suo aggiornamento, fatto salvo quanto previsto al par. 3.2.7, quarto paragrafo.

Il Responsabile dovrà operare attenendosi alle istruzioni che verranno impartite dal Titolare rendendo disponibile al Titolare ogni utile informazione per il corretto adempimento degli obblighi di cui all'articolo 35 del Regolamento.

Il Responsabile del trattamento si impegna altresì ad assistere il Titolare nell'attività di consultazione preventiva dell'Autorità di controllo prevista dall'articolo 36 del Regolamento.

3.2.16 MODIFICHE NORMATIVE

Nell'eventualità di qualsiasi modifica delle Norme in materia di protezione dei dati personali, il Responsabile del trattamento supporta, nel rispetto dei vincoli della Convenzione e nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse, il Titolare negli adeguamenti necessari.

3.3 RINVIO

Per tutto quanto non espressamente disciplinato nel presente atto, si richiamano gli obblighi previsti a carico del Responsabile del trattamento nella Convenzione e dalle Norme in materia di protezione dei dati personali.



*CONVENZIONE PER L'AFFIDAMENTO DELLE ATTIVITÀ DI REALIZZAZIONE E
GESTIONE DELL'ECOSISTEMA DATI SANITARI (EDS) PREVISTO
DALL'INVESTIMENTO M6C2 - 1.3.1 DEL PNRR - FASCICOLO SANITARIO
ELETTRONICO – EX ART. 12 COMMA 15-QUATER DEL DECRETO-LEGGE N. 179 DEL
2012*

ALLEGATO G - PRIVACY

*ATTRIBUZIONE DEL RUOLO E DEGLI OBBLIGHI DI CUI ALL'ART. 28 DEL
REGOLAMENTO UE 2016/679*

INDICE

1.	DEFINIZIONI	4
2.	ATTRIBUZIONE DEL RUOLO DI RESPONSABILE	6
3.	ISTRUZIONI	8
3.1	ELEMENTI ESSENZIALI DEI TRATTAMENTI CHE IL SUB-RESPONSABILE È AUTORIZZATO A SVOLGERE	8
3.2	OBLIGHI DEL SUB-RESPONSABILE DEL TRATTAMENTO NEI CONFRONTI DEL RESPONSABILE E/O TITOLARE	8
3.2.1	LIMITI E TERMINI DEL TRATTAMENTO DEI DATI PERSONALI	8
3.2.2	ISTRUZIONI DEL RESPONSABILE	9
3.2.3	FORNITURA DEI DATI AL RESPONSABILE	9
3.2.4	REGISTRO DEI TRATTAMENTI	9
3.2.5	AUTORITÀ DI CONTROLLO	10
3.2.6	COMUNICAZIONE E DIFFUSIONE DI DATI	10
3.2.7	RICORSO AD ALTRI SUB-RESPONSABILI DEL TRATTAMENTO	10
3.2.8	RISERVATEZZA E FORMAZIONE DELLE PERSONE AUTORIZZATE AL TRATTAMENTO	11
3.2.9	OBLIGHI DEL SUB-RESPONSABILE NELL'AMBITO DEI DIRITTI ESERCITATI DAGLI INTERESSATI	11
3.2.10	MISURE DI SICUREZZA	12
3.2.11	CANCELLAZIONE E DISTRUZIONE DEI DATI	12
3.2.12	ISPEZIONI E REVISIONE	12
3.2.13	CODICI DI CONDOTTA	12

PAG. 3 DI 14

ALLEGATO G - PRIVACY

3.2.14	VIOLAZIONI DEI DATI	13
3.2.15	VALUTAZIONE DI IMPATTO	13
3.2.16	MODIFICHE NORMATIVE	14
3.3 RINVIO		14
1.	ALLEGATI	14

ALLEGATO G - PRIVACY**1. DEFINIZIONI**

Nel presente documento si intende per

- “*Amministrazione Cliente*”, le Amministrazioni e/o altri enti o persone giuridiche destinatarie dei servizi erogati dalla Sogei attraverso la Convenzione, che rivestono la qualifica di Titolari del Trattamento - Ministero della Salute -, ovvero la qualifica di Responsabile del trattamento - Agenzia Nazionale per i Servizi Sanitari Regionali (AGENAS) e per cui Sogei riveste la qualifica di Sub-Responsabile del trattamento;
- “*Dati Personalini*” qualsiasi informazione relativa a una persona fisica identificata o identificabile (interessato) - ivi inclusi i dati di cui agli artt. 9 e 10 del Regolamento - trattata dal Responsabile del trattamento per conto del Titolare;
- “*Contratto*” si intende la Convenzione per l'affidamento delle attività di realizzazione e gestione dell'ecosistema dati sanitari (EDS) previsto dall'investimento m6c2 - 1.3.1 del PNRR - fascicolo sanitario elettronico – ex art. 12 comma 15-quater del decreto-legge n. 179 del 2012, stipulata tra l il Ministero della Salute, Agenas, il Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei Ministri e Sogei S.p.A.;
- “*Norme in materia di protezione dei dati personali*” il Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento nell'ordinamento nazionale al Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali di cui al D.lgs. 30 giugno 2003 n. 196, come modificato e integrato dal D.lgs. n. 101/2018;
- “*Misure di Sicurezza*” le misure di sicurezza tecniche e organizzative adeguate garantire un livello di sicurezza adeguato al rischio di cui all'art. 32 del Regolamento;
- “*Personne autorizzate al trattamento*” persone che in qualità di dipendenti, collaboratori, amministratori di sistema o consulenti del Responsabile del trattamento e/o del Sub-Responsabile del trattamento sono stati da questi autorizzati al trattamento dei dati personali sotto la loro diretta autorità;
- “*Registro delle attività di trattamento*” o “*Registro*”, il registro tenuto dal Responsabile del trattamento di tutte le categorie di attività relative al trattamento svolte per conto del Titolare del trattamento, di cui all'art. 30 del GDPR;
- “*Regolamento*” o “*GDPR*” il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27.04.2016, relativo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati);
- “*Responsabile iniziale del trattamento*” o “*Responsabile del trattamento*” o “*Responsabile*” ai sensi dell'art. 4, n. 8 del Regolamento, la persona fisica o

ALLEGATO G - PRIVACY

giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento individuato per i trattamenti dati di seguito specificati per conto del Titolare o dell'eventuale Contitolare del trattamento, individuato in relazione al Contratto in AGENAS;

- “*Sub-Responsabile del trattamento*” o “*Sub-Responsabile*” la società Sogei S.p.A., il fornitore o i suoi subappaltatori e subfornitori, individuati con procedura a evidenza pubblica, di cui Sogei S.p.A. si avvale per effettuare eventuali trattamenti di dati personali per conto del Responsabile e/o del Titolare;
- “*Titolare del trattamento*” o “*Titolare*” ai sensi dell’art. 4, n. 7 del Regolamento, la persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali nel Ministero della Salute;
- “*Trattamento*” qualsiasi operazione o insieme di operazioni compiute con o senza l’ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, come la raccolta, la registrazione, l’organizzazione, la strutturazione, la conservazione, l’adattamento o la modifica, l’estrazione, la consultazione, l’uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma messa a disposizione, il raffronto o l’interconnessione, la limitazione, allineamento o combinazione, la cancellazione o la distruzione;
- “*Violazione dei dati personali (data breach)*” la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso ai dati personali trasmessi, conservati o comunque trattati.

ALLEGATO G - PRIVACY**2. ATTRIBUZIONE DEL RUOLO DI RESPONSABILE**

Premesso che

- l'Agenzia Nazionale per i Servizi Sanitari Regionali (AGENAS) svolge i compiti ad essi demandati dalla Costituzione, dalla legge e dai propri atti regolamentari;
- Il Ministero della Salute ha sottoscritto apposito atto di attribuzione a AGENAS del ruolo di Responsabile del trattamento dei dati personali ai sensi dell'art. 28 del Regolamento (allegato F del Contratto);
- Sogei riveste il ruolo di società in house al Ministero dell'economia e delle finanze, in ragione delle disposizioni di legge e di Statuto che ne regolano l'attività;
- a tale riguardo è stato stipulato il contratto in relazione al quale è necessario procedere alla sottoscrizione di apposito atto di attribuzione a Sogei S.p.A. del ruolo di Sub-Responsabile del trattamento dei dati personali ai sensi dell'art. 28 del Regolamento (cd. designazione);
- Sogei S.p.A. presenta garanzie sufficienti in termini di conoscenza specialistica, affidabilità, esperienza e risorse per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del Regolamento, compreso il profilo relativo alla sicurezza del trattamento.

e che le premesse formano parte integrante e sostanziale del presente atto,

l'Agenzia Nazionale per i Servizi Sanitari Regionali (AGENAS), Roma, Via delle Puglie, 23, Codice Fiscale 97113690586, in persona del Presidente Prof. Enrico Coscioni, domiciliato per la carica presso la sede legale, in qualità di Responsabile del trattamento, ai sensi dell'art. 28 del Regolamento.

ATTRIBUISCE A

Sogei S.p.A., con sede legale in Roma, via M. Carucci n. 99, codice fiscale 02327910580, partita IVA 01043931003, in persona del legale rappresentante dott. Andrea Quacivì, domiciliato per la carica presso la sede sociale, il ruolo di Sub-Responsabile del trattamento dei dati personali effettuato nell'esecuzione del Contratto ai sensi dell'art. 28 del regolamento.

A tale riguardo il Sub-Responsabile del trattamento, sottoscrivendo il presente atto:

- conferma la sua diretta e approfondita conoscenza degli obblighi che si assume in relazione a quanto disposto dal Regolamento e, più in generale, dalle Norme in materia di protezione dei dati personali;
- si obbliga a procedere al trattamento dei dati – laddove questo sia necessario all'esecuzione delle prestazioni affidate – attenendosi in materia di sicurezza dei dati, oltre che al rispetto della normativa vigente in materia di protezione dei

PAG. 7 DI 14

ALLEGATO G - PRIVACY

dati personali anche, alle istruzioni di carattere generale nonché a ogni altra istruzione documentata concordate con il Responsabile e/o il Titolare.

Di seguito sono definite le istruzioni di carattere generale, che possono essere integrate e modificate nel tempo per iscritto dal Responsabile e/o dal Titolare.

3. ISTRUZIONI

3.1 ELEMENTI ESSENZIALI DEI TRATTAMENTI CHE IL SUB-RESPONSABILE È AUTORIZZATO A SVOLGERE

Il Sub-Responsabile è autorizzato a trattare per conto del Responsabile tutti i dati personali necessari per la corretta esecuzione del Contratto.

La durata del trattamento è limitata e coincide con la durata del Contratto ovvero di sue eventuali proroghe, fatti salvi l'adempimento di specifici obblighi di legge o di documentate istruzioni impartite dal Responsabile e/o dal Titolare.

Il tipo di dati personali trattati dell'utente finale sono i seguenti:

- dati raccolti e generati dall'Ecosistema Dati Sanitari (EDS) di cui all'art. 12, comma 15-quater, del decreto-legge n. 179 del 2012 e s.m.i., la cui gestione operativa è affidata all'AGENAS.

Le categorie di interessati sono coloro a cui si riferiscono i dati trattati attraverso l'Ecosistema Dati Sanitari così come definita nel Contratto nonché coloro che fruiscono dei servizi messi a disposizione dal Ministero della Salute.

Per l'esecuzione delle attività di cui al Contratto, il Sub-Responsabile del trattamento è autorizzato in via generale, ai sensi dell'art. 28, paragrafo 2 del Regolamento, a ricorrere ove necessario ad altri responsabili del trattamento (Sub-Responsabili) individuati con procedure a evidenza pubblica, assumendo, ricorrendone le condizioni, gli obblighi di cui all'art. 28, paragrafo 4 del Regolamento, come precisato nel successivo punto 3.2.7 del presente atto.

3.2 OBBLIGHI DEL SUB-RESPONSABILE DEL TRATTAMENTO NEI CONFRONTI DEL RESPONSABILE E/O TITOLARE

3.2.1 *LIMITI E TERMINI DEL TRATTAMENTO DEI DATI PERSONALI*

Il Sub-Responsabile è tenuto a trattare i dati personali solo e nei limiti in cui ciò sia necessario per l'esecuzione delle prestazioni contrattuali e le relative finalità.

3.2.2 *ISTRUZIONI DEL RESPONSABILE*

Il Sub-Responsabile è tenuto a trattare i dati personali soltanto su istruzione documentata del Responsabile e/o del Titolare, anche in caso di trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il Sub-Responsabile; in tal caso esso è tenuto ad informare il Responsabile e/o del Titolare circa tale obbligo giuridico prima del trattamento, a meno che il diritto vietи tale informazione per rilevanti motivi di interesse pubblico.

Il Sub-Responsabile non può trasferire i dati personali verso un Paese terzo o un'organizzazione internazionale, salvo che non abbia preventivamente ottenuto un'autorizzazione scritta del Responsabile e/o del Titolare. Tale autorizzazione, con la sottoscrizione del presente atto, viene concessa al Sub-Responsabile, e quindi ai suoi Sub-Responsabili, per tutti quei casi in cui questi ultimi ne abbiano necessità per il corretto funzionamento dei servizi e per l'erogazione degli stessi.

Ove il Sub-Responsabile rilevi la sua impossibilità a rispettare le istruzioni impartite dal Responsabile e/o dal Titolare deve attuare comunque le possibili e ragionevoli misure di salvaguardia e deve avvertire immediatamente il Responsabile e concordare eventuali ulteriori misure di protezione.

Qualora il Sub-Responsabile ritenga che una delle istruzioni violi il Regolamento o altre disposizioni nazionali o comunitarie deve informare immediatamente il Responsabile.

3.2.3 *FORNITURA DEI DATI AL RESPONSABILE*

Qualora il Responsabile o soggetto/funzione da esso incaricato/a abbia necessità, per lo svolgimento dei propri compiti istituzionali, di accedere a dati non disponibili attraverso i servizi applicativi, li richiede per iscritto, esplicitando la tipologia dei dati, la tempistica e la modalità di fornitura, al Sub-Responsabile il quale è tenuto a renderli disponibili, secondo linee guida da concordare.

3.2.4 *REGISTRO DEI TRATTAMENTI*

Il Sub-Responsabile tiene un Registro di tutte le categorie di attività relative al trattamento (o ai trattamenti) svolti per conto del Responsabile. Il Sub-Responsabile ed il Responsabile devono assicurare la coerenza reciproca dei propri Registri.

ALLEGATO G - PRIVACY

Il Sub-Responsabile mette a disposizione dell'Autorità di controllo il Registro, ove richiesto, dandone al contempo informazione al Responsabile.

3.2.5 AUTORITÀ DI CONTROLLO

Il Sub-Responsabile è tenuto in ogni caso a cooperare, su richiesta, con l'Autorità di controllo nell'esecuzione dei suoi compiti.

Il Sub-Responsabile si obbliga a cooperare con il Responsabile e/o Titolare al fine di fornire tutte le informazioni, i dati e la documentazione necessaria affinché il Responsabile e/o Titolare possano adempiere alle richieste dell'Autorità di controllo ovvero qualora si rendessero necessarie informazioni in caso di precontenzioso o contenzioso.

3.2.6 COMUNICAZIONE E DIFFUSIONE DI DATI

Il Sub-Responsabile non può comunicare e/o diffondere dati senza l'esplicita autorizzazione del Responsabile, fatte salve le particolari esigenze di riservatezza espressamente esplicitate dall'Autorità Giudiziaria.

3.2.7 RICORSO AD ALTRI SUB-RESPONSABILI DEL TRATTAMENTO

Gli eventuali altri Sub-Responsabili del trattamento dovranno rispettare gli obblighi in materia di protezione dei dati personali imposti al Sub-Responsabile dalla normativa in materia di protezione dei dati personali e dal Responsabile con il presente atto e le eventuali ulteriori istruzioni documentate che lo stesso dovesse impartire.

A tal fine gli eventuali altri Sub-Responsabili sono autorizzati dal Sub-Responsabile a designare ai sensi dell'art. 28 del Regolamento i fornitori quali Sub-Responsabili.

Agli eventuali altri Sub-Responsabili verranno imposti, con l'atto di attribuzione del ruolo stesso di Sub-Responsabile ai sensi dell'art. 28 del Regolamento- che può essere anche contenuto, ove possibile, nella documentazione della procedura ad evidenza pubblica - i medesimi obblighi e le medesime istruzioni ricevute dalle altre parti, salvo che la particolare natura del servizio acquisito richieda necessariamente l'adesione a condizioni generali inerenti la protezione dei dati personali stabilite dal fornitore.

ALLEGATO G - PRIVACY

In tale caso il fornitore sarà nominato quale Sub-Responsabile ed il Responsabile terrà conto, a riguardo, che l'adempimento alle prescrizioni del Regolamento, ivi incluse quelle relative alle misure di sicurezza ed alla privacy by default e by design da parte del Sub-Responsabile, saranno attuate sulla base delle condizioni e dei termini per la protezione dei dati personali stabilite da quest'ultimo.

Qualora l'eventuale altro Sub-Responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Sub-Responsabile iniziale del trattamento conserva nei confronti del Responsabile del trattamento l'intera responsabilità dell'adempimento degli obblighi del l'eventuale altro Sub-Responsabile ove abbia trasferito allo stesso gli stessi obblighi e le stesse istruzioni ricevute dal Responsabile.

Il Sub-Responsabile si impegna a informare il Responsabile di eventuali modifiche riguardanti l'aggiunta o la sostituzione di altri sub-responsabili del trattamento, dando così al Responsabile l'opportunità di opporsi a tali modifiche.

Il Sub-Responsabile si impegna comunque a rispettare le condizioni di cui ai paragrafi 2 e 4 dell'art. 28 del Regolamento, per quanto applicabili.

3.2.8 RISERVATEZZA E FORMAZIONE DELLE PERSONE AUTORIZZATE AL TRATTAMENTO

Il Sub-Responsabile garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza e che siano adeguatamente formate in relazione alle Norme in materia di protezione dei dati personali e pienamente edotte rispetto alle istruzioni impartite dal Responsabile.

3.2.9 OBBLIGHI DEL SUB-RESPONSABILE NELL'AMBITO DEI DIRITTI ESERCITATI DAGLI INTERESSATI

Il Sub-Responsabile, ove richiesto, deve collaborare e supportare nel dare riscontro scritto, anche di mero diniego, alle istanze trasmesse dagli Interessati nell'esercizio dei diritti previsti dagli artt. 15-23 del GDPR, vale a dire alle istanze per l'esercizio del diritto di accesso, di rettifica, di integrazione, di cancellazione e di opposizione, diritto alla limitazione del trattamento, diritto alla portabilità dei dati, diritto a non essere oggetto di un processo decisionale automatizzato, compresa la profilazione.

Qualora gli interessati trasmettano la richiesta per l'esercizio dei loro diritti al Sub-Responsabile, quest'ultimo deve inoltrarla tempestivamente al Responsabile e/o Titolare.

3.2.10 MISURE DI SICUREZZA

Il Sub-Responsabile, sulla base delle indicazioni del Responsabile, adotta le misure richieste dall'art. 32 del Regolamento.

Nell'esecuzione del Contratto, il Sub-Responsabile supporta il Responsabile nel tener conto dei principi della protezione dei dati fin dalla progettazione e protezione per impostazione predefinita.

Fatto salvo quanto previsto al par. 3.2.7, quarto paragrafo, il Sub-Responsabile dovrà operare attenendosi alle previsioni contenute nel documento condiviso di "Metodologia per la protezione dei dati e per la valutazione d'impatto", se applicabile alla tipologia di servizio erogato, rendendo disponibile al Responsabile ogni utile informazione per il corretto adempimento degli obblighi di cui agli articoli 25, 32 e 35 del Regolamento. Tale documento, allegato alle presenti istruzioni, sarà oggetto di revisione condivisa, secondo le modalità contenute nello stesso.

3.2.11 CANCELLAZIONE E DISTRUZIONE DEI DATI

È facoltà del Responsabile, terminata la prestazione dei servizi relativi al trattamento, ottenere in qualunque momento la cancellazione o la restituzione di tutti i dati personali e la cancellazione totale di tutte le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati.

3.2.12 ISPEZIONI E REVISIONE

Il Sub-Responsabile mette a disposizione del Responsabile tutte le informazioni necessarie per dimostrare il rispetto degli obblighi a suo carico, consente e contribuisce alle attività di revisione, comprese le ispezioni, realizzate dal Responsabile e/o Titolare, o da altro soggetto da questi incaricato, anche attraverso periodiche attività di audit, con modalità che saranno, di volta in volta, concordate.

3.2.13 CODICI DI CONDOTTA

Ne caso in cui il Sub-Responsabile del trattamento aderisca a un codice di condotta approvato ai sensi dell'articolo 40 del Regolamento o a un meccanismo di certificazione approvato ai sensi dell'articolo 42 del Regolamento, tale adesione può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai paragrafi 1 e 4 dell'art. 28 del Regolamento.

3.2.14 VIOLAZIONI DEI DATI

Il Sub-Responsabile del trattamento si dichiara consapevole degli obblighi che incombono sul Responsabile e/o Titolare del trattamento, ai sensi dell'art. 33 del Regolamento, in caso di violazione dei dati che sia tale da presentare un rischio per i diritti e le libertà fondamentali delle persone.

Il Sub-Responsabile si impegna a comunicare al Responsabile la violazione dei dati personali "senza ingiustificato ritardo", ai sensi e nei termini previsti dall'art. 33 del Regolamento. Tale obbligo di cooperazione si impone anche nel caso in cui il Responsabile debba comunicare la violazione all'interessato.

Il Sub-Responsabile si atterrà al "Flusso di notifica di Data Breach all'Autorità di controllo" allegato alle presenti istruzioni.

3.2.15 VALUTAZIONE D'IMPATTO

Per svolgere la valutazione d'impatto sulla protezione dei dati personali il Responsabile e/o il Titolare possono consultarsi con il proprio Responsabile della protezione dei dati, ai sensi dell'art. 35, comma 2, del Regolamento.

Il Sub-Responsabile del trattamento si impegna ad assistere il Responsabile e/o il Titolare, a livello tecnico e organizzativo, nello svolgimento della valutazione d'impatto, così come disciplinata dall'art. 35 citato, in tutte le ipotesi in cui il trattamento preveda o necessiti della preliminare valutazione di impatto sulla protezione dei dati personali o del suo aggiornamento, fatto salvo quanto previsto al par. 2.7, quarto paragrafo.

Il Sub-Responsabile dovrà operare attenendosi alle previsioni contenute nel documento condiviso di "Metodologia per la protezione dei dati e per la valutazione d'impatto", se applicabile alla tipologia di servizio erogato, rendendo disponibile al Responsabile e/o Titolare ogni utile informazione per il corretto adempimento degli obblighi di cui all'articolo 35 del Regolamento. Tale documento, allegato alle presenti istruzioni, sarà oggetto di revisione condivisa, secondo le modalità contenute nello stesso.

Il Sub-Responsabile del trattamento si impegna altresì ad assistere il Responsabile e/o il Titolare nell'attività di consultazione preventiva dell'Autorità di controllo prevista dall'articolo 36 del Regolamento.

3.2.16 MODIFICHE NORMATIVE

Nell'eventualità di qualsiasi modifica delle Norme in materia di protezione dei dati personali, il Sub-Responsabile del trattamento supporta, nel rispetto dei vincoli del Contratto e nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse, il Responsabile e/o il Titolare negli adeguamenti necessari.

3.3 RINVIO

Per tutto quanto non espressamente disciplinato nel presente atto, si richiamano gli obblighi previsti a carico del Sub-Responsabile del trattamento nel Contratto e dalle Norme in materia di protezione dei dati personali.

1. ALLEGATI

- **Allegato G1:** Metodologia per la protezione dei dati e per la valutazione d'impatto
- **Allegato G2:** Flusso di notifica di Data Breach all'Autorità di controllo

IS-00-PR-07
PAG. 1 DI 70
07 LUGLIO 2020



***METODOLOGIA
PER LA PROTEZIONE DEI DATI
E PER LA VALUTAZIONE D'IMPATTO***

<i>Strutture organizzative di competenza:</i> SGD – F. Lazzini	<i>Responsabile della redazione:</i> SGD.SIP – E. Trasatti
<i>Approvazioni:</i> DZS – F. Amadei	<i>Ente emittente:</i> DZS – F. Amadei

*METODOLOGIA
PER LA PROTEZIONE DEI DATI
E PER LA VALUTAZIONE D'IMPATTO*

IS-00-PR-07
PAG. 2 DI 70
07 LUGLIO 2020

INDICE

1. ELENCO DELLE MODIFICHE APPORTATE AL DOCUMENTO	6
2. INTRODUZIONE	7
2.1 SCOPO	7
2.2 CAMPO DI APPLICABILITÀ	7
2.3 STANDARD E NORMATIVE DI RIFERIMENTO	8
2.4 DOCUMENTAZIONE CORRELATA	8
2.5 ACRONIMI E GLOSSARIO	9
3. SINTESI DELL'APPROCCIO METODOLOGICO	12
4. FLUSSO A - ANALISI E VALUTAZIONE DEL TRATTAMENTO DA PARTE DEL TITOLARE	17
4.1 FLUSSO E CARTA DELLE RESPONSABILITÀ	17
4.2 DESCRIZIONE SISTEMATICA DEL TRATTAMENTO	18
4.3 VALUTAZIONE DI NECESSITÀ E PROPORZIONALITÀ	21
4.4 GARANZIA DEI DIRITTI DELL'INTERESSATO	22
5. FLUSSO B - ANALISI E VALUTAZIONE DEL SERVIZIO ICT DA PARTE DEL TITOLARE E DEL RESPONSABILE	24
5.1 FLUSSO E CARTA DELLE RESPONSABILITÀ	24
5.2 DESCRIZIONE SISTEMATICA DEL SERVIZIO ICT	27
5.3 IDENTIFICAZIONE E CLASSIFICAZIONE DEI DATI	30
5.4 VALUTAZIONE DEI RISCHI PER L'ORGANIZZAZIONE	31
5.5 VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTÀ DELL'INTERESSATO	32

**METODOLOGIA
PER LA PROTEZIONE DEI DATI
E PER LA VALUTAZIONE D'IMPATTO**

IS-00-PR-07
PAG. 3 DI 70
07 LUGLIO 2020

5.6	VALUTAZIONE DELLE CATEGORIE DI TRATTAMENTO A ELEVATO RISCHIO	34
5.7	IDENTIFICAZIONE DI MISURE ADEGUATE PER VALUTAZIONE DI IMPATTO (PIA)	35
5.8	CONSULTAZIONE DEL DPO	36
5.9	VALUTAZIONE COMPLESSIVA DEI RISCHI DEL SERVIZIO ICT	36
5.10	IDENTIFICAZIONE DI MISURE ADEGUATE PER LA SICUREZZA DEL SERVIZIO ICT	37
5.11	VALUTAZIONE DI ADEGUATEZZA DELLE MISURE DI SICUREZZA	38
5.12	REDAZIONE DEL DOCUMENTO “MISURE DI SICUREZZA E PRIVACY DEL SERVIZIO ICT”	38
6.	FLUSSO C - VALUTAZIONI FINALI DA PARTE DEL TITOLARE	40
6.1	FLUSSO E CARTA DELLE RESPONSABILITÀ	40
6.2	ACCETTAZIONE DEL RISCHIO E DELL'ADEGUATEZZA DELLE MISURE	41
6.3	CONSULTAZIONE DELL'AUTORITÀ DI CONTROLLO	42
ALLEGATI		44
1.	CONFORMITÀ DELLA METODOLOGIA A NORME E STANDARD	45
1.1	CONFORMITÀ ALLE LINEE GUIDA WP 248 REV.01	45
1.2	CONFORMITÀ ALLO STANDARD ISO/IEC 29134:2017	48
2.	FOURSEC	50
3.	FLUSSO B.2 - VALUTAZIONE DI RISCHI E MISURE PER IL TRATTAMENTO DA PARTE DEL TITOLARE	51
3.1	FLUSSO E CARTA DELLE RESPONSABILITÀ	51
3.2	DESCRIZIONE SINTETICA DELLE ATTIVITÀ	54
4.	VALUTAZIONE DI RISERVATEZZA E INTEGRITÀ' PER SERVIZI ICT	55
5.	VALUTAZIONE DI DISPONIBILITÀ' PER SERVIZI ICT	57

**METODOLOGIA
PER LA PROTEZIONE DEI DATI
E PER LA VALUTAZIONE D'IMPATTO**

IS-00-PR-07
PAG. 4 DI 70
07 LUGLIO 2020

6. VALUTAZIONE DEI RISCHI PER GLI INTERESSATI RELATIVI AI DATI TRATTATI	60
6.1 MINACCE E SCENARI DI RISCHIO	60
6.2 CRITERI PER LA VALUTAZIONE DELL'IMPATTO	61
6.3 VALUTAZIONE DELL'IMPATTO	62
6.4 VALUTAZIONE DELLA PROBABILITÀ DI ACCADIMENTO	65
6.5 VALUTAZIONE DEL RISCHIO INTRINSECO PER DIRITTI E LIBERTÀ DELL'INTERESSATO	66
7. VALUTAZIONE DEI RISCHI PER GLI INTERESSATI RELATIVI ALLE CATEGORIE DI TRATTAMENTO	69

INDICE DELLE TABELLE

Tabella 1 - Flusso A: Matrice RACI	18
Tabella 2 - Informazioni descrittive del trattamento	19
Tabella 3 - Schema di supporto alla compilazione delle categorie	21
Tabella 4 – Flusso B: Matrice RACI	26
Tabella 5 – Informazioni descrittive del Servizio ICT	28
Tabella 6 – Schema di supporto alla compilazione delle categorie.....	30
Tabella 7 – Classificazione privacy del dato.....	31
Tabella 8 - Matrice per la valorizzazione dei rischi per l'interessato	33
Tabella 9 – Applicazione misure PIA.....	36
Tabella 10 - Rischio intrinseco del Servizio ICT	37
Tabella 11 – Applicazione misure per la sicurezza del Servizio ICT	38
Tabella 12 - Flusso C: Matrice RACI	41
Tabella 13 - Criteri di accettabilità per la PIA secondo WP 248.....	47
Tabella 14 – Analisi dei requisiti dello standard ISO/IEC 29134	49
Tabella 15 – Flusso B2: Matrice RACI	53
Tabella 16 – Valutazione del rischio per perdita di Riservatezza e Integrità	55
Tabella 17 – Legenda per la valutazione del rischio di perdita di Riservatezza e Integrità	56
Tabella 18 – Valutazione del rischio per perdita di Disponibilità	57
Tabella 19 - Legenda per la valutazione del rischio di perdita di Disponibilità	59
Tabella 20 – Minacce e scenari di rischio.....	61
Tabella 21 – Legenda per la valutazione impatto	64
Tabella 22 – Legenda per la valutazione probabilità di accadimento.....	65
Tabella 23 - Stima del rischio intrinseco per i diritti e le libertà dell'interessato.....	68

**METODOLOGIA
PER LA PROTEZIONE DEI DATI
E PER LA VALUTAZIONE D'IMPATTO**

IS-00-PR-07
PAG. 5 DI 70
07 LUGLIO 2020

Tabella 24 - Categorie trattamento ad alto rischio per diritti e libertà interessato.....70

1. ELENCO DELLE MODIFICHE APPORTATE AL DOCUMENTO

Variazioni rispetto alla precedente versione				
Struttura proponente	Pagina	Paragrafo	Descrizione modifiche	Motivazione
DZS		5.7 5.10 5.11 6.2	Modifica delle modalità di applicazione delle misure di sicurezza eliminando il caso di "misura non applicata" Modifica dei criteri di valutazione di adeguatezza delle misure applicate Modifica dei criteri di accettazione di adeguatezza delle misure applicate	Definizione di valori di applicabilità delle misure di sicurezza necessari per mitigare i rischi.
DZS		5.4	Rischio per l'organizzazione valutato sia in termini di <i>probabilità</i> di accadimento dell'evento negativo che dell'impatto conseguente	Adeguamento ai criteri di valutazione del rischio per l'interessato

2. INTRODUZIONE

Il 25 maggio 2016 è entrato in vigore il “Regolamento 2016/679 del Parlamento europeo e del Consiglio, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati” (di seguito Regolamento) [2].

Il Regolamento ha l'obiettivo di garantire una disciplina sulla protezione dei dati personali uniforme e omogenea nell'Unione europea e ha una portata altamente innovativa rispetto alle precedenti normative in ambito privacy poiché sostituisce gli adempimenti di natura formale burocratica con attività sostanziali finalizzate a una maggiore responsabilizzazione e consapevolezza dei rischi.

Il Regolamento è definitivamente applicato in tutti i Paesi Ue dal 25 maggio 2018; in Italia il d.lgs 101/2018 [7], in vigore dal 19 settembre 2018, modifica il Codice per la protezione dei dati personali (d.lgs 196/2003) adeguandolo alla nuova normativa.

Il Regolamento introduce requisiti innovativi per la protezione dei dati personali, con ricadute organizzative, operative e tecnologiche che riguardano i principali processi di gestione del dato. Tra le principali novità vi è l'obbligo per il Titolare del trattamento di procedere a una valutazione d'impatto che, secondo quanto recita l'art. 35, deve essere compiuta dal titolare quando «un tipo di trattamento [...] può presentare un rischio elevato per i diritti e le libertà delle persone fisiche».

2.1 SCOPO

Scopo del presente documento è descrivere la metodologia di protezione dei dati personali, ai sensi di quanto previsto dall'art. 25 del Regolamento, che si integra nel processo di produzione del software di Sogei. In tale contesto viene inoltre descritta la valutazione d'impatto, ai sensi di quanto previsto dall'art. 35 del Regolamento, per i trattamenti di dati personali che presentino un rischio elevato per i diritti e le libertà degli interessati. In tale metodologia sono integrati anche i criteri di valutazione dei rischi per l'organizzazione al fine di definire le misure di sicurezza complessive per le informazioni trattate.

2.2 CAMPO DI APPLICABILITÀ

La metodologia descritta in questo documento si applica allo sviluppo dei Servizi ICT erogati da Sogei per i Dipartimenti del MEF (Economia) e altri enti/amministrazioni (Altre convenzioni).

**METODOLOGIA
PER LA PROTEZIONE DEI DATI
E PER LA VALUTAZIONE D'IMPATTO**

IS-00-PR-07
PAG. 8 DI 70
07 LUGLIO 2020

Tale metodologia può essere applicata anche a trattamenti di tipo cartaceo o basati su strumenti informatici di office automation, valutandone in modo analogo i rischi ma prendendo in considerazione misure di sicurezza specifiche per tali ambiti (Allegato 3 FLUSSO B.2 - VALUTAZIONE DI RISCHI E MISURE PER IL TRATTAMENTO).

2.3 STANDARD E NORMATIVE DI RIFERIMENTO

- [1] D.Lgs. n. 196/03 Codice in materia di protezione dei dati personali;
- [2] Regolamento Ue n. 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati che abroga la direttiva 95/46/CE (Regolamento Generale sulla protezione dei dati);
- [3] Documento WP 243 – Linee guida sui responsabili della protezione dei dati (RPD) del 13 dicembre 2016;
- [4] Documento WP 248 rev. 0.1 – Linee guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento “possa presentare un rischio elevato” ai sensi del regolamento 2016/679 del 4 ottobre 2017;
- [5] Standard ISO/IEC 29134:2017 Information technology -- Security techniques - - Guidelines for privacy impact assessment;
- [6] Rettifiche del Regolamento, pubblicate sulla Gazzetta Ufficiale dell'Unione europea 127 del 23 maggio 2018;
- [7] Decreto legislativo 10 agosto 2018, n. 101 recante “Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (*regolamento generale sulla protezione dei dati*)” approvato dal Consiglio dei Ministri n. 14 dell’8 agosto 2018.

2.4 DOCUMENTAZIONE CORRELATA

- [8] Task Support System, pubblicato sulla intranet aziendale;
- [9] IS-00-PR-05 - FOURSec - Misure per la protezione dei dati di trattamenti e Servizi ICT;
- [10]IS-18-PR-01 - Misure di sicurezza e privacy del Servizio ICT.

2.5 ACRONIMI E GLOSSARIO

- **Autorità di controllo o Autorità Garante:** l'autorità pubblica indipendente istituita da uno Stato UE ai sensi dell'articolo 51 del GDPR;
- **Applicazione:** Collezione integrata di procedure automatizzate e dati che forniscono supporto ad un obiettivo applicativo; è formata da uno o più componenti, moduli, o sottosistemi;
- **Dato personale:** «Qualsiasi informazione riguardante una persona fisica identificata o identificabile (“interessato”); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale» (GDPR, art. 4 punto 1);
- **Danno:** conseguenza di un evento che compromette la protezione delle persone fisiche con riguardo al trattamento dei loro dati personali;
- **DPO (Data Protection Officer) o Responsabile della Protezione dei dati personali (RPD):** il soggetto nominato dal Titolare o dal Responsabile del trattamento in presenza di trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala oppure nel trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e a reati;
- **FOURSec (Framework to Organize Under Rules Security):** framework multicomppliance costituito da 260 misure di sicurezza che sintetizzano circa 600 singoli requisiti derivati da normative, standard, istruzioni contrattuali e politiche interne [9];
- **GDPR:** General Data Protection Regulation o Regolamento europeo n.679/2016, di seguito anche **Regolamento** [2]
- **Impatto:** insieme delle conseguenze in termini di danni o perdite che il verificarsi di un evento ha sul pieno raggiungimento dell'obiettivo della protezione delle persone fisiche con riguardo al trattamento dei loro dati personali;
- **Interessato:** la persona fisica cui si riferiscono i dati personali;
- **Minaccia:** causa potenziale di un rischio di compromissione della protezione delle persone fisiche con riguardo al trattamento dei loro dati personali;
- **Misure di sicurezza:** insieme degli accorgimenti tecnici e organizzativi volti a ridurre al minimo il rischio che i dati vadano distrutti o persi anche in modo accidentale, che le persone non autorizzate possano avere accesso ai dati e che siano effettuati trattamenti contrari alle norme di legge o diversi da quelli per cui i dati sono stati raccolti;

- **Owner del trattamento:** la persona di riferimento per un determinato trattamento. Risponde al Titolare del trattamento;
- **Privacy by default:** il principio secondo il quale il Titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento;
- **Privacy by design:** il principio secondo il quale il Titolare del trattamento mette in atto misure tecniche e organizzative adeguate, volte ad attuare in modo efficace i principi di protezione dei dati fin dalla progettazione del trattamento per tutelare i diritti degli interessati;
- **Privacy Impact Assessment (PIA) o Valutazione d'impatto:** l'azione che il Titolare del trattamento deve effettuare prima di procedere a un trattamento di dati personali per tutelare gli interessati in caso di rischio elevato per i loro diritti e le loro libertà;
- **Probabilità:** possibilità del concretizzarsi di un evento;
- **Registro dei trattamenti:** il documento che contiene tutte le informazioni base del trattamento che deve essere redatto, secondo le rispettive responsabilità e competenze, sia dal Titolare sia dal Responsabile del trattamento ed esibito su richiesta all'Autorità di controllo;
- **Responsabile del trattamento:** la persona fisica o giuridica, l'autorità pubblica, il Servizio ICT o altro organismo che tratta dati personali per conto del Titolare del trattamento (di seguito anche **Responsabile**);
- **Responsabile del Servizio ICT:** è il riferimento per tutto ciò che riguarda il Servizio ICT e risponde al Titolare o al Responsabile del trattamento ove designato;
- **Rischio intrinseco:** incertezza sul raggiungimento dell'obiettivo della protezione dei dati, che si verifica come combinazione dell'impatto di un evento e della probabilità del suo verificarsi;
- **Rischio residuo:** rischio intrinseco valutato dopo il suo trattamento, ovvero dopo l'applicazione delle misure di sicurezza;
- **Scenario di rischio:** descrizione generale e/o specifica di un insieme di minacce;
- **Servizio ICT:** insieme di applicazioni informatiche omogenee (identificate da uno o più kit di applicazione) e della relativa infrastruttura tecnologica, in grado di supportare lo svolgimento di un processo/sottoprocesso amministrativo – e, nei casi previsti dalla normativa (GDPR) connesso al “Trattamento” dei dati e per le quali sia comunque opportuno esercitare il controllo/monitoraggio (prestazioni, costi, consumi, ecc.) a livello di unica entità;

- **Titolare del trattamento:** la persona fisica o giuridica, l'autorità pubblica, il Servizio ICT o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali (di seguito anche **Titolare**);
- **Trattamento:** «Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, la diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione» (GDPR, art. 4);
- **Valutazione del rischio:** il processo di identificazione, stima del livello di rischio, valutazione e trattamento del rischio. In ambito GDPR il processo di analisi del rischio si svolge tenuto conto della natura dei dati, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche (GDPR, art. 24.1).

3. SINTESI DELL'APPROCCIO METODOLOGICO

Il processo di valutazione dei rischi supporta il Titolare e il Responsabile del trattamento a mettere in atto misure tecniche e organizzative volte a garantire un livello di sicurezza adeguato al rischio, conformemente ai principi sulla protezione dei dati dettati dal Regolamento [2].

La presente metodologia a supporto del processo integra la valutazione dei rischi per i diritti e le libertà dell'interessato ai sensi di quanto previsto dall'art 25 del Regolamento [2] (*privacy by design*) e dall'art. 35 (*Privacy Impact Assessment - PIA*) con la valutazione dei rischi relativi alla sicurezza delle informazioni secondo lo standard ISO/IEC 27001:2013.

La metodologia descritta nel documento è stata sviluppata sulla base delle prescrizioni contenute nel Regolamento ([2]), delle linee guida del documento WP 248 [4] e tenendo conto dell'approccio descritto nello standard ISO/IEC 29134 [4].

La presente metodologia sarà fatta oggetto di revisione periodica almeno annuale, e comunque nei casi in cui se ne ravvisi la necessità in relazione a novità normative o interpretative.

Il documento è focalizzato sulla metodologia di valutazione dei rischi collegati ad asset di tipo informatico (Servizi ICT) a supporto del trattamento e, conseguentemente, è integrata nel processo di sviluppo del software. Può però essere generalizzata a trattamenti di archivi cartacei o supportati da strumenti informatici di office automation prevedendo idonee misure di sicurezza.

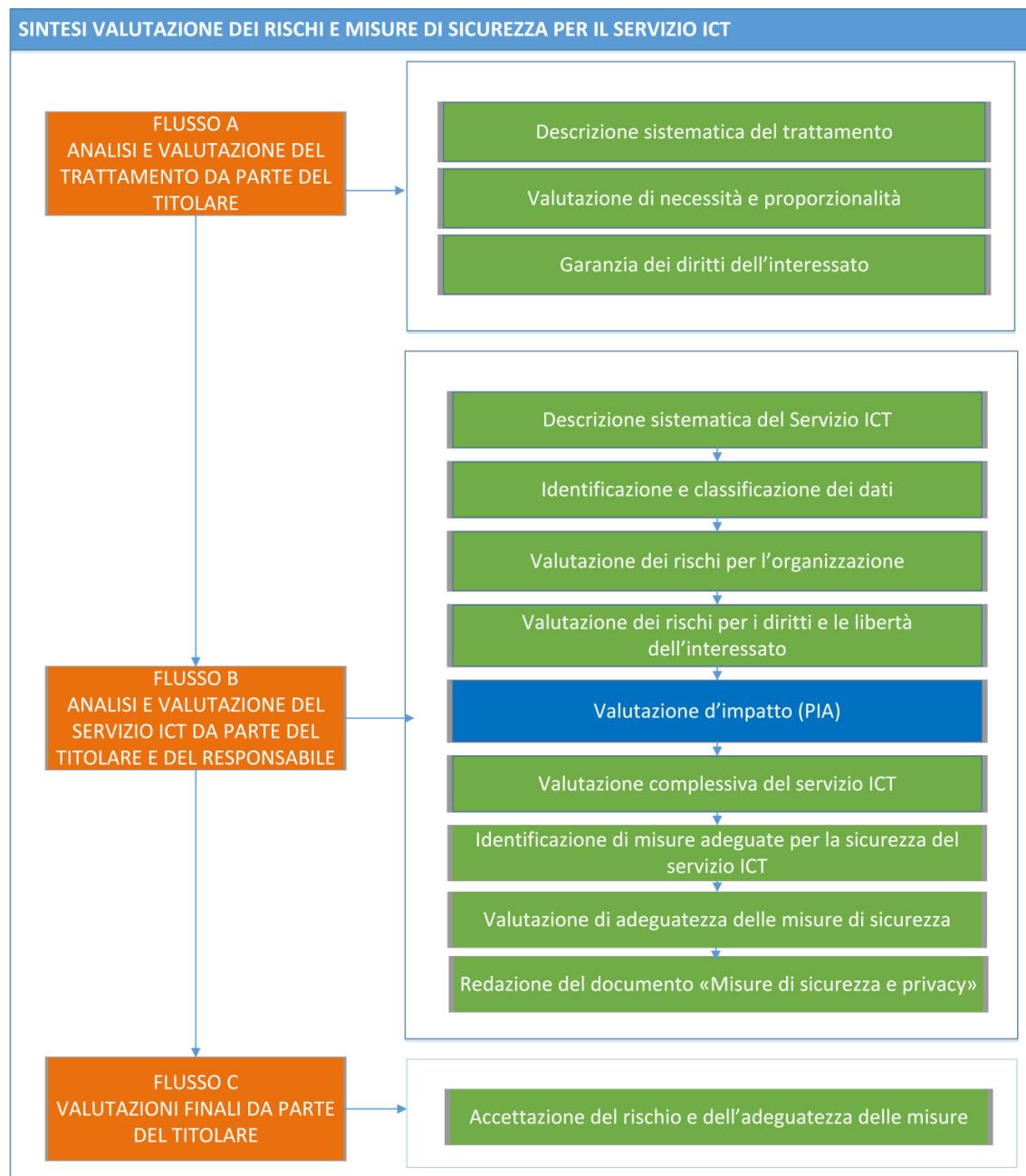
Di seguito il flusso di sintesi¹ per la valutazione dei rischi e delle misure di sicurezza per il Servizio ICT, suddiviso in tre parti:

FLUSSO A. Analisi e valutazione del trattamento da parte del Titolare

FLUSSO B. Analisi e valutazione del Servizio ICT da parte del Titolare e del Responsabile, ove designato

FLUSSO C. Valutazioni finali del Titolare.

¹ Nel flusso sono rappresentate, in colore diverso, le attività che riguardano la privacy by design e la sicurezza delle informazioni (colore verde) e quelle che riguardano la valutazione di impatto (colore blu).



RUOLI E RESPONSABILITÀ'

Il ruolo di Titolare è assunto dall'Amministrazione per cui Sogei opera come Responsabile esterno in forza di un rapporto contrattuale o da Sogei stessa nel caso di trattamenti di propria competenza.

L'Owner del trattamento e il Responsabile del Servizio ICT operano rispettivamente per conto del Titolare e del Responsabile del trattamento, ove sia designato, ad esempio quando il Servizio ICT è erogato da Sogei per conto dell' Amministrazione.

Il DPO del Titolare fornisce, se richiesto, un parere relativamente alla valutazione di impatto (PIA) in corso e vigila sul suo svolgimento.

FLUSSO A

La prima parte del processo comprende le attività che riguardano la progettazione del trattamento, in particolare:

- descrizione sistematica del trattamento (par. 4.2);
- valutazione di necessità e proporzionalità del trattamento (par. 4.3);
- garanzie per i diritti degli interessati (par. 4.4).

Tali attività sono svolte dall'Owner del trattamento per conto del Titolare fin dalla progettazione iniziale del trattamento per consentirne una valutazione complessiva e dimostrarne la conformità al Regolamento [2] implementando gli strumenti necessari per consentire agli interessati di esercitare i loro diritti.

FLUSSO B

La seconda parte del processo comprende le attività che riguardano la progettazione del Servizio ICT a supporto del trattamento:

- descrizione sistematica del Servizio ICT (par. 5.2);
- identificazione e la classificazione dei dati (par. 5.3);
- valutazione dei rischi per l'organizzazione (par.5.4);
- valutazione dei rischi per i diritti e le libertà dell'interessato (par.5.5);
- valutazione d'impatto (PIA)
 - valutazione delle categorie di trattamento ad elevato rischio (par.5.6)
 - identificazione di misure adeguate per valutazione di impatto (par. 5.7)
 - consultazione del DPO (par. 5.8)
- valutazione complessiva dei rischi del Servizio ICT (par. 5.9)
- identificazione di misure adeguate per la sicurezza del Servizio ICT (par. 5.10)
- valutazione di adeguatezza delle misure di sicurezza (par. 5.11)
- redazione del documento "Misure di sicurezza e privacy del Servizio ICT" (par. 5.12).

Tali attività sono svolte dall'Owner del trattamento e dal Responsabile del Servizio ICT fin dalla fase di analisi dei requisiti del Servizio ICT e consistono nell'individuazione di misure di sicurezza adeguate ai rischi valutati rispetto alle caratteristiche del Servizio ICT e alla tipologia dei dati trattati.

La valutazione d'impatto (PIA) è obbligatoria a condizione che il trattamento di dati personali presenti un rischio potenzialmente elevato per i diritti e le libertà degli interessati. Ne consegue che occorre individuare i criteri per valutare la presenza di un rischio potenzialmente elevato relativo a eventi illeciti di accesso, diffusione, modifica, indisponibilità o perdita dei dati personali.

Il Gruppo di lavoro Articolo 29 per la protezione dei dati - organo consultivo della Commissione Ue su questa materia - ha emesso le linee guida WP248 [4] in tema di PIA e in esse vengono proposte 9 categorie di trattamento che individuano un potenziale rischio elevato. Il criterio utilizzato nella metodologia qui presentata valuta la presenza di un rischio potenzialmente elevato se il Servizio ICT rientra in almeno due delle categorie definite ad alto rischio dalle linee guida WP248.

Nel caso di rischio elevato per l'interessato si procede dunque con lo svolgimento di PIA individuando misure di sicurezza adeguate ai rischi.

Riguardo alla valutazione complessiva dei rischi del Servizio ICT, il calcolo viene effettuato combinando i rischi dell'organizzazione inerenti alla perdita di riservatezza, integrità e disponibilità delle informazioni e i rischi per gli interessati. Le misure di protezione adeguate al rischio complessivo del Servizio ICT sono state individuate nell'ambito del framework multicomppliance FOURSec (*Framework to Organize Under Rules Security*) [9].

Una volta valutato il rischio complessivo del Servizio ICT, il Responsabile del Servizio ICT identifica le misure di sicurezza tecnicamente applicabili; l'Owner del trattamento con il Responsabile del Servizio ICT specifica se le misure di sicurezza sono da applicare nell'intervento in corso o successivamente in appositi piani di rientro.

Il Responsabile del Servizio ICT compila infine il documento "Misure di Sicurezza e Privacy del Servizio ICT" [10] per documentare le valutazioni dei rischi e della adeguatezza delle misure di sicurezza.

FLUSSO C

La terza parte del processo comprende le attività che riguardano le valutazioni finali dell'Owner del trattamento (par. 6.2) il quale può:

- approvare il documento "Misure di Sicurezza e Privacy del Servizio ICT" confermando l'adeguatezza delle misure in relazione ai rischi e autorizzare il Responsabile del Servizio ICT a procedere all'implementazione;
- non approvare il documento "Misure di Sicurezza e Privacy del Servizio ICT" e procedere alla ridefinizione degli elementi del servizio, misure di sicurezza e requisiti applicativi, eventualmente ricorrendo ad un riesame interno, coinvolgendo superiori livelli di responsabilità nell'organizzazione e, se del caso, il proprio DPO.

Oggetto di valutazione e approvazione sono in particolare i seguenti elementi:

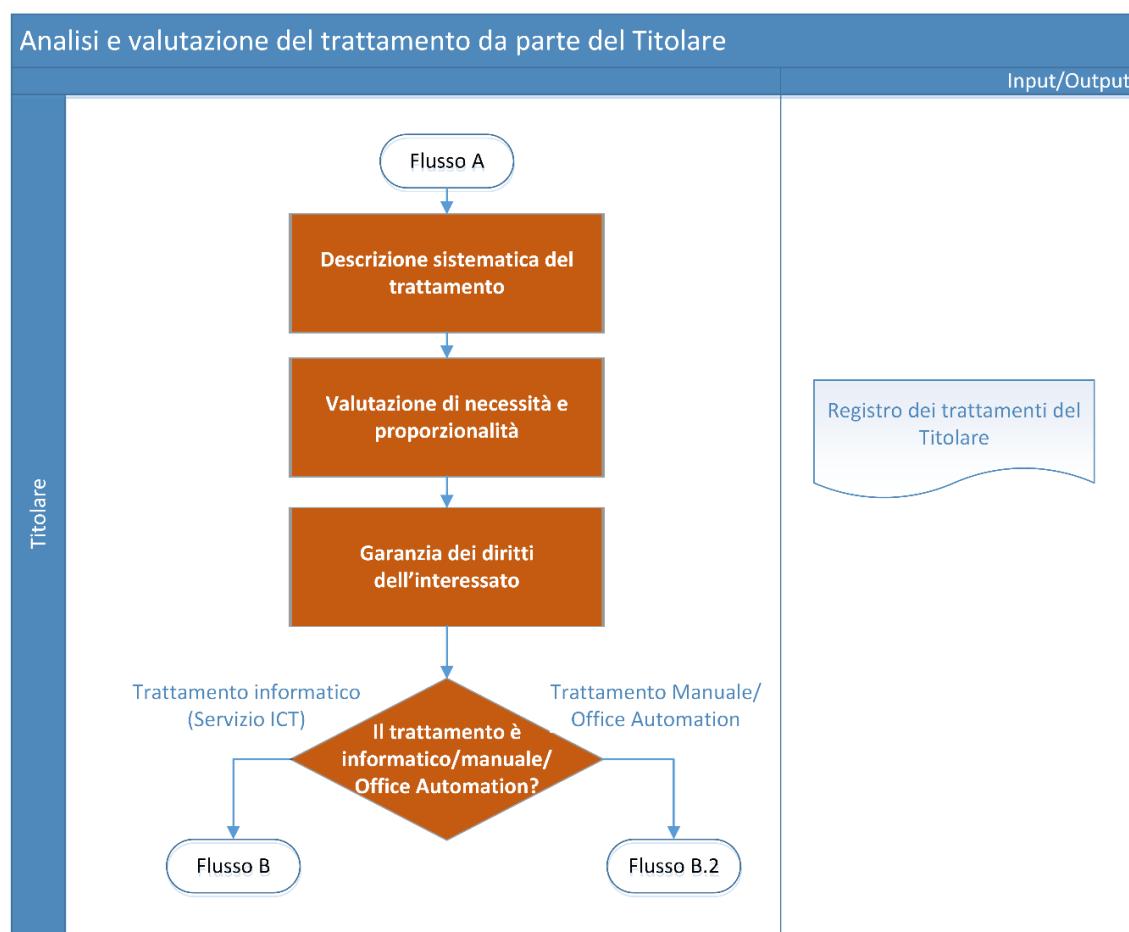
- rischi per i diritti e le libertà degli interessati - compresa la valutazione d'impatto, ove necessaria - relativi al trattamento di dati personali;
- rischi per l'organizzazione del Titolare, relativi alla sicurezza delle informazioni elaborate;
- adeguatezza delle misure di sicurezza da applicare per mitigare i rischi.

Nel caso in cui, a seguito di un'eventuale valutazione d'impatto, l'Owner del trattamento ritenga che le misure per mitigare il rischio per gli interessati non siano adeguate è necessario consultare, tramite il DPO, l'Autorità di controllo (par. 6.3), prima dell'inizio delle attività di sviluppo del Servizio ICT.

4. FLUSSO A - ANALISI E VALUTAZIONE DEL TRATTAMENTO DA PARTE DEL TITOLARE

4.1 FLUSSO E CARTA DELLE RESPONSABILITÀ

Di seguito è riportato il flusso di analisi e valutazione del trattamento di dati personali.



Le informazioni raccolte nelle diverse fasi del flusso confluiscono nel Registro dei trattamenti del Titolare.

La tabella riportata di seguito elenca le attività di analisi e valutazione di un trattamento e, per ognuna, le responsabilità secondo la matrice RACI².

Nome Attività	Ruoli / Responsabilità		
	Resp. Servizio ICT	Owner trattamento	DPO (Titolare/Responsabile)
Descrizione sistematica del trattamento	C	R	I
Valutazione di necessità e proporzionalità	I	R	I
Garanzia dei diritti dell'interessato	I	R	I

Tabella 1 - Flusso A: Matrice RACI

4.2 DESCRIZIONE SISTEMATICA DEL TRATTAMENTO

L'Owner del trattamento descrive le caratteristiche del trattamento, come indicato in Tabella 2, seguendo lo schema di supporto alla compilazione riportato in Tabella 3.

DATI IDENTIFICATIVI DEL TRATTAMENTO	
Processo	<i>Processo all'interno del quale viene realizzato il trattamento</i>

² La matrice è organizzata secondo il modello RACI che prevede quattro ruoli:

R = Responsible. Esegue l'attività e ne è responsabile. Per la stessa attività è ammessa una responsabilità condivisa, ossia è possibile la presenza di più "R".

A = Accountable. Coordina, supervisiona e approva i vari task che compongono l'attività; può eseguirne alcuni ed è responsabile anche degli aspetti economici. È unico per l'attività e deve essere individuato nel caso vi sia la presenza di più "R".

C = Consulted. È consultato poiché possiede informazioni e/o capacità necessarie per portare a termine l'attività.

I = Informed. È informato dei risultati dell'attività.

Trattamento	<i>Identificativo, nome, descrizione funzionale, informazioni sulla struttura referente del trattamento</i>
Titolare	<i>Soggetto che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali</i>
Responsabile	<i>Informazioni sul Responsabile del trattamento (es. nome, indirizzo, contatti, etc.)</i>
Contitolare	<i>Informazioni (es. nome, indirizzo, contatti, etc.) sul soggetto che, unitamente al Titolare, determina le finalità e i mezzi del trattamento</i>
Strumenti	<i>Strumenti utilizzati per il trattamento anche in base al tipo di trattamento (es. servizi informatici, servizi informatici non software, servizi software, servizi infrastrutturali)</i>
IDENTIFICAZIONE E CLASSIFICAZIONE DEI DATI	
Dati	<i>Categorie di dati personali</i>
Termini di cancellazione	<i>Tempi o criteri di cancellazione dei dati</i>
CARATTERISTICHE GENERALI DEL TRATTAMENTO	
Tipologia	<i>Tipologia del trattamento (es. informatico, cartaceo o eseguito su postazioni di lavoro tramite strumenti di office automation)</i>
Finalità	<i>Scopo perseguito con il trattamento</i>
Fondamenti di licetità	<i>Base giuridica e contrattuale che legittima il trattamento dei dati</i>
Interessati	<i>Categorie di persone fisiche cui si riferiscono i dati</i>
Destinatari	<i>Categorie destinatari di comunicazioni e relativa descrizione</i>
Trasferimenti dati	<i>Trasferimento dati extra Ue e relative garanzie</i>

Tabella 2 - Informazioni descrittive del trattamento

VALORIZZAZIONE CATEGORIE	
Dati	<p><i>Dati personali comuni anagrafici contabili e fiscali, inerenti possidenze e riscossione inerenti il rapporto di lavoro tracciamenti dati inerenti situazioni giudiziarie civili, amministrative, tributarie</i></p> <p><i>Dati personali specifici geolocalizzazione audio/video/foto dati di profilazione</i></p>

VALORIZZAZIONE CATEGORIE	
	<p><u>Dati personali finanziari</u> dati relativi all'esistenza di rapporti finanziari (coordinate bancarie, consistenze saldi, movimenti, giacenza media, etc.)</p> <p><u>Dati personali sensibili</u> convincioni religiose o filosofiche/opinioni politiche/origine razziale/adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale</p> <p><u>Dati personali ipersensibili</u> stato di salute, assistenza sanitaria, orientamento/vita sessuale genetici</p> <p><u>Dati personali giudiziari</u> casellario giudiziale qualità di indagato/imputato o altre situazioni giudiziarie (condanne penali e reati o connesse misure di sicurezza)</p> <p><u>Dati personali biometrici</u> impronte digitali altre caratteristiche biometriche firma grafometrica</p>
Tipologia	<p>Supportato da Servizi ICT</p> <p>Supportato da strumenti di office automation</p> <p>Supportato da archivi cartacei</p>
Finalità	<p>Gestione amministrativo contabile</p> <p>Informazione/formazione, istruzione, cultura</p> <p>Ricerca e statistica</p> <p>Settore economico</p> <p>Settore sanitario</p> <p>Settore fiscale, tributario</p> <p>Gestione della sicurezza fisica (es. sedi, locali,...)</p> <p>Applicazione contratti di lavoro</p>
Fondamenti di licetà	<p>Consenso dell'interessato</p> <p>Esecuzione di un contratto con l'interessato</p> <p>Obbligo legale per il titolare</p> <p>Salvaguardia interessi vitali dell'interessato o altra persona fisica</p> <p>Esecuzione di un compito di interesse pubblico o pubblici poteri del titolare derivante da normativa nazionale</p> <p>Esecuzione di un compito di interesse pubblico o pubblici poteri del titolare derivante da regolamento UE</p> <p>Altri fondamenti connessi al trattamento di categorie particolari di dati personali - art. 9 par. 2</p> <p>Richiesta pubblica autorità</p> <p>Statuto</p>
Interessati	<p>Cittadini</p> <p>Personale dipendente e familiari</p>

VALORIZZAZIONE CATEGORIE	
	<i>Contraenti, offerenti e candidati</i>
	<i>Rappresentanti e dipendenti di enti/istituzioni (associazioni di categoria/ordini professionali, ecc.)</i>
	<i>Componenti organi dell'Ente</i>
	<i>Persone fisiche extra UE</i>
	<i>Visitatori</i>
	<i>Minorenni</i>
	<i>Operatori economici</i>
	<i>Professionisti, intermediari</i>
	<i>Altri soggetti - Persone fisiche</i>
Destinatari	<i>Persona fisica</i>
	<i>Persona giuridica</i>
	<i>Pubblica amministrazione</i>
	<i>Autorità pubblica</i>
Trasferimenti dati	<i>Paese terzo o organizzazione internazionale</i>
	<i>Garanzie e autorizzazioni ex art. 46 del Regolamento</i>

Tabella 3 - Schema di supporto alla compilazione delle categorie

L'uso di codici di condotta (art. 35, par. 8 del Regolamento) non è referenziabile allo stato dell'arte, in quanto non risultano approvati, al momento, schemi o codici applicabili allo specifico contesto in cui opera Sogei (i.e. rapporti con la PA).

4.3 VALUTAZIONE DI NECESSITÀ E PROPORZIONALITÀ

L'Owner del trattamento esegue una valutazione formale di necessità, pertinenza e proporzionalità dei dati rispetto alle finalità del trattamento e descrive:

- perché i dati raccolti sono necessari, rispetto alle finalità del trattamento e ai fondamenti di liceità;
- perché i dati raccolti non sono eccedenti rispetto alle finalità e quindi, secondo il principio di minimizzazione, si raccolgono e trattano, per impostazione predefinita del trattamento (ovverosia *by default*) solo i dati minimi indispensabili per le finalità specifiche;
- in che modo che i dati trattati sono adeguati al raggiungimento degli obiettivi del trattamento;
- in quale modo i dati sono corretti e aggiornati;
- perché i dati sono limitati alla sola realizzazione delle finalità, nel rispetto dei tempi e dei criteri di cancellazione.

4.4 GARANZIA DEI DIRITTI DELL'INTERESSATO

L'Owner del trattamento dimostra di aver definito e di garantire i diritti degli interessati, in relazione allo specifico trattamento, al fine di fornire i mezzi per esercitarli agevolmente, specificando anche le motivazioni che eventualmente ne impediscono l'attuazione. Di seguito è elencato l'insieme di tali diritti e alcuni esempi a titolo di chiarimento:

- informazioni fornite agli interessati, ad esempio l'interessato è posto a conoscenza almeno dell'identità del titolare e delle finalità del trattamento cui sono destinati i dati (*informativa*), al fine di manifestare l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento (*consenso*);
- diritto di accesso e portabilità dei dati, ad esempio l'interessato ha il diritto di ottenere la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso di ottenere l'accesso a tali dati. Inoltre l'interessato ha il diritto di ricevere tali dati in un formato strutturato, di uso comune e leggibile da dispositivo automatico e, se possibile in funzione delle specificità del trattamento, di trasmettere tali dati a un altro Titolare;
- diritto di rettifica e cancellazione, ad esempio l'interessato ha il diritto di ottenere la correzione e l'integrazione dei dati personali inesatti o incompleti che lo riguardano senza ingiustificato ritardo. In casi particolari e in base alle caratteristiche specifiche del trattamento, ha il diritto di ottenere la cancellazione dei dati personali che lo riguardano;
- diritto di opposizione e limitazione del trattamento, in casi particolari e in base alle caratteristiche specifiche del trattamento, l'interessato ha il diritto di opporsi al trattamento per motivi connessi alla sua situazione particolare e, di conseguenza, il Titolare si astiene, anche temporaneamente, dal trattare ulteriormente i dati, salvo dimostrare l'esistenza di motivi legittimi cogenti che prevalgono sui diritti e sulle libertà dell'interessato oppure per l'accertamento l'esercizio o la difesa di un diritto in sede giudiziaria;
- rapporti con i Responsabili del trattamento, ad esempio se il Titolare del trattamento designa i Responsabili, è necessario che questi presentino garanzie sufficienti per mettere in atto misure adeguate a garantire la tutela dei diritti dell'interessato;
- garanzie per i trasferimenti internazionali dei dati, ad esempio l'interessato ha diritto alla protezione dei dati personali che lo riguardano e ad appropriate garanzie, anche nel caso in cui i dati fossero trasferiti verso un Paese terzo o un'organizzazione internazionale;
- consultazione preventiva dell'Autorità di controllo (par. 6.3), ad esempio se dalla valutazione d'impatto sulla protezione dei dati risulta un rischio elevato per i diritti e le libertà delle persone fisiche, si consulta l'Autorità di controllo prima dell'inizio delle attività di trattamento. L'Autorità di controllo fornisce un

parere in merito al fine di garantire che il trattamento rispetti in ogni caso il Regolamento e può avvalersi dei propri poteri, tra cui rivolgere ammonimenti o ammonizioni, imporre limitazioni o divieti. L'Autorità di controllo, inoltre, viene notificata di eventuali violazioni di dati personali (*data breach*) e può ingiungere al Titolare di comunicare all'interessato la violazione stessa.

5. FLUSSO B - ANALISI E VALUTAZIONE DEL SERVIZIO ICT DA PARTE DEL TITOLARE E DEL RESPONSABILE

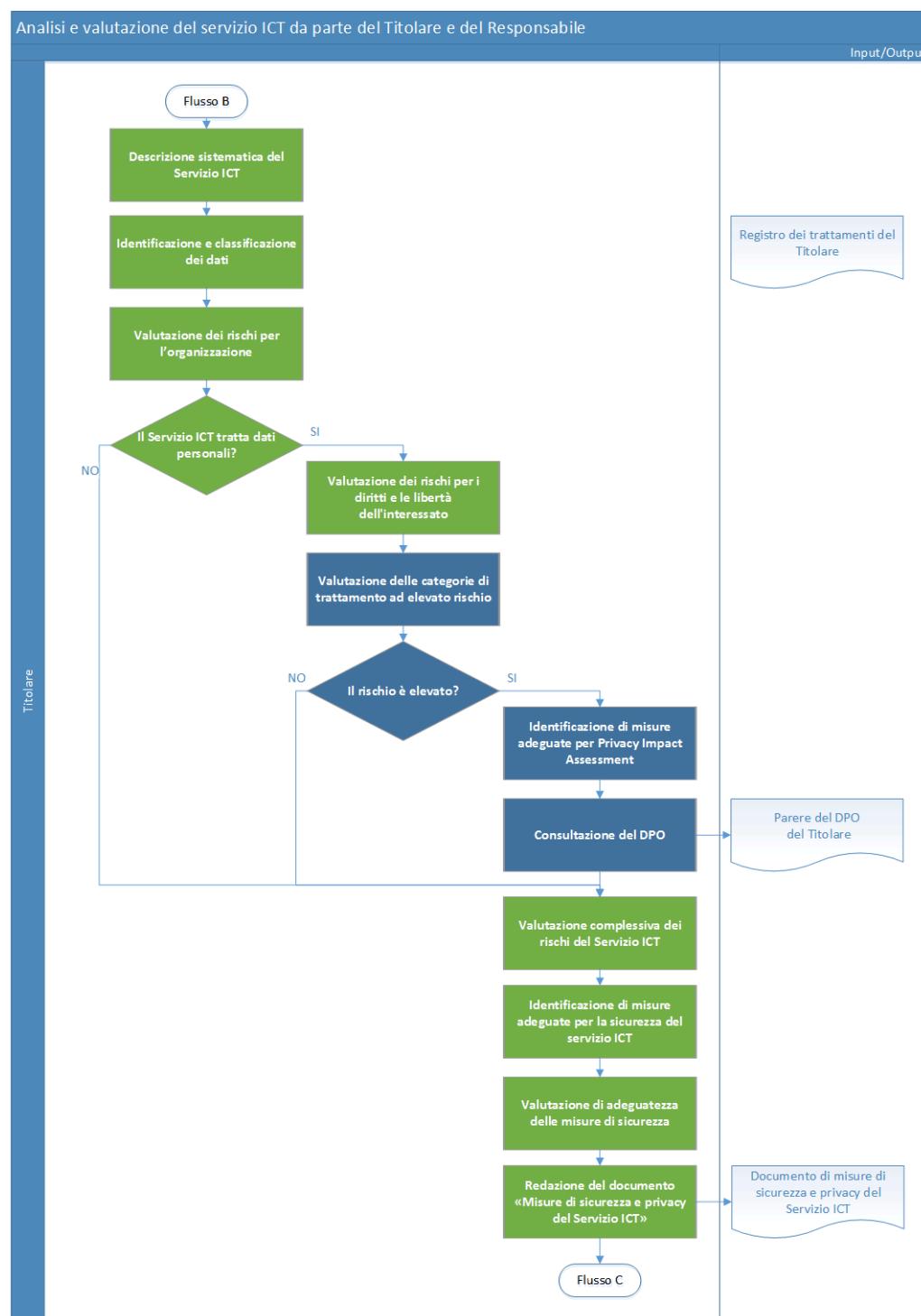
5.1 FLUSSO E CARTA DELLE RESPONSABILITÀ

Di seguito è riportato il flusso di valutazione³, relativamente al Servizio ICT, dei rischi per i diritti e le libertà degli interessati, compresa la valutazione d'impatto (PIA), e dei rischi relativi alla sicurezza delle informazioni.

³ Nel flusso sono rappresentate, in colore diverso, le attività che riguardano la privacy by design e la sicurezza delle informazioni (colore verde) e quelle che riguardano la valutazione di impatto (colore blu).

**METODOLOGIA
PER LA PROTEZIONE DEI DATI
E PER LA VALUTAZIONE D'IMPATTO**

IS-00-PR-07
PAG. 25 DI 70
07 LUGLIO 2020



La tabella seguente elenca le attività e le responsabilità secondo la matrice RACI.⁴

Nome Attività	Ruoli / Responsabilità		
	Responsabile Servizio ICT	Owner trattamento	DPO Titolare/Responsabile
Descrizione sistematica del Servizio ICT	C	A	I
Identificazione e classificazione dei dati	C	A	I
Valutazione dei rischi per l'organizzazione	C	A	-
Valutazione dei rischi per i diritti e le libertà degli interessati	C	A	I
Valutazione delle categorie di trattamento ad elevato rischio	C	A	I
Identificazione di misure adeguate per privacy impact assessment	R	A	I
Consultazione del DPO	I	A	C
Valutazione complessiva dei rischi del Servizio ICT	C	A	I
Identificazione di misure adeguate per la sicurezza del Servizio ICT	R	A	I
Valutazione di adeguatezza delle misure di sicurezza	R	A	I
Redazione del documento "Misure di sicurezza e privacy del Servizio ICT..."	R	A	I

Tabella 4 – Flusso B: Matrice RACI

⁴ La matrice è organizzata secondo il modello RACI che prevede quattro ruoli:

R = Responsible. Esegue l'attività e ne è responsabile. Per la stessa attività è ammessa una responsabilità condivisa, ossia è possibile la presenza di più "R".

A = Accountable. Coordina, supervisiona e approva i vari task che compongono l'attività; può eseguirne alcuni ed è responsabile anche degli aspetti economici. È unico per l'attività e deve essere individuato nel caso vi sia la presenza di più "R".

C = Consulted. È consultato poiché possiede informazioni e/o capacità necessarie per portare a termine l'attività.

I = Informed. È informato dei risultati dell'attività.

Parte delle informazioni prodotte dalle attività del flusso confluiscono nei Registri dei trattamenti del Titolare e del Responsabile.

5.2 DESCRIZIONE SISTEMATICA DEL SERVIZIO ICT

Partendo dal trattamento del Titolare, l'Owner del trattamento, con il supporto del Responsabile del Servizio ICT, descrive le caratteristiche del Servizio ICT come indicato in Tabella 5, seguendo lo schema di supporto alla compilazione riportato in Tabella 6.

DATI IDENTIFICATIVI DEL SERVIZIO ICT	
Codice	<i>Codice del Servizio ICT</i>
Nome	<i>Nome del Servizio ICT</i>
Descrizione	<i>Descrizione funzionale del Servizio ICT</i>
Titolare	<i>Titolare del trattamento supportato dal Servizio ICT</i>
Interscambio dati	<i>Indica se il Servizio ICT permette lo scambio di dati personali tra pubbliche amministrazioni secondo il provvedimento del Garante del 2 luglio 2015</i>
Cloud	<i>Indica se vengono utilizzati servizi cloud esterni</i>
Numero di utenti	<i>Numero degli utenti del Servizio ICT</i>
Tipologia di utenti	<i>Tipologia degli utenti del Servizio ICT (cittadini, dipendenti, ecc)</i>
INFORMAZIONI SUL TRATTAMENTO (da riportare solo se il Servizio ICT tratta dati personali)	
Finalità	<i>Scopo perseguito con il trattamento</i>
Fondamenti di licetità	<i>Base giuridica e contrattuale che legittima il trattamento dei dati</i>
Interessati	<i>Categorie di persone fisiche cui si riferiscono i dati</i>
Destinatari	<i>Categorie dei destinatari di comunicazioni</i>
Termini di cancellazione dei tracciamenti	<i>Tempi o criteri di cancellazione dei tracciamenti (log)</i>
Trasferimenti dati	<i>Trasferimento dati extra Ue e relative garanzie</i>

Processi privacy implementati	<i>Procedure implementate sul Servizio ICT per garantire i diritti dell'interessato in merito ai propri dati personali (consenso, informativa, rettifica, cancellazione, ...)</i>
--------------------------------------	---

Tabella 5 – Informazioni descrittive del Servizio ICT

VALORIZZAZIONE CATEGORIE	
Interscambio dati	<i>Interoperabilità (il Servizio ICT permette lo scambio di dati personali e viene invocato dalle amministrazioni appartenenti al SIF)</i>
	<i>Cooperazione applicativa (il Servizio ICT permette lo scambio di dati personali e viene invocato da amministrazioni esterne al SIF)</i>
	<i>Generico (il Servizio ICT non permette lo scambio di dati personali tra pubbliche amministrazioni)</i>
Cloud	SI/NO
Tipologia di utenti	<i>Dipendenti Sogei</i>
	<i>Collaboratori Sogei (tecnicici, consulenti, ...)</i>
	<i>Dipendenti dell'amministrazione titolare per servizi di front-office</i>
	<i>Dipendenti dell'amministrazione titolare per servizi di Direzione Centrale</i>
	<i>Dipendenti dell'amministrazione titolare per servizi di back-office</i>
	<i>Dipendenti altre PA</i>
	<i>Cittadini</i>
	<i>Associazioni di categoria</i>
	<i>Professionisti</i>
	<i>Operatori economici</i>
	<i>Intermediari</i>
	<i>Punti di commercializzazione</i>
	<i>Concessionari</i>
	<i>Fornitori</i>
Finalità	<i>Collaboratori dei clienti istituzionali</i>
	<i>Altro (specificare)</i>
	<i>Gestione amministrativo contabile</i>
	<i>Informazione/formazione, istruzione, cultura</i>
	<i>Ricerca e statistica</i>
	<i>Settore economico</i>
	<i>Settore sanitario</i>
	<i>Settore fiscale, tributario</i>

**METODOLOGIA
PER LA PROTEZIONE DEI DATI
E PER LA VALUTAZIONE D'IMPATTO**

IS-00-PR-07
PAG. 29 DI 70
07 LUGLIO 2020

VALORIZZAZIONE CATEGORIE	
	<i>Gestione della sicurezza fisica (es. sedi, locali,...)</i>
	<i>Applicazione contratti di lavoro</i>
Fondamenti di liceità	<i>Consenso dell'interessato</i> <i>Esecuzione di un contratto con l'interessato</i> <i>Obbligo legale per il titolare</i> <i>Salvaguardia interessi vitali dell'interessato o altra persona fisica</i> <i>Esecuzione di un compito di interesse pubblico o pubblici poteri del titolare derivante da normativa nazionale</i> <i>Esecuzione di un compito di interesse pubblico o pubblici poteri del titolare derivante da regolamento UE</i> <i>Altri fondamenti connessi al trattamento di categorie particolari di dati personali - art. 9 par. 2</i> <i>Richiesta pubblica autorità</i> <i>Statuto</i>
Interessati	<i>Cittadini</i> <i>Personale dipendente e familiari</i> <i>Contraenti, offerenti e candidati</i> <i>Rappresentanti e dipendenti di enti/istituzioni (associazioni di categoria/ordini professionali, ...)</i> <i>Componenti organi dell'Ente</i> <i>Persone fisiche extra UE</i> <i>Visitatori</i> <i>Minorenni</i> <i>Operatori economici</i> <i>Professionisti, intermediari</i> <i>Altri soggetti - Persone fisiche</i>
Destinatari	<i>Persona fisica</i> <i>Persona giuridica</i> <i>Pubblica amministrazione</i> <i>Autorità pubblica</i>
Trasferimenti dati	<i>Paese terzo o organizzazione internazionale</i> <i>Garanzie e autorizzazioni ex art. 46 del Regolamento</i>
Termine di cancellazione dei tracciamenti	<i>Breve (1 anno)</i> <i>Medio (2 anni)</i> <i>Lungo (30 anni)</i> <i>Indeterminato</i>
	<i>Informativa</i>

VALORIZZAZIONE CATEGORIE	
Processi privacy implementativi⁵	<i>Consenso</i>
	<i>Data breach</i>
	<i>Diritto di accesso ai dati</i>
	<i>Diritto di opposizione/cancellazione</i>
	<i>Diritto di rettifica</i>
	<i>Diritto alla limitazione dei dati</i>

Tabella 6 – Schema di supporto alla compilazione delle categorie

5.3 IDENTIFICAZIONE E CLASSIFICAZIONE DEI DATI

Partendo dal trattamento/processo del titolare, l'Owner del trattamento, con il supporto del Responsabile del Servizio ICT, identifica:

- i dati appartenenti al dominio in esame e ne fornisce una descrizione;
- i tempi di cancellazione dei dati, ossia il periodo massimo consentito per il trattamento. Ove possibile indica il periodo esatto oltre il quale i dati devono essere cancellati oppure descrive il criterio utilizzato per la cancellazione.

Se il Servizio ICT tratta dati personali, questi devono essere classificati secondo quanto riportato in Tabella 7.

⁵ Per una descrizione delle categorie di processi privacy implementabili a garanzia dei diritti dell'interessato riferirsi al par. 4.4 Garanzia dei diritti dell'interessato.

Macro categoria di dati personali	Categoria di dati personali
Dati personali comuni	anagrafici contabili e fiscali, inerenti possidenze e riscossione inerenti il rapporto di lavoro tracciamenti dati inerenti situazioni giudiziarie civili, amministrative, tributarie
Dati personali specifici	geolocalizzazione audio/video/foto dati di profilazione
Dati personali finanziari	dati relativi all'esistenza di rapporti finanziari (coordinate bancarie, consistenze saldi, movimenti, giacenza media, etc.)
Dati personali sensibili	convizioni religiose o filosofiche/opinioni politiche/origine razziale/adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale
Dati personali ipersensibili	stato di salute, assistenza sanitaria, orientamento/vita sessuale genetici
Dati personali giudiziari	casellario giudiziale qualità di indagato/imputato o altre situazioni giudiziarie (condanne penali e reati o connesse misure di sicurezza)
Dati personali biometrici	impronte digitali altre caratteristiche biometriche firma grafometrica

Tabella 7 – Classificazione privacy del dato

5.4 VALUTAZIONE DEI RISCHI PER L'ORGANIZZAZIONE

L'Owner del trattamento, con il supporto del Responsabile del Servizio ICT, valuta i rischi per l'organizzazione in termini di perdita degli attributi di riservatezza, integrità e disponibilità delle informazioni gestite.

In particolare il rischio per l'organizzazione viene valutato in termini di:

- *Impatto per l'organizzazione*, stimato sulla base del livello di gravità (trascurabile, basso, medio o alto) delle seguenti tipologie di dati:
 - perdita finanziaria;

- compromissione (rallentamento, blocco) delle attività di business;
- perdita di immagine;
- sanzioni amministrative e/o penali previste da normativa.

L'impatto è valutato come il valore massimo delle gravità dei danni indicate per ogni attributo R, I (Tabella 17 – Legenda per la valutazione del rischio di perdita di Riservatezza e Integrità) e D (Tabella 19 - Legenda per la valutazione del rischio di perdita di Disponibilità).

- *Probabilità per l'organizzazione*, (trascurabile, bassa, media o alta), stimata sulla base degli agenti interni, esterni e errori/eventi accidentali, (Tabella 22 – Legenda per la valutazione probabilità di accadimento).

Il valore del rischio intrinseco è espresso per ciascuna minaccia come combinazione dell'impatto e della probabilità di accadimento dell'evento negativo, secondo la stessa matrice utilizzata per la valorizzazione del rischio per l'interessato, (cfr. Tabella 8).

5.5 VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTÀ DELL'INTERESSATO

Per ogni Servizio ICT a supporto di un trattamento di dati personali, l'Owner del trattamento, con il supporto del Responsabile del Servizio ICT, effettua la valutazione dei rischi per l'interessato calcolando la probabilità di accadimento delle minacce applicabili e la gravità del danno, al fine di individuare le misure di sicurezza adeguate ad attenuare tale rischio.

La valutazione dei rischi sui diritti e sulle libertà dell'interessato consta delle seguenti attività:

- identificazione delle minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilità dei dati;
- individuazione degli scenari di rischio specifici relativi alle categorie di dati personali;
- valutazione dei potenziali rischi sui diritti e le libertà degli interessati. Il rischio è inteso come uno scenario descrittivo di un evento dannoso e delle relative conseguenze, stimate in termini di gravità e probabilità di accadimento.

Le minacce applicabili sono:

- accesso non autorizzato e/o trattamento illegittimo relativo a dati;
- divulgazione non autorizzata o accidentale di dati;
- modifica non autorizzata o accidentale di dati;

- perdita, distruzione accidentale o illegale di dati;
- indisponibilità temporanea o prolungata di dati.

Gli scenari di rischio specifici si ottengono applicando ogni minaccia alle differenti categorie di dati (Tabella 20 – Minacce e scenari di rischio).

Per ciascuno scenario specifico l'Owner del trattamento, con il supporto del Responsabile del Servizio ICT, valuta il livello di rischio intrinseco, espresso come combinazione dell'impatto e della sua probabilità di accadimento.

L'impatto rappresenta le conseguenze derivanti da un evento negativo. Più sono elevate le conseguenze più alto è percepito il rischio. La valutazione dell'impatto tiene conto delle seguenti tipologie di danni (Tabella 21):

- danno fisico-biologico;
- danno finanziario;
- danno reputazionale;
- danno di identità.

La valorizzazione dell'impatto segue una scala predefinita (trascutibile, basso, medio, alto), e deriva dal valore massimo di danno rispetto alle tipologie indicate.

La probabilità di accadimento segue una scala predefinita (trascutibile, basso, medio, alto) e indica quanto è probabile che si verifichi un evento negativo. Dipende dal contesto interno ed esterno del Servizio ICT e viene stimata utilizzando la Tabella 22 – Legenda per la valutazione probabilità di accadimento.

La valutazione del rischio intrinseco deve essere eseguita per ogni scenario specifico applicabile. La Tabella 23 - Stima del rischio intrinseco per i diritti e le libertà dell'interessato, rappresenta un esempio di valutazione precompilata.

Il valore del rischio intrinseco è espresso per ciascun scenario applicabile come combinazione dell'impatto e della probabilità di accadimento dell'evento negativo utilizzando la seguente Tabella 8.

Rischio intrinseco		Probabilità di accadimento			
		Trascutibile	Basso	Medio	Alto
Impatto	Trascutibile	Trascutibile	Trascutibile	Trascutibile	Trascutibile
	Basso	Basso	Basso	Basso	Basso
	Medio	Basso	Basso	Medio	Alto
	Alto	Basso	Medio	Alto	Alto

Tabella 8 - Matrice per la valorizzazione dei rischi per l'interessato

In caso di un nuovo Servizio ICT o di modifiche significative a un Servizio ICT esistente dovranno necessariamente essere rivalutati tutti gli scenari, apportando i dovuti aggiornamenti.

5.6 VALUTAZIONE DELLE CATEGORIE DI TRATTAMENTO A ELEVATO RISCHIO

La valutazione d'impatto (PIA) è obbligatoria qualora il trattamento presenti un rischio elevato per i diritti e le libertà dell'interessato.

Il Comitato europeo per la protezione dei dati, attraverso il documento WP 248 [4], al fine di fornire un insieme più concreto di trattamenti che richiedono una valutazione d'impatto sulla protezione dei dati in virtù del loro rischio intrinseco, suggerisce di prendere in esame le seguenti nove categorie (Tabella 24):

1. Valutazione o assegnazione di un punteggio (incluse le attività di profilazione e le analisi di tipo predittivo) riferita ad un individuo;
2. Decisioni automatizzate con significativi effetti giuridici o di analogo natura;
3. Monitoraggio sistematico di individui (es. mediante videosorveglianza);
4. Elaborazione di dati sensibili o aventi caratteristiche strettamente personali (es. giudiziari o altri tipi di dati strettamente personali il cui trattamento possa comportare alti rischi per l'interessato come la geolocalizzazione). Si assume che il Servizio ICT appartenga a questa categoria se dalla valutazione dei rischi per i diritti e le libertà degli interessati (par.5.5) emerge un rischio intrinseco alto relativamente agli scenari di rischio specifici applicabili
5. Elaborazione di dati su larga scala (es. per numero di individui coinvolti, volumi complessivi, durata o persistenza, ambito geografico);
6. Combinazione o raffronto tra banche dati provenienti da due o più operazioni di trattamento effettuati per scopi diversi;
7. Elaborazione di dati relativi a soggetti vulnerabili per cui è più accentuato lo squilibrio di poteri fra interessato e titolare del trattamento (es. minori, anziani, dipendenti);
8. Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;
9. Impedimento all'interessato di esercitare un diritto o di avvalersi di un Servizio ICT o di un contratto.

Se il Servizio ICT rientra in almeno due tra le suddette categorie o se a giudizio dell'Owner del trattamento anche una sola categoria nel contesto di riferimento costituisce un elevato rischio per l'interessato, è necessario procedere con lo svolgimento della valutazione di impatto (PIA) identificando le misure di sicurezza

adeguate (par.5.7) prima di passare alle fasi di valutazione complessiva dei rischi e individuazione delle relative misure (par. 5.9 e 5.10).

5.7 IDENTIFICAZIONE DI MISURE ADEGUATE PER VALUTAZIONE DI IMPATTO (PIA)

Nel caso in cui il Servizio ICT rientri in almeno due categorie di trattamento ad elevato rischio per l'interessato (par. 5.6) o, se a giudizio dell'Owner, comprenda anche una sola categoria è necessario procedere con l'identificazione di misure di sicurezza PIA adeguate al livello di rischio in relazione alle singole minacce.

Tali misure sono selezionate dal framework multicomppliance di Sogei, FOURSec (*Framework to Organize Under Rules Security*) [9] che associa specifiche misure di sicurezza da applicare in caso di valutazione d'impatto corrispondenti ad un elevato livello di rischio per l'interessato.

Il Responsabile del Servizio ICT indica in base ai vincoli architetturali l'insieme delle misure applicabili al contesto con la modalità di implementazione.

L'Owner del trattamento con il supporto del Responsabile del Servizio ICT valuta, tenendo conto della natura dei dati trattati, dei costi/tempi di attuazione come anche dei livelli di rischio, le misure da applicare nell'intervento in corso o successivamente in appositi piani di rientro, utilizzando la guida contenuta nella seguente Tabella 9.

Applicabilità misura	Modalità di implementazione
<u>Già applicata nell'intervento</u> (rif. Obiettivo)	<i>Descrivere le modalità di implementazione della misura di sicurezza</i>
<u>Da applicare nell'intervento</u> (rif. Obiettivo)	<i>Descrivere le modalità di implementazione della misura di sicurezza</i>
<u>Da applicare successivamente - urgente</u>	<i>Descrivere le azioni di miglioramento, ove possibile</i>
<u>Da applicare successivamente – non urgente</u>	<i>Descrivere le azioni di miglioramento, ove possibile</i>

<u>Non applicabile</u> (la misura non è tecnicamente applicabile o pertinente nel contesto di riferimento)	<i>Specificare le motivazioni per cui la misura non è tecnicamente applicabile o pertinente al contesto di riferimento</i>
--	--

Tabella 9 – Applicazione misure PIA

Nel caso in cui il Servizio ICT sia composto da Applicazioni non omogenee relativamente ai dati trattati è necessario indicare l'applicabilità delle misure di sicurezza specifiche per ognuna di tali Applicazioni.

5.8 CONSULTAZIONE DEL DPO

Tutte le misure di sicurezza ritenute tecnicamente applicabili per mitigare i rischi per l'interessato devono essere applicate.

Qualora l'Owner del trattamento ravvisi la sussistenza di rischi significativi per l'interessato, in caso di parziale adozione delle misure nell'intervento in corso, procede alla consultazione del proprio DPO.

5.9 VALUTAZIONE COMPLESSIVA DEI RISCHI DEL SERVIZIO ICT

L'Owner del trattamento, con il supporto del Responsabile del Servizio ICT, valuta i livelli complessivi di rischio intrinseco per le minacce applicabili al Servizio ICT. Tale calcolo è effettuato, come da seguente Tabella 10, sulla base di:

- rischi per i diritti e le libertà degli interessati (par.5.5);
- rischi per l'organizzazione derivanti dalla perdita di riservatezza, integrità e disponibilità delle informazioni (par.5.4).

Minaccia	Rischio intrinseco per interessato	Rischio intrinseco per organizzazione	Rischio intrinseco per Servizio ICT
Accesso non autorizzato e/o trattamento illecito relativo a dati	Valutazione dei rischi per l'interessato	Max (rischio Riservatezza, Integrità)	Max (Rischio interessato, organizz)
Divulgazione non autorizzata o accidentale di dati	Valutazione dei rischi per l'interessato	Rischio Riservatezza	Max (Rischio interessato, organizz)
Modifica non autorizzata o accidentale di dati	Valutazione dei rischi per l'interessato	Rischio Integrità	Max (Rischio interessato, organizz)

Perdita, distruzione accidentale o illegale di dati	Valutazione dei rischi per l'interessato	Rischio Disponibilità a lungo termine	Max (Rischio interessato,organizz)
Indisponibilità temporanea o prolungata di dati	Valutazione dei rischi per l'interessato	Max (Rischio Disponibilità a breve e medio termine)	Max (Rischio interessato,organizz)

Tabella 10 - Rischio intrinseco del Servizio ICT

Il rischio intrinseco complessivo del Servizio ICT è dato dal valore massimo tra il rischio intrinseco per l'interessato e il rischio intrinseco per l'organizzazione.

5.10 IDENTIFICAZIONE DI MISURE ADEGUATE PER LA SICUREZZA DEL SERVIZIO ICT

In base al livello di rischio intrinseco complessivo del Servizio ICT (par. 5.9), risultante dalla valutazione del rischio intrinseco per l'interessato e per l'organizzazione, viene estratto dal framework FOURSec [9] un elenco di misure di sicurezza in relazione ad ogni minaccia.

Il Responsabile del Servizio ICT indica in base ai vincoli architetturali l'insieme delle misure applicabili al contesto con la modalità di implementazione.

L'Owner del trattamento con il supporto del Responsabile del Servizio ICT valuta, tenendo conto della natura dei dati trattati, dei costi/tempi di attuazione come anche dei livelli di rischio, le misure da applicare nell'intervento in corso o successivamente in appositi piani di rientro, utilizzando la guida contenuta nella seguente Tabella 11.

Applicabilità misura	Modalità di implementazione
<u>Già applicata nell'intervento</u> (rif. Obiettivo)	<i>Descrivere le modalità di implementazione della misura di sicurezza</i>
<u>Da applicare nell'intervento</u> (rif. Obiettivo)	<i>Descrivere le modalità di implementazione della misura di sicurezza</i>
<u>Da applicare successivamente - urgente</u>	<i>Descrivere le azioni di miglioramento, ove possibile</i>
<u>Da applicare successivamente – non urgente</u>	<i>Descrivere le azioni di miglioramento, ove possibile</i>

<u>Non applicabile</u> (la misura non è tecnicamente applicabile o pertinente nel contesto di riferimento)	<i>Specificare le motivazioni per cui la misura non è tecnicamente applicabile o pertinente al contesto di riferimento</i>
--	--

Tabella 11 – Applicazione misure per la sicurezza del Servizio ICT

Nel caso in cui il Servizio ICT sia composto da Applicazioni non omogenee relativamente ai dati trattati, è necessario indicare l'applicabilità delle misure specifiche per ognuna di tali Applicazioni.

5.11 VALUTAZIONE DI ADEGUATEZZA DELLE MISURE DI SICUREZZA

Per ricondurre i rischi intrinseci per l'interessato e per l'organizzazione a valori trascurabili, tutte le misure di sicurezza applicabili in relazione al contesto ed ai vincoli architetturali devono essere adottate.

L'adeguatezza delle misure in relazione ai rischi è valutata in funzione delle misure da applicare nell'intervento in corso o successivamente con le relative priorità di attuazione, in particolare è espressa secondo la seguente terminologia:

- accettabile, se tutte le misure applicabili sono già applicate o sono da applicare nell'intervento in corso;
- accettabile con riserva, se per alcune misure applicabili sono previsti piani di rientro urgenti;
- da verificare, se per alcune misure applicabili sono previsti piani di rientro non urgenti.

In caso di parziale adozione delle misure di sicurezza nell'intervento in corso, il Responsabile del Servizio ICT rende evidenti all'Owner del trattamento le criticità che ne possono derivare. Tali evidenze costituiscono i razionali che supportano l'Owner del trattamento nella valutazione di adeguatezza delle misure di sicurezza per mitigare i rischi.

5.12 REDAZIONE DEL DOCUMENTO “MISURE DI SICUREZZA E PRIVACY DEL SERVIZIO ICT”

Il Responsabile del Servizio ICT compila il documento “Misure di sicurezza e privacy del Servizio ICT” [10] per documentare le valutazioni, concordate con

l'Owner del trattamento, relative ai rischi e all'adeguatezza delle misure di sicurezza.

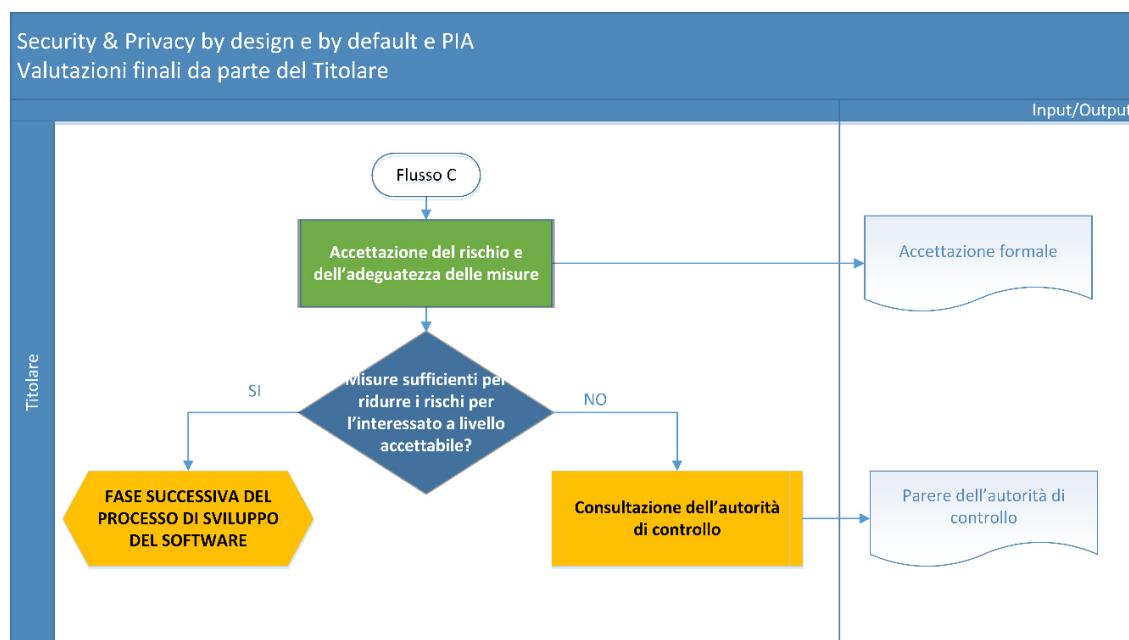
Il Responsabile del Servizio ICT invia il documento contestualmente al documento "Analisi dei Requisiti"/"Specifiche di intervento" se previsto o, in caso contrario, in un momento utile a garantire comunque uno sviluppo coerente del Servizio ICT.

È richiesta l'approvazione da parte dell'Owner del trattamento del documento "Misure di sicurezza e privacy del Servizio ICT" che avverrà contestualmente all'approvazione del documento "Analisi dei Requisiti"/"Specifiche di intervento", se previsto o, in caso contrario in modo specifico.

6. FLUSSO C - VALUTAZIONI FINALI DA PARTE DEL TITOLARE

6.1 FLUSSO E CARTA DELLE RESPONSABILITÀ

Di seguito è riportato il flusso⁶ relativo alle valutazioni finali da parte del Titolare.



La tabella riportata di seguito elenca le attività di analisi e valutazione di un trattamento e, per ognuna, le responsabilità secondo la matrice RACI.⁷.

⁶ Nel flusso sono rappresentate, in colore diverso, le attività che riguardano la privacy by design (colore verde) e quelle che riguardano la valutazione di impatto (colore blu).

⁷ La matrice è organizzata secondo il modello RACI che prevede quattro ruoli:

R = Responsible. Esegue l'attività e ne è responsabile. Per la stessa attività è ammessa una responsabilità condivisa, ossia è possibile la presenza di più "R".

A = Accountable. Coordina, supervisiona e approva i vari task che compongono l'attività; può eseguirne alcuni ed è responsabile anche degli aspetti economici. È unico per l'attività e deve essere individuato nel caso vi sia la presenza di più "R".

C = Consulted. È consultato poiché possiede le capacità necessarie per portare a termine l'attività.

I = Informed. È informato dei risultati dell'attività.

Nome attività	Ruoli / Responsabilità		
	Responsabile Servizio ICT	Owner trattamento	DPO Titolare
Accettazione del rischio e dell'adeguatezza delle misure	I	R	I
Consultazione dell'Autorità di controllo	I	R	C

Tabella 12 - Flusso C: Matrice RACI

6.2 ACCETTAZIONE DEL RISCHIO E DELL'ADEGUAZIONE DELLE MISURE

L'Owner del trattamento sulla base delle informazioni raccolte può:

- approvare il documento "Misure di sicurezza e privacy del Servizio ICT", confermando l'adeguatezza delle misure di sicurezza per mitigare i rischi e autorizzare il Responsabile del Servizio ICT a procedere alla progettazione e allo sviluppo dell'applicazione;
- non approvare il documento "Misure di sicurezza e privacy del Servizio ICT", richiedendo l'applicazione di ulteriori misure di sicurezza nell'intervento in corso e autorizzare il Responsabile del Servizio ICT a procedere previa implementazione di tali misure; in tal caso il Responsabile del Servizio ICT aggiorna il documento "Misure di sicurezza e privacy", segnalando eventuali problematiche realizzative di natura tecnica, nonché eventuali costi connessi all'implementazione delle misure richieste, procedendo successivamente alla progettazione e sviluppo;
- non approvare il documento "Misure di sicurezza e privacy del Servizio ICT" e richiedere l'applicazione di minori misure di sicurezza nell'intervento in corso spostando le restanti misure applicabili in piani di rientro successivi; in tal caso il Responsabile del Servizio ICT segnala formalmente all'Owner del trattamento tutte le criticità conseguenti.

In particolare:

- nei casi in cui l'analisi contenuta nel documento "Misure di sicurezza e privacy del Servizio ICT" si conclude con una valutazione dell'adeguatezza delle misure "accettabile" in quanto è prevista l'implementazione di tutte le misure di sicurezza applicabili, l'Owner del trattamento, se valuta che siano stati

correttamente riportati e mitigati i rischi per l'organizzazione e per l'interessato, può procedere all'approvazione del documento;

- invece, nei casi in cui l'analisi contenuta nel documento "Misure di sicurezza e privacy del Servizio ICT" si concluda con una valutazione dell'adeguatezza delle misure da applicare nell'intervento in corso "accettabile con riserva" o "da verificare" e l'Owner del trattamento ravvisi la sussistenza di rischi significativi per il servizio ICT da avviare a fronte della pianificazione a breve o lungo termine delle restanti misure applicabili, l'Owner può valutare se procedere ad un riesame interno, coinvolgendo superiori livelli di responsabilità nell'organizzazione del Titolare, fino ad un eventuale coinvolgimento del proprio DPO. A seguito dell'esito di tali ulteriori valutazioni e consultazioni l'Owner del trattamento può:
 - approvare il documento "Misure di sicurezza e privacy del Servizio ICT", confermando l'adeguatezza delle misure da applicare nell'intervento in corso e le misure da applicare successivamente in appositi piani di rientro con relativo livello di urgenza;
 - non approvare il documento e ridefinire, in considerazione di tempi e costi, alcuni elementi del servizio, misure di sicurezza o requisiti applicativi, al fine di individuarne ed eliminarne i punti critici. A seguito di tale revisione si dovrà procedere alla rivalutazione dell'adeguatezza delle misure di sicurezza, aggiornando la documentazione di supporto e il documento "Misure di sicurezza e privacy ICT". Qualora, a seguito della valutazione d'impatto, l'Owner del trattamento sia del parere che rimangano elevati rischi per l'interessato, consulta preventivamente l'Autorità di controllo tramite il DPO (par. 6.3) e, se del caso, raccoglie le opinioni degli interessati o dei loro rappresentanti (art. 35, comma 9 del Regolamento).

L'Owner del trattamento può procedere analogamente anche per l'approvazione conclusiva del documento "Misure di sicurezza e privacy del trattamento" inherente a un trattamento cartaceo o supportato da strumenti di office automation, valutando la necessità di ricorrere a un riesame interno e/o a un riesame del trattamento, come sopra descritto (Allegato 3 - FLUSSO B.2 - VALUTAZIONE DI RISCHI E MISURE PER IL TRATTAMENTO DA PARTE DEL TITOLARE).

6.3 CONSULTAZIONE DELL'AUTORITÀ DI CONTROLLO

Se dalla valutazione d'impatto sulla protezione dei dati risulta che il trattamento presenta un rischio elevato per i diritti e le libertà delle persone fisiche e l'Owner del trattamento è del parere che il rischio non possa essere ragionevolmente attenuato, si consulta l'Autorità di controllo prima dell'inizio delle attività di trattamento (art. 36 del Regolamento).

**METODOLOGIA
PER LA PROTEZIONE DEI DATI
E PER LA VALUTAZIONE D'IMPATTO**

IS-00-PR-07
PAG. 43 DI 70
07 LUGLIO 2020

L'Autorità di controllo fornisce un parere scritto e può avvalersi dei poteri stabiliti dal Regolamento, al fine di garantire il rispetto della normativa (es. può fornire consulenza notificando eventuali violazioni, rivolgere avvertimenti e ammonizioni, ingiungere di conformare i trattamenti alle disposizioni del Regolamento, imporre limitazioni o divieti al trattamento, ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali).

*METODOLOGIA
PER LA PROTEZIONE DEI DATI
E PER LA VALUTAZIONE D'IMPATTO*

IS-00-PR-07
ALLEGATO
PAG. 44 DI 70
07 LUGLIO 2020

ALLEGATI

1. CONFORMITÀ DELLA METODOLOGIA A NORME E STANDARD

La metodologia di PIA descritta nel presente documento è stata sviluppata sulla base delle prescrizioni contenute nel Regolamento [2], delle linee guida del documento WP 248 [4] e tenendo conto dell'approccio descritto nello standard ISO/IEC 29134 [4]. Nei paragrafi seguenti si elencano i criteri di accettabilità per la PIA estratti dalle linee guida e dallo standard ISO e se ne raffrontano i contenuti rispetto alla presente metodologia.

1.1 CONFORMITÀ ALLE LINEE GUIDA WP 248 REV.01

Il Gruppo di lavoro Articolo 29 propone, all'interno del documento di linee guida WP248 ([4], Allegato 2), una serie di criteri che possono essere utilizzati per stabilire se una metodologia specifica per l'esecuzione di una valutazione di impatto comprenda gli elementi sufficienti a garantire il rispetto delle disposizioni del Regolamento.

La Tabella 13 elenca i criteri presenti nell'Allegato 2 del WP248 e, per ognuno, ne riporta la descrizione e il paragrafo del presente documento in cui sono referenziati, tenendo in considerazione che le attività di PIA sono completamente integrate all'interno del processo di produzione del software.

Criterio WP 248	Descrizione criterio WP 248	Paragrafo di riferimento
<i>Descrizione sistematica del trattamento (art. 35, par. 7, lettera a)</i>	<ul style="list-style-type: none"> • <i>si tiene conto della natura, dell'ambito, del contesto e delle finalità del trattamento (considerando 90);</i> • <i>sono indicati i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi;</i> • <i>si dà una descrizione funzionale del trattamento;</i> • <i>si specificano gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);</i> • <i>si tiene conto dell'osservanza di codici di condotta approvati (art. 35, par. 8)</i> 	Par. 4.2 Descrizione sistematica del trattamento

**METODOLOGIA
PER LA PROTEZIONE DEI DATI
E PER LA VALUTAZIONE D'IMPATTO**

IS-00-PR-07
ALLEGATO
PAG. 46 DI 70
07 LUGLIO 2020

Criterio WP 248	Descrizione criterio WP 248	Paragrafo di riferimento
valutazione di necessità e proporzionalità del trattamento (art. 35, par. 7, lettera b)	<ul style="list-style-type: none"> • <i>si definiscono le misure previste per rispettare il regolamento (art. 35, par. 7, lettera d) e considerando 90) tenendo conto di quanto segue:</i> <ul style="list-style-type: none"> ▪ <i>misure che contribuiscono alla proporzionalità e alla necessità del trattamento sulla base di:</i> <ul style="list-style-type: none"> – <i>finalità specifiche, esplicite e legittime (art. 5(1), lettera b);</i> – <i>liceità del trattamento (art. 6);</i> – <i>dati adeguati, pertinenti e limitati a quanto necessario (art. 5(1)c));</i> – <i>periodo limitato di conservazione (art. 5(1), lettera e));</i> ▪ <i>misure che contribuiscono ai diritti degli interessati:</i> <ul style="list-style-type: none"> – <i>informazioni fornite agli interessati (artt. 12, 13, 14);</i> – <i>diritto di accesso e portabilità dei dati (artt. 15 e 20);</i> – <i>diritto di rettifica e cancellazione (artt. 16, 17, 19);</i> – <i>diritto di opposizione e limitazione del trattamento (artt. 18, 19, 21);</i> – <i>rapporti con responsabili del trattamento (art. 28);</i> – <i>garanzie per i trasferimenti internazionali di dati (Capo V);</i> 	Par. 4.3 Valutazione di necessità e proporzionalità Cap. 3 Flusso B.2 - Valutazione di rischi e misure per il trattamento da parte del titolare
	<ul style="list-style-type: none"> – <i>consultazione preventiva (art. 36)</i> 	Par. 4.3 Valutazione di necessità e proporzionalità Cap. 3 Flusso B.2 - Valutazione di rischi e misure per il trattamento da parte del titolare
		Par. 6.3 Consultazione dell'Autorità di controllo

**METODOLOGIA
PER LA PROTEZIONE DEI DATI
E PER LA VALUTAZIONE D'IMPATTO**

IS-00-PR-07
ALLEGATO
PAG. 47 DI 70
07 LUGLIO 2020

Criterio WP 248	Descrizione criterio WP 248	Paragrafo di riferimento
gestione dei rischi per i diritti e le libertà degli interessati (art. 35, par. 7, lettera c)	<ul style="list-style-type: none"> • <i>Si determinano l'origine, la natura, la particolarità e la gravità dei rischi (cfr. considerando 84) o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati:</i> <ul style="list-style-type: none"> ▪ <i>si tiene conto delle fonti di rischio (considerando 90);</i> ▪ <i>si identificano gli impatti potenziali sui diritti e le libertà degli interessati in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilità dei dati;</i> ▪ <i>si identificano le minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilità dei dati;</i> ▪ <i>si stimano probabilità e gravità (considerando 90);</i> • <i>si stabiliscono le misure previste per gestire i rischi di cui sopra (art. 35, par. 7, lettera d) e considerando 90);</i> 	Par 5.5 Valutazione dei rischi per i diritti e le libertà dell'interessato Par 5.6 Valutazione delle categorie di trattamento ad elevato rischio
coinvolgimento dei soggetti interessati	<ul style="list-style-type: none"> • <i>si chiede consulenza al RPD/DPO (art. 35, par. 2);</i> • <i>si sentono gli interessati o i loro rappresentanti (art. 35, par. 9), se del caso.</i> 	Par 5.7 Identificazione di misure adeguate per valutazione di impatto (PIA) Par 5.10 Identificazione di misure adeguate per la sicurezza del Servizio ICT Par 5.11 Valutazione di adeguatezza delle misure di sicurezza
		Par 5.8 Consultazione del DPO (ruolo e responsabilità del DPO)
		Par. 6.2 Accettazione del rischio e dell'adeguatezza delle misure

Tabella 13 - Criteri di accettabilità per la PIA secondo WP 248

Rispetto ai criteri riportati nel WP 248, si precisa e si osserva quanto segue:

- l'art. 35, par. 8 del Regolamento relativo all'uso di codici di condotta non è referenziabile allo stato dell'arte, in quanto non risultano approvati, al momento, schemi o codici applicabili allo specifico contesto in cui opera Sogei (i.e. rapporti con la PA);
- se un trattamento è necessario per adempiere ad un obbligo di legge o per l'esecuzione di un compito di interesse pubblico ed è già stata condotta una valutazione di impatto per lo specifico trattamento, non è necessario per il titolare rieseguire nuovamente la PIA (art. 35, par. 10 del Regolamento);
- al momento non sono noti schemi di PIA applicabili al settore in cui opera Sogei; in ogni caso il Regolamento non indica una procedura specifica da seguire ai fini della PIA, lasciando ai titolari la definizione dello schema;
- la descrizione delle misure che “*contribuiscono alla proporzionalità e alla necessità del trattamento*” (artt. 5 e 35, par. 7, lett. b), del Regolamento) è principalmente di tipo concettuale;
- l'opportunità per il titolare di “*raccogliere le opinioni degli interessati o dei loro rappresentanti se del caso*” (art. 35, par. 9 del Regolamento) è contemplata come ipotesi, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti; il titolare dovrebbe comunque documentare le motivazioni della mancata consultazione, qualora decidesse di non attuarla.

1.2 CONFORMITÀ ALLO STANDARD ISO/IEC 29134:2017

Lo standard ISO/IEC 29134, basato sulla ISO/IEC 31000 (che rappresenta lo standard di riferimento per la gestione del rischio), definisce il processo per la valutazione d'impatto e il riesame periodico, fornendo un esempio per la stima degli impatti e uno specifico modello da utilizzare per il rapporto di valutazione.

L'approccio proposto dallo standard declina la valutazione d'impatto in diverse fasi operative, che vanno dalla preparazione della PIA al follow-up, ciascuna delle quali articolata in attività specifiche. La Tabella 14 elenca le fasi e, per ognuna, ne riporta le attività e il paragrafo del presente documento in cui sono referenziate, tenendo in considerazione che le attività di PIA sono completamente integrate all'interno del processo di produzione del software.

ISO/IEC 29134:2017 Fase	ISO/IEC 29134:2017 Attività	Paragrafo di riferimento
<i>Fase 1 Preparazione della PIA</i>	Necessità Team Pianificazione Stakeholder	Par 4.1 Flusso e Carta delle responsabilità Par 5.3 Identificazione e classificazione dei dati

**METODOLOGIA
PER LA PROTEZIONE DEI DATI
E PER LA VALUTAZIONE D'IMPATTO**

IS-00-PR-07
ALLEGATO
PAG. 49 DI 70
07 LUGLIO 2020

ISO/IEC 29134:2017 Fase	ISO/IEC 29134:2017 Attività	Paragrafo di riferimento
Fase 2 Esecuzione della PIA	Flussi informativi	Par 5.1 Flusso e Carta delle responsabilità
	Casi d'uso	Par 5.5 Valutazione dei rischi per i diritti e le libertà dell'interessato Par 5.6 Valutazione delle categorie di trattamento ad elevato rischio
	Contromisure esistenti	5.7 Identificazione di misure adeguate per valutazione di impatto (PIA)
	Valutazione del rischio	Par 5.5 Valutazione dei rischi per i diritti e le libertà dell'interessato Par 5.6 Valutazione delle categorie di trattamento ad elevato rischio
	Trattamento del rischio	5.11 Valutazione di adeguatezza delle misure di sicurezza (valutazione di adeguatezza delle misure di sicurezza specifiche di PIA)
Fase 3 Follow up	Report	IS-18-PR-01 - Misure di sicurezza e privacy del Servizio ICT.
	Implementazione del piano	Fase di progettazione e realizzazione del Servizio ICT
	Audit	Fase di progettazione e realizzazione del Servizio ICT
	Gestione dei cambiamenti alla PIA	IS-18-PR-01 - Misure di sicurezza e privacy del Servizio ICT.

Tabella 14 – Analisi dei requisiti dello standard ISO/IEC 29134

2. FOURSEC

FOURSec (*Framework to Organize Under Rules Security*) [9] è un framework di misure di sicurezza volto alla protezione delle informazioni e dell'infrastruttura tecnologica di Sogei. Ogni misura è il risultato di una integrazione e omogeneizzazione di requisiti di sicurezza derivanti da normative nazionali ed europee (GDPR, provvedimenti del Garante), standard (ISO/IEC 27001:2013), framework di riferimento per la cybersecurity (Framework nazionale per la cybersecurity, NIST Cybersecurity Framework), istruzioni contrattuali delle Amministrazioni e politiche aziendali di sicurezza e privacy.

Ai fini della metodologia per la protezione dei dati e per la valutazione d'impatto viene utilizzato un estratto delle circa 260 misure di sicurezza in esso contenute, applicabile ai trattamenti di dati personali effettuati con l'ausilio di Servizi ICT o con il supporto di strumenti di office automation o di documenti cartacei. La selezione delle misure adeguate per ogni trattamento/ Servizio ICT viene effettuata sulla base della minaccia e del livello di rischio ad esse associato.

Oltre alle misure selezionate sulla base del profilo di rischio del trattamento/ Servizio ICT, Sogei protegge tutte le informazioni che tratta in qualità di Titolare o di Responsabile con un set di misure infrastrutturali elencate in specifici allegati ai registri dei trattamenti.

*METODOLOGIA
PER LA PROTEZIONE DEI DATI
E PER LA VALUTAZIONE D'IMPATTO*

IS-00-PR-07
ALLEGATO
PAG. 51 DI 70
07 LUGLIO 2020

3. FLUSSO B.2 - VALUTAZIONE DI RISCHI E MISURE PER IL TRATTAMENTO DA PARTE DEL TITOLARE

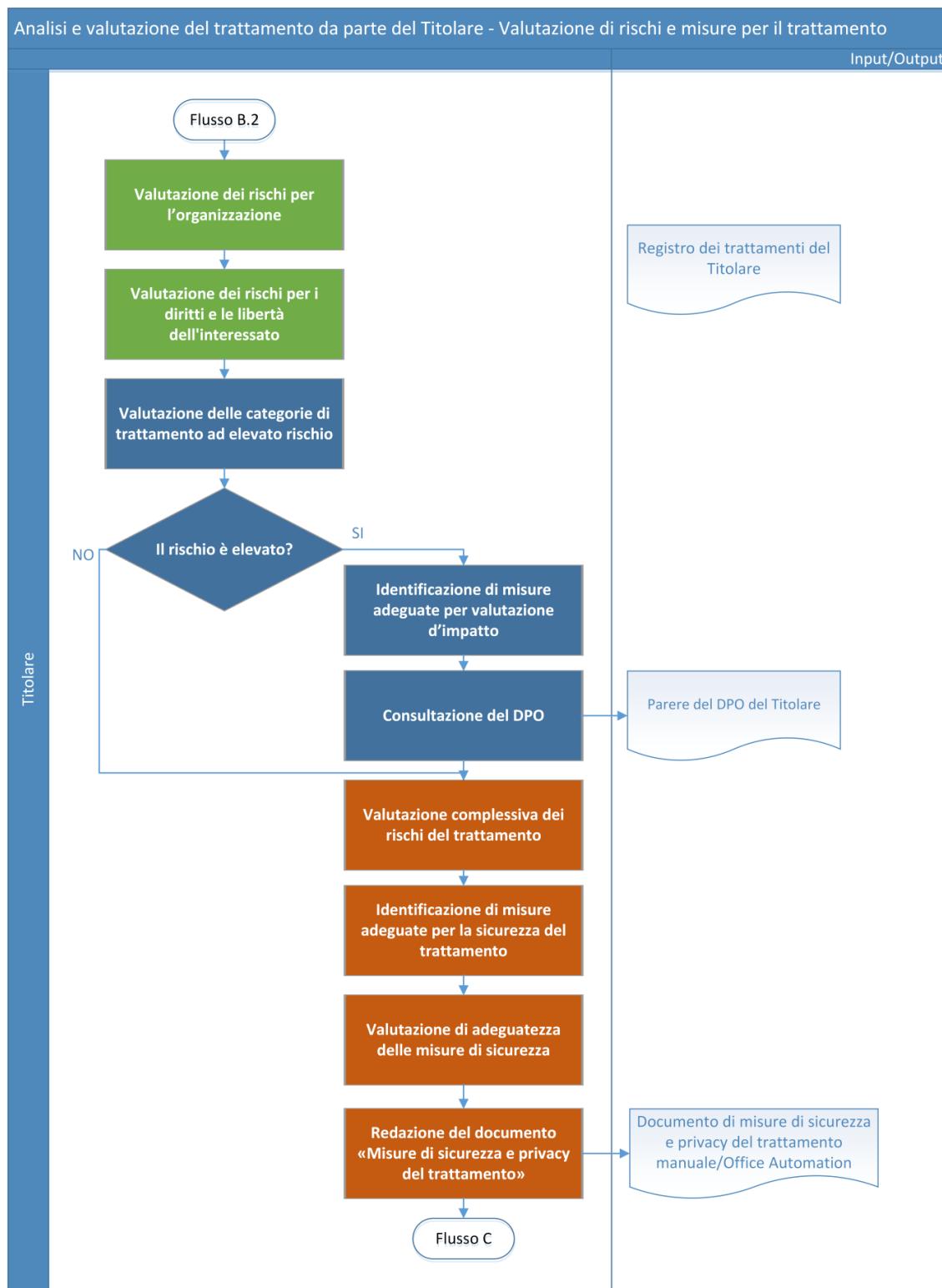
3.1 FLUSSO E CARTA DELLE RESPONSABILITÀ

Di seguito è riportato il flusso di valutazione⁸, relativamente alle attività di trattamento cartaceo o supportato da strumenti informatici di office automation, dei rischi per i diritti e le libertà dell’interessato, compresa la valutazione d’impatto (PIA), e dei rischi relativi alla sicurezza delle informazioni.

⁸ Nel flusso sono rappresentate, in colore diverso, le attività relative ai trattamenti (colore arancio), quelle che riguardano la privacy by design e la sicurezza delle informazioni (colore verde) e quelle che riguardano la valutazione di impatto (colore blu).

**METODOLOGIA
PER LA PROTEZIONE DEI DATI
E PER LA VALUTAZIONE D'IMPATTO**

IS-00-PR-07
ALLEGATO
PAG. 52 DI 70
07 LUGLIO 2020



**METODOLOGIA
PER LA PROTEZIONE DEI DATI
E PER LA VALUTAZIONE D'IMPATTO**

IS-00-PR-07
ALLEGATO
PAG. 53 DI 70
07 LUGLIO 2020

La tabella riportata di seguito elenca le attività del flusso riportando per ognuna le responsabilità secondo la matrice RACI.⁹

Nome Attività	Ruoli / Responsabilità	
	Owner Trattamento	DPO Titolare
Valutazione dei rischi per l'organizzazione	R	-
Valutazione dei rischi per i diritti e le libertà degli interessati	R	I
Valutazione delle categorie di trattamento ad elevato rischio	R	I
Identificazione di misure adeguate per privacy impact assessment	R	I
Consultazione del DPO	R	C
Valutazione complessiva dei rischi del Servizio ICT	R	I
Identificazione di misure adeguate per la sicurezza del Servizio ICT	R	I
Valutazione di adeguatezza delle misure di sicurezza	R	I
Redazione del documento "Misure di sicurezza e privacy del trattamento ..."	R	I

Tabella 15 – Flusso B2: Matrice RACI

⁹ La matrice è organizzata secondo il modello RACI che prevede quattro ruoli:

R = Responsible. Esegue l'attività e ne è responsabile. Per la stessa attività è ammessa una responsabilità condivisa, ossia è possibile la presenza di più "R".

A = Accountable. Coordina, supervisiona e approva i vari task che compongono l'attività; può eseguirne alcuni ed è responsabile anche degli aspetti economici. È unico per l'attività e deve essere individuato nel caso vi sia la presenza di più "R".

C = Consulted. È consultato poiché possiede informazioni e/o capacità necessarie per portare a termine l'attività.

I = Informed. È informato dei risultati dell'attività.

*METODOLOGIA
PER LA PROTEZIONE DEI DATI
E PER LA VALUTAZIONE D'IMPATTO*

IS-00-PR-07
ALLEGATO
PAG. 54 DI 70
07 LUGLIO 2020

3.2 DESCRIZIONE SINTETICA DELLE ATTIVITÀ

L'approccio per la valutazione dei rischi e per l'individuazione di misure adeguate al trattamento, nel caso in cui il trattamento sia eseguito su supporti cartacei o tramite strumenti di office automation, è del tutto analogo a quanto descritto relativamente ai trattamenti supportati da Servizi ICT (cap. 5, FLUSSO B - ANALISI E VALUTAZIONE DEL SERVIZIO ICT DA PARTE DEL TITOLARE E DEL RESPONSABILE).

Le principali differenze si sostanziano in:

- conduzione delle attività descritte a cura dell'Owner del trattamento, con l'eventuale supporto dei responsabili/esperti della sicurezza fisica o dei servizi di office automation dell'organizzazione;
- identificazione e valutazione di misure di sicurezza specifiche per l'ambito dei trattamenti cartacei o effettuati con strumenti di office automation;
- redazione ed approvazione, da parte dell'Owner del trattamento, del documento di "Misure di sicurezza e privacy del trattamento".

4. VALUTAZIONE DI RISERVATEZZA E INTEGRITÀ PER SERVIZI ICT

Area d'analisi	Impatto	Perdita Finanziaria	Compromissione (rallentamento, blocco, ...) delle attività di business	Perdita di immagine	Sanzioni amministrative e/o penali previste da normative ¹⁰
Riservatezza	Che impatto ha l'accesso non autorizzato ¹¹ ai dati da parte di personale interno o esterno?	Nullo, Basso Medio, Alto	Nullo, Basso Medio, Alto	Nullo, Basso Medio, Alto	Nullo, Basso Medio, Alto
Integrità	Che impatto ha un'alterazione non autorizzata ¹² dei dati?	Nullo, Basso Medio, Alto	Nullo, Basso Medio, Alto	Nullo, Basso Medio, Alto	Nullo, Basso Medio, Alto

Tabella 16 – Valutazione del rischio per perdita di Riservatezza e Integrità

Valutazione Impatto ¹³	Perdita Finanziaria ¹⁴	Compromissione (rallentamento, blocco, ...) delle attività di business ¹⁵	Perdita di immagine	Sanzioni amministrative e/o penali previste da normative ¹⁶
Trascurabile	Perdita finanziaria nulla (n.a.)	Nessun impatto sui processi e/o sugli utenti	Nessuna perdita d'immagine	Non esiste normativa specifica applicabile al trattamento dei dati

¹⁰ Violazione degli obblighi di legge relativi alla normativa privacy o ad altre normative specifiche applicabili al trattamento del dato

¹¹ Per dolo, colpa, errore, malfunzionamento.

¹² Per dolo, colpa, errore, malfunzionamento.

¹³ La valutazione dell'impatto va effettuata sul singolo evento più grave che presumibilmente può accadere.

¹⁴ La perdita finanziaria è stimata sui processi di business del cliente nel caso si tratti di servizi informatici erogati per conto dell'Amministrazione (in particolare nel caso in cui il Servizio ICT tratti direttamente transazioni finanziarie, come servizi di pagamento allo sportello o giocate su eventi sportivi) o sui processi di business aziendali nel caso si tratti di servizi informatici interni.

¹⁵ La compromissione (rallentamento e/o blocco delle attività di business) sono stimate sui processi di business del cliente nel caso si tratti di servizi informatici erogati per conto dell'Amministrazione o sui processi di business aziendali nel caso si tratti di servizi informatici interni.

¹⁶ Violazione degli obblighi di legge relativi al codice privacy o ad altre normative specifiche applicabili al trattamento del dato

**METODOLOGIA
PER LA PROTEZIONE DEI DATI
E PER LA VALUTAZIONE D'IMPATTO**

IS-00-PR-07
ALLEGATO
PAG. 56 DI 70
07 LUGLIO 2020

Valutazione Impatto ¹³	Perdita Finanziaria ¹⁴	Compromissione (rallentamento, blocco, ...) delle attività di business ¹⁵	Perdita di immagine	Sanzioni amministrative e/o penali previste da normative ¹⁶
Basso	Perdita finanziaria trascurabile	Impatto operativo di bassa entità in quanto i dati interessano, ad esempio, un solo processo e/o un numero molto limitato di utenti	Perdita d'immagine di bassa rilevanza in quanto i dati interessano un limitato bacino di utenza e/o la compromissione degli stessi può interessare la stampa locale	Esiste normativa specifica applicabile al trattamento dei dati gestiti che non prevede sanzioni amministrative e/o penali
Medio	Impatto finanziario di media rilevanza in quanto i dati sono riconducibili a Servizi ICT che trattano indirettamente "movimentazioni economiche" (es. consultivazioni, budget, ...)	Impatto operativo di media entità in quanto i dati interessano, ad esempio, un numero medio di processi e/o di utenti	Perdita di immagine di media rilevanza in quanto i dati sono d'interesse per alcune categorie di utenti esterni e/o la compromissione degli stessi può generare: -news negative su media a diffusione nazionale -richiesta di informativa dell'azionista e degli organi di controllo	Esistono sanzioni previste dalla normativa privacy, in quanto sono trattati dati personali (ma non sensibili o giudiziari) Esistono sanzioni amministrative previste da altra normativa specifica applicabili al trattamento dei dati in oggetto (es. D. Lgs. 231/01 per processi aziendali)
Alto	Impatto finanziario di elevata rilevanza in quanto i dati sono riconducibili a Servizi ICT che gestiscono direttamente "movimentazioni economiche" (es. pagamenti, giocate, ...)	Impatto operativo di alta entità in quanto i dati interessano, ad esempio, un numero consistente di processi e/o di utenti	Perdita di immagine di elevata rilevanza in quanto i dati sono d'interesse per gran parte degli utenti esterni e/o la compromissione degli stessi può generare: -interventi negativi sulla stampa nazionale -interventi dell'azionista e degli organi di controllo -interventi politici	Esistono sanzioni previste dalla normativa privacy, in quanto sono trattati dati personali sensibili e/o giudiziari Esistono sanzioni penali previste da altra normativa specifica applicabili al trattamento dei dati in oggetto

Tabella 17 – Legenda per la valutazione del rischio di perdita di Riservatezza e Integrità

5. VALUTAZIONE DI DISPONIBILITÀ PER SERVIZI ICT

Area d'analisi	Impatto	Perdita Finanziaria	Compromissione (rallentamento, blocco, ...) delle attività di business	Perdita di immagine	Sanzioni amministrative e/o penali previste da normative ¹⁷
Disponibilità¹⁸	Che impatto ha l'indisponibilità a breve (inferiore a 1 ora) del Servizio ICT?	Nullo, Basso Medio, Alto	Nullo, Basso Medio, Alto	Nullo, Basso Medio, Alto	Nullo, Basso Medio, Alto
	Che impatto ha l'indisponibilità media (tra 1 e 4 ore) del Servizio ICT?	Nullo, Basso Medio, Alto	Nullo, Basso Medio, Alto	Nullo, Basso Medio, Alto	Nullo, Basso Medio, Alto
	Che impatto ha l'indisponibilità prolungata (superiore a 4 ore) del Servizio ICT?	Nullo, Basso Medio, Alto	Nullo, Basso Medio, Alto	Nullo, Basso Medio, Alto	Nullo, Basso Medio, Alto

Tabella 18 – Valutazione del rischio per perdita di Disponibilità

¹⁷ Violazione degli obblighi di legge relativi alla normativa privacy o ad altre normative specifiche applicabili al trattamento del dato

¹⁸ Si applicano i criteri previsti per la Business Impact Analysis

**METODOLOGIA
PER LA PROTEZIONE DEI DATI
E PER LA VALUTAZIONE D'IMPATTO**

IS-00-PR-07
ALLEGATO
PAG. 58 DI 70
07 LUGLIO 2020

Valutazione Impatto ¹⁹	Perdita Finanziaria ²⁰	Compromissione (rallentamento, blocco, ...) delle attività di business ²¹	Perdita di immagine	Sanzioni amministrative e/o penali previste da normative ²²
Trascurabile	Perdita finanziaria nulla (n.a.)	Nessun impatto sui processi e/o sugli utenti	Nessuna perdita d'immagine	Non esiste normativa specifica applicabile al trattamento dei dati
Basso	Perdita finanziaria trascurabile	Impatto operativo di bassa entità in quanto i dati interessano, ad esempio, un solo processo e/o un numero molto limitato di utenti	Perdita d'immagine di bassa rilevanza in quanto i dati interessano un limitato bacino di utenza e/o la compromissione degli stessi può interessare la stampa locale	Esiste normativa specifica applicabile al trattamento dei dati gestiti che non prevede sanzioni amministrative e/o penali
Medio	Impatto finanziario di media rilevanza in quanto i dati sono riconducibili a Servizi ICT che trattano indirettamente "movimentazioni economiche" (es. consuntivazioni, budget, ...)	Impatto operativo di media entità in quanto i dati interessano, ad esempio, un numero medio di processi e/o di utenti	Perdita di immagine di media rilevanza in quanto i dati sono d'interesse per alcune categorie di utenti esterni e/o la compromissione degli stessi può generare: - news negative su media a diffusione nazionale - richiesta di informativa dell'azionista e degli organi di controllo	Esistono sanzioni previste dalla normativa privacy, in quanto sono trattati dati personali (ma non sensibili o giudiziari) Esistono sanzioni amministrative previste da altra normativa specifica applicabili al trattamento dei dati in oggetto (es. D. Lgs. 231/01 per processi aziendali)

¹⁹ La valutazione dell'impatto va effettuata sul singolo evento più grave che presumibilmente può accadere.

²⁰ La perdita finanziaria è stimata sui processi di business del cliente nel caso si tratti di servizi informatici erogati per conto dell'Amministrazione (in particolare nel caso in cui il Servizio ICT tratti direttamente transazioni finanziarie, come servizi di pagamento allo sportello o giocate su eventi sportivi) o sui processi di business aziendali nel caso si tratti di servizi informatici interni.

²¹ La compromissione (rallentamento e/o blocco delle attività di business) sono stimate sui processi di business del cliente nel caso si tratti di servizi informatici erogati per conto dell'Amministrazione o sui processi di business aziendali nel caso si tratti di servizi informatici interni.

²² Violazione degli obblighi di legge relativi alla normativa privacy o ad altre normative specifiche applicabili al trattamento del dato

**METODOLOGIA
PER LA PROTEZIONE DEI DATI
E PER LA VALUTAZIONE D'IMPATTO**

IS-00-PR-07
ALLEGATO
PAG. 59 DI 70
07 LUGLIO 2020

Valutazione Impatto ¹⁹	Perdita Finanziaria ²⁰	Compromissione (rallentamento, blocco, ...) delle attività di business ²¹	Perdita di immagine	Sanzioni amministrative e/o penali previste da normative ²²
Alto	Impatto finanziario di elevata rilevanza in quanto i dati sono riconducibili a Servizi ICT che gestiscono direttamente "movimentazioni economiche" (es. pagamenti, giocate, ...)	Impatto operativo di alta entità in quanto i dati interessano, ad esempio, un numero consistente di processi e/o di utenti	Perdita di immagine di elevata rilevanza in quanto i dati sono d'interesse per gran parte degli utenti esterni e/o la compromissione degli stessi può generare: <ul style="list-style-type: none">- interventi negativi sulla stampa nazionale- interventi dell'azionista e degli organi di controllo- interventi politici	Esistono sanzioni previste dalla normativa privacy, in quanto sono trattati dati personali sensibili e/o giudiziari Esistono sanzioni penali previste da altra normativa specifica applicabili al trattamento dei dati in oggetto

Tabella 19 - Legenda per la valutazione del rischio di perdita di Disponibilità

6. VALUTAZIONE DEI RISCHI PER GLI INTERESSATI RELATIVI AI DATI TRATTATI

6.1 MINACCE E SCENARI DI RISCHIO

Minacce	Scenari di rischio specifici
Accesso, trattamento non autorizzato o illegittimo relativo a dati	Accesso, trattamento non autorizzato o illegittimo relativo a dati personali comuni Accesso, trattamento non autorizzato o illegittimo relativo a dati personali sensibili Accesso, trattamento non autorizzato o illegittimo relativo a dati personali ipersensibili Accesso, trattamento non autorizzato o illegittimo relativo a dati personali specifici Accesso, trattamento non autorizzato o illegittimo relativo a dati personali giudiziari Accesso, trattamento non autorizzato o illegittimo relativo a dati personali biometrici
Divulgazione non autorizzata o accidentale di dati	Divulgazione non autorizzata o accidentale di dati personali comuni Divulgazione non autorizzata o accidentale di dati personali sensibili Divulgazione non autorizzata o accidentale di dati personali ipersensibili Divulgazione non autorizzata o accidentale di dati personali specifici Divulgazione non autorizzata o accidentale di dati personali giudiziari Divulgazione non autorizzata o accidentale di dati personali biometrici
Modifica non autorizzata o accidentale di dati	Modifica non autorizzata o accidentale di dati personali comuni Modifica non autorizzata o accidentale di dati personali sensibili Modifica non autorizzata o accidentale di dati personali ipersensibili Modifica non autorizzata o accidentale di dati personali specifici Modifica non autorizzata o accidentale di dati personali giudiziari Modifica non autorizzata o accidentale di dati personali biometrici
Perdita, distruzione accidentale o illegale di dati	Perdita, distruzione accidentale o illegale di dati personali comuni Perdita, distruzione accidentale o illegale di dati personali sensibili Perdita, distruzione accidentale o illegale di dati personali ipersensibili Perdita, distruzione accidentale o illegale di dati personali specifici

Minacce	Scenari di rischio specifici
	Perdita, distruzione accidentale o illegale di dati personali giudiziari
	Perdita, distruzione accidentale o illegale di dati personali biometrici
Indisponibilità temporanea o prolungata di dati	Indisponibilità temporanea o prolungata di dati personali comuni
	Indisponibilità temporanea o prolungata di dati personali sensibili
	Indisponibilità temporanea o prolungata di dati personali ipersensibili
	Indisponibilità temporanea o prolungata di dati personali specifici
	Indisponibilità temporanea o prolungata di dati personali giudiziari
	Indisponibilità temporanea o prolungata di dati personali biometrici

Tabella 20 – Minacce e scenari di rischio

6.2 CRITERI PER LA VALUTAZIONE DELL'IMPATTO

Danno	Descrizione
Danno fisico-biologico	La lesione di attività vitali quali: la modificazione all'aspetto esteriore di una persona; la riduzione dalla capacità di relazionarsi con altri individui; la riduzione della capacità lavorativa e/o dell'attitudine di una persona a lavorare; la perdita di chance lavorative; la perdita della capacità sessuale; il danno psichico.
Danno finanziario	Inteso come la perdita economica che colpisce direttamente l'individuo limitandone le capacità di attendere alle proprie incombenze (i.e. perdita dello stipendio).
Danno reputazionale	Inteso come la perdita della considerazione che un individuo gode nell'ambiente sociale in cui vive.
Danno di identità	Inteso come il furto che un individuo può subire della propria identità digitale con conseguenze, nei casi più gravi, anche di natura penale.

6.3 VALUTAZIONE DELL'IMPATTO

Legenda per la compilazione della matrice dell'impatto

Impatto	Danno fisico-biologico	Danno finanziario	Danno reputazionale	Danno di identità
Trascurabile	La persona fisica/interessato non ha subito una lesione nel fisico o nella psiche. Non ci sono ripercussioni negative, di carattere non patrimoniale, della lesione psicofisica	la persona fisica/interessato non ha subito una perdita economica e/o un mancato guadagno tali da comprometterne dignità e libertà	la persona fisica/interessato non subisce nessun tipo di danno che possa lederne dignità, immagine e reputazione	la persona fisica/interessato non subisce nessuna lesione della propria identità digitale
Bassa	La persona fisica può subire una lesione di lieve entità nel fisico o nella psiche. Probabili ripercussioni negative, di carattere non patrimoniale, della lesione psicofisica che possono portare ad una liquidazione del danno biologico, da parte del giudice di lieve entità (i.e. invalidità temporanea che consiste nel numero di giorni necessari per la guarigione e per il ritorno alla normale attività)	la persona fisica/interessato ha subito una perdita economica e/o un mancato guadagno classificabile come lieve (i.e. tempo dedicato allo svolgimento di pratiche burocratiche, mancata possibilità di pagare le utenze in tempo utile per non incorrere in sanzioni per il blocco dei sistemi informatici (riscossione/pagamento)	la persona fisica/interessato subisce un semplice fastidio a causa di informazioni di carattere non sensibile divulgate e/o ricevute in maniera difforme rispetto la realtà (i.e. attribuzione di titoli scolastici diversi, indicazioni di condizioni di tipo familiare non coerenti)	la persona fisica/interessato subisce un semplice fastidio dovuto a informazioni ricevute o richieste nel caso di omonimia (richiesta di pagamenti/tasse/imposte, mancata risposta a chiarimenti e/o istanze)

**METODOLOGIA
PER LA PROTEZIONE DEI DATI
E PER LA VALUTAZIONE D'IMPATTO**

IS-00-PR-07
ALLEGATO
PAG. 63 DI 70
07 LUGLIO 2020

Impatto	Danno fisico-biologico	Danno finanziario	Danno reputazionale	Danno di identità
Media	La persona fisica ha subito una lesione di media entità nel fisico o nella psiche. Ripercussioni negative, di carattere non patrimoniale, della lesione psicofisica che portano ad una liquidazione da parte del giudice del danno biologico (i.e. invalidità temporanea che consiste nel numero di giorni necessari per la guarigione e per il ritorno alla normale attività: invalidità permanente determinata in base all'età del danneggiato e dal grado di invalidità permanente calcolato sui "c. d. punti")	la persona fisica/interessato ha subito una perdita economica e/o un mancato guadagno che può comportare: pagamenti imprevisti (multe e/o imposte dovuti per calcoli errati), costi aggiuntivi (spese bancarie, spese legali), mancato accesso a servizi amministrativi o commerciali, aumento dei costi (ad esempio prezzi assicurativi aumentati), promozione di carriera persa	la persona fisica/interessato subisce l'invio di messaggi di tipo pubblicitario o promozionale che possono svelare un aspetto della propria vita riservato e risultare lesive della sua dignità (gravidanza, trattamento farmacologico, disoccupazione, difficoltà economiche, patologie mediche)	la persona fisica/interessato subisce un'illecita intrusione nella propria sfera personale da parte di soggetti terzi con scopi discriminatori (razzismo, sessismo, intimidazione politica e/o sociale)
Alta	La persona fisica ha subito una grave lesione nel fisico o nella psiche. Evidenti ripercussioni negative, di carattere non patrimoniale, della lesione psicofisica. La liquidazione da parte del giudice del danno biologico comporta un esborso economico molto oneroso (i.e. invalidità temporanea che consiste nel numero di giorni necessari per la guarigione e per il ritorno alla normale attività: invalidità	la persona fisica/interessato ha subito una perdita economica e/o un mancato guadagno che può comportare: elevate difficoltà finanziarie con obbligo di richiesta di prestiti, perdita di proprietà e/o alloggi, mancata possibilità di adempiere ad obbligazioni contrattuali per indisponibilità di denaro, perdita di occupazione/tirocini /impiego (anche a tempo determinato), impossibilità di	la persona fisica/interessato subisce gravi conseguenze per la propria dignità e che portano alla perdita di onorabilità/danni all'immagine (notizie su TV, stampa o social media), perdita/impossibilità occupazionale, lesione della propria posizione creditizia/economica	la persona fisica/interessato subisce conseguenze irreversibili quali sanzioni di tipo penale, perdita di diritti/status amministrativo/autoromia (i.e. procedura di interdizione, inabilitazione, disconoscimento della patria potestà)

**METODOLOGIA
PER LA PROTEZIONE DEI DATI
E PER LA VALUTAZIONE D'IMPATTO**

IS-00-PR-07
ALLEGATO
PAG. 64 DI 70
07 LUGLIO 2020

Impatto	Danno fisico-biologico	Danno finanziario	Danno reputazionale	Danno di identità
	permanente determinata in base all'età del danneggiato e dal grado di invalidità permanente calcolato sui "c. d. punti")	proseguire il percorso di studio/abilitazione/perfezionamento intrapreso		

Tabella 21 – Legenda per la valutazione impatto

6.4 VALUTAZIONE DELLA PROBABILITÀ DI ACCADIMENTO

Legenda per la valutazione della probabilità di accadimento

T	Agenti INTERNI	Un potenziale attaccante interno non otterrebbe vantaggi significativi (es. a seguito di compromissione dei dati o del servizio).
		Il clima dell'organizzazione in relazione all'ambito in analisi (es. opinioni, pareri, ...) è positivo.
	Agenti ESTERNI	Il servizio non risulta di interesse sociale, economico, politico e mediatico.
B	Agenti INTERNI	Un potenziale attaccante esterno non otterrebbe vantaggi significativi (es. a seguito di compromissione dei dati o del servizio).
		Il contesto di riferimento (es. normativa di riferimento, tipologie di soggetti coinvolti, complessità operativa, ...) non è complesso.
	Errori/eventi ACCIDENTALI	La frequenza di accadimento degli eventi accidentali registrati è molto bassa.
B	Agenti INTERNI	Un potenziale attaccante interno potrebbe ottenere lievi vantaggi (es. a seguito di compromissione dei dati o del servizio).
		Il clima dell'organizzazione in relazione all'ambito in analisi è o potrebbe essere influenzato da criticità non significative (es. opinioni contrarie, incertezze, ...).
	Agenti ESTERNI	Il servizio risulta di scarso interesse sociale, economico, politico e mediatico.
M	Agenti INTERNI	Un potenziale attaccante esterno potrebbe ottenere lievi vantaggi (es. a seguito di compromissione dei dati o del servizio).
		Il contesto di riferimento (es. normativa di riferimento, tipologie di soggetti coinvolti, complessità operativa, ...) è di bassa complessità.
	Errori/eventi ACCIDENTALI	La frequenza di accadimento degli eventi accidentali registrati è bassa.
M	Agenti INTERNI	Un potenziale attaccante interno potrebbe ottenere vantaggi (es. a seguito di compromissione dei dati o del servizio).
		Il clima dell'organizzazione in relazione all'ambito in analisi è o potrebbe essere parzialmente negativo (es. dissensi, opposizioni).

A	Agenti ESTERNI	Il servizio è di interesse sociale, economico, politico e mediatico o risulta significativo per le attività di determinate categorie di utenti esterni (es. professionisti, fornitori, ...).
		Un potenziale attaccante esterno potrebbe ottenere vantaggi (es. a seguito di compromissione dei dati o del servizio).
	Errori/eventi ACCIDENTALI	Il contesto di riferimento (es. normativa di riferimento, tipologie di soggetti coinvolti, complessità operativa, ...) è di ordinaria complessità.
		La frequenza di accadimento degli eventi accidentali registrati è media.
	Agenti INTERNI	Un potenziale attaccante interno potrebbe ottenere grandi vantaggi (es. a seguito di compromissione dei dati o del servizio).
		Il clima dell'organizzazione in relazione all'ambito in analisi è o potrebbe essere fortemente negativo (es. forti dissensi, proteste).
	Agenti ESTERNI	Il servizio risulta di grande interesse sociale, economico, politico e mediatico (es. pubblicizzato sulla stampa nazionale) e l'ambito in cui si colloca è in particolare fermento.
		Un potenziale attaccante esterno potrebbe ottenere grandi vantaggi (es. a seguito di compromissione dei dati o del servizio).
	Errori/eventi ACCIDENTALI	Il contesto di riferimento (es. normativa di riferimento, tipologie di soggetti coinvolti, complessità operativa, ...) presenta una elevata complessità.
		La frequenza di accadimento degli eventi accidentali registrati è alta.

Tabella 22 – Legenda per la valutazione probabilità di accadimento

6.5 VALUTAZIONE DEL RISCHIO INTRINSECO PER DIRITTI E LIBERTÀ DELL'INTERESSATO

Si riporta un esempio di valutazione e compilazione della tabella dei rischi per i diritti e le libertà degli interessati, in relazione alle categorie di dati trattati.

**METODOLOGIA
PER LA PROTEZIONE DEI DATI
E PER LA VALUTAZIONE D'IMPATTO**

IS-00-PR-07
ALLEGATO
PAG. 67 DI 70
07 LUGLIO 2020

Minacce	Rischio Intrinseco per scenario specifico	Probabilità di accadimento	Gravità Danno Fisico-Biologico	Gravità Danno Finanziario	Gravità Danno Reputazionale	Gravità Danno Identità	Rischio Intrinseco (max per scenario specifico)	Rischio Intrinseco relativo alla minaccia
Accesso, trattamento non autorizzato o illecito relativo a dati	Accesso, trattamento non autorizzato o illecito relativo a dati personali comuni	M	M	M	M	M	M	Max dei rischi intrinseci sugli scenari applicabili
	Accesso, trattamento non autorizzato o illecito relativo a dati sensibili	A	M	A	A	A	A	
	Accesso, trattamento non autorizzato o illecito relativo a dati ipersensibili	A	A	A	A	A	A	
	Accesso, trattamento non autorizzato o illecito relativo a dati specifici	A	M	A	A	A	A	
	Accesso, trattamento non autorizzato o illecito relativo a dati giudiziari	A	M	A	A	A	A	
	Accesso, trattamento non autorizzato o illecito relativo a dati biometrici	A	M	M	A	A	A	
Divulgazione non autorizzata o accidentale di dati	Divulgazione non autorizzata o accidentale di dati personali comuni	M	M	M	M	M	M	Max dei rischi intrinseci sugli scenari applicabili
	Divulgazione non autorizzata o accidentale di dati sensibili	A	M	A	A	A	A	
	Divulgazione non autorizzata o accidentale di dati ipersensibili	A	A	A	A	A	A	
	Divulgazione non autorizzata o accidentale di dati specifici	A	M	A	A	A	A	
	Divulgazione non autorizzata o accidentale di dati giudiziari	A	M	A	A	A	A	
	Divulgazione non autorizzata o accidentale di dati biometrici	A	M	A	A	A	A	
Modifica non autorizzata o accidentale di dati	Modifica non autorizzata o accidentale di dati personali comuni	M	M	M	M	M	M	Max dei rischi intrinseci sugli scenari applicabili
	Modifica non autorizzata o accidentale di dati sensibili	A	M	A	A	A	A	
	Modifica non autorizzata o accidentale di dati ipersensibili	A	A	A	A	A	A	

**METODOLOGIA
PER LA PROTEZIONE DEI DATI
E PER LA VALUTAZIONE D'IMPATTO**

IS-00-PR-07
ALLEGATO
PAG. 68 DI 70
07 LUGLIO 2020

Minacce	Rischio Intrinseco per scenario specifico	Probabilità di accadimento	Gravità Danno Fisico-Biologico	Gravità Danno Finanziario	Gravità Danno Reputazionale	Gravità Danno Identità	Rischio Intrinseco (max per scenario specifico)	Rischio Intrinseco relativo alla minaccia
	Modifica non autorizzata o accidentale di dati specifici	A	M	A	A	A	A	Max dei rischi intrinseci sugli scenari applicabili
	Modifica non autorizzata o accidentale di dati giudiziari	A	M	A	A	A	A	
	Modifica non autorizzata o accidentale di dati biometrici	A	M	A	A	A	A	
Perdita, distruzione accidentale o illecita di dati	Perdita, distruzione accidentale o illecita di dati personali comuni	M	M	M	M	M	M	Max dei rischi intrinseci sugli scenari applicabili
	Perdita, distruzione accidentale o illecita di dati sensibili	M	M	A	M	A	A	
	Perdita, distruzione accidentale o illecita di dati ipersensibili	M	A	A	M	A	A	
	Perdita, distruzione accidentale o illecita di dati specifici	M	M	A	M	A	A	
	Perdita, distruzione accidentale o illecita di dati giudiziari	M	M	A	M	A	A	
	Perdita, distruzione accidentale o illecita di dati biometrici	M	M	M	M	A	A	
Indisponibilità temporanea o prolungata di dati	Indisponibilità temporanea o prolungata di dati personali comuni	M	M	M	M	M	M	Max dei rischi intrinseci sugli scenari applicabili
	Indisponibilità temporanea o prolungata di dati sensibili	M	M	A	M	A	A	
	Indisponibilità temporanea o prolungata di dati ipersensibili	M	A	A	M	A	A	
	Indisponibilità temporanea o prolungata di dati specifici	M	M	A	M	A	A	
	Indisponibilità temporanea o prolungata di dati giudiziari	M	M	A	M	A	A	
	Indisponibilità temporanea o prolungata di dati biometrici	M	M	M	M	A	A	

Tabella 23 - Stima del rischio intrinseco per i diritti e le libertà dell'interessato

7. VALUTAZIONE DEI RISCHI PER GLI INTERESSATI RELATIVI ALLE CATEGORIE DI TRATTAMENTO

Criteri per individuazione di trattamenti ad alto rischio per diritti e libertà dell'interessato	Esempi di trattamento
Valutazione o assegnazione di un punteggio (incluse le attività di profilazione e le analisi di tipo predittivo) riferita ad un individuo	Il trattamento prevede: - l'uso di database per la valutazione del rischio creditizio, per la lotta alle frodi o al riciclaggio e al finanziamento del terrorismo (AML/CTF); - test genetici offerti direttamente ai consumatori per finalità predittive del rischio di determinate patologie o in generale per lo stato di salute; - la creazione di profili comportamentali o marketing a partire dalle operazioni o dalla navigazione compiute sul sito web del Titolare.
Decisioni automatizzate con significativi effetti giuridici o di analoga natura	Il trattamento può comportare l'esclusione di una persona fisica da determinati benefici ovvero la sua discriminazione. Il trattamento che produce effetti minimi o nulli su un interessato non soddisfa questo specifico criterio.
Monitoraggio sistematico di individui (es. mediante videosorveglianza)	Il trattamento prevede il monitoraggio sistematico in termini di controllo e sorveglianza di soggetti interessati, anche in spazi pubblici (ad es. videosorveglianza di stazioni, aeroporti, aree di grandi dimensioni)
Elaborazione di dati sensibili o dati aventi carattere altamente personale	Il trattamento prevede l'uso di categorie di dati particolari (stato di salute, opinioni politiche, credo religioso, etc.) o che possano accrescere i rischi per i diritti e le libertà degli interessati (dati di localizzazione, finanziari, dati strettamente personali e confidenziali, etc.) di cui agli artt. 9 e 10 del RGPD
Elaborazione di dati su larga scala (es. per numero di individui coinvolti, volumi complessivi, durata o persistenza, ambito geografico)	Il trattamento prevede che siano elaborati dati su larga scala in termini di : - numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; - volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; - durata, o persistenza, dell'attività di trattamento; - ambito geografico dell'attività di trattamento.
Combinazione o raffronto tra banche dati provenienti da due o più operazioni di trattamento effettuati per scopi diversi	Il trattamento prevede che siano per esempio utilizzati dati derivanti da due o più trattamenti ma svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato (ad es. dati raccolti per finalità di erogazione di servizi a famiglie associati a dati riferiti alle possibilità di spesa sulla base di condizioni reddituali)

**METODOLOGIA
PER LA PROTEZIONE DEI DATI
E PER LA VALUTAZIONE D'IMPATTO**

IS-00-PR-07
ALLEGATO
PAG. 70 DI 70
07 LUGLIO 2020

Elaborazione di dati relativi a soggetti vulnerabili per cui è più accentuato lo squilibrio di poteri fra interessato e titolare del trattamento (es. minori, anziani, dipendenti)	Il trattamento prevede l'elaborazione di dati e di informazioni riferite a minori o a persone che non siano in grado di opporsi o acconsentire, in modo consapevole e ragionato, al trattamento dei propri dati personali (i soggetti con patologie psichiatriche, i richiedenti asilo, gli anziani, i pazienti) e ogni interessato per il quale si possa identificare una situazione di disequilibrio nel rapporto con il rispettivo titolare del trattamento.
Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative	il trattamento prevede l'associazione di tecniche dattiloskopiche (digitazione del PIN) con il riconoscimento del volto per migliorare il controllo degli accessi fisici oppure il trattamento l'utilizzo di applicazioni legate al c.d. "Internet delle cose" (biomedicale, monitoraggio, servizi ai cittadini riferibili alle smart city)
Impedimento all'interessato di esercitare un diritto o di avvalersi di un servizio o di un contratto	Il trattamento non prevede il diritto alla portabilità dei dati o la cancellazione dei dati

Tabella 24 - Categorie trattamento ad alto rischio per diritti e libertà interessato



FLUSSO DI NOTIFICA DI *DATA BREACH* ALL'AMMINISTRAZIONE TITOLARE

Nel presente documento è descritto il flusso di notifica delle violazioni dei dati personali che presentano un rischio per i diritti e le libertà delle persone fisiche (*Data Breach*) in conformità a quanto previsto dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 ("Regolamento Generale sulla Protezione dei Dati" - d'ora in avanti "RGPD").

Ai sensi dell'articolo 4 del RGPD per "violazione dei dati personali" si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Il flusso inizia con l'identificazione di una possibile "violazione dei dati personali" nell'ambito della gestione di un evento di sicurezza e si conclude con l'invio della notifica di avvenuto *Data Breach* all'Amministrazione Titolare affinché quest'ultima possa adempiere agli obblighi previsti dagli articoli 33 e 34 del RGPD.

Il flusso prevede l'interazione e lo scambio di informazioni tra:

- Ministero della Salute (Amministrazione Titolare interessata dall'evento) e il Responsabile Protezione Dati della stessa (d'ora in avanti RPD)
- Agenzia Nazionale per i Servizi Sanitari Regionali - AGENAS (Responsabile del Trattamento ex art. 28 RGPD) e il RPD della stessa
- Sogei (Sub-Responsabile del Trattamento) e il RPD della stessa

al fine di consentire all'Amministrazione Titolare di adempiere alle prescrizioni previste dal RGPD.

1. DESCRIZIONE DEL FLUSSO

Il flusso di notifica all'Amministrazione Titolare prevede i passi di seguito elencati.

-
- Il CERT Sogei (struttura aziendale preposta al trattamento degli incidenti di sicurezza informatica), nel corso della gestione di un incidente di sicurezza, rileva una possibile "violazione dei dati personali". Il CERT Sogei comunica all'Amministrazione Titolare, al Responsabile del Trattamento e ai rispettivi RPD che è in corso la valutazione di un incidente di sicurezza, fornendo, altresì, una prima sommaria descrizione dell'incidente e assegnando un identificativo univoco allo stesso. Il CERT Sogei invia le informazioni scrivendo agli *indirizzi di posta forniti dall'Amministrazione Titolare e dal Responsabile del Trattamento a cui notificare l'incidente*.

Nel caso in cui sia l'Amministrazione Titolare a venire a conoscenza di un incidente di sicurezza caratterizzato da una possibile "violazione dei dati personali" che necessita dell'intervento di Sogei, l'Amministrazione Titolare informa il Responsabile del Trattamento e il relativo RPD scrivendo agli *indirizzi di posta comunicati a cui notificare l'incidente*, nonché Sogei e il relativo RPD scrivendo a cert@sogei.it e ufficiodpo@sogei.it. Il CERT Sogei avvia la verifica fornendo eventualmente informazioni aggiuntive a quelle ricevute e assegnando un identificativo univoco all'incidente.

Nel caso in cui sia il Responsabile del Trattamento a venire a conoscenza di un incidente di sicurezza caratterizzato da una possibile "violazione dei dati personali" che necessita dell'intervento di Sogei, il Responsabile del Trattamento informa l'Amministrazione Titolare e il relativo RPD scrivendo agli *indirizzi di posta forniti a cui notificare l'incidente*, nonché Sogei e il relativo RPD scrivendo a cert@sogei.it e ufficiodpo@sogei.it. Il CERT Sogei avvia la verifica fornendo eventualmente informazioni aggiuntive a quelle ricevute e assegnando un identificativo univoco all'incidente.

- Il CERT Sogei verifica la presenza o meno della "violazione di dati personali".
- In caso di esito negativo della verifica, il CERT Sogei termina il processo, comunicando all'Amministrazione Titolare, al Responsabile del Trattamento e ai rispettivi RPD la chiusura dell'incidente caratterizzato dall'identificativo precedentemente comunicato e le motivazioni.
- In caso di esito positivo della verifica (ossia è stata accertata la "violazione di dati personali" ed è stata valutata la gravità dell'evento da intendersi come la stima del potenziale impatto sugli interessati derivante dalla violazione), il CERT Sogei comunica immediatamente e senza ingiustificato ritardo e in modo dettagliato il *Data Breach* all'Amministrazione Titolare, al Responsabile del Trattamento e, contestualmente, ai rispettivi RPD, riportando le informazioni di propria competenza, indicate nel successivo paragrafo 2. La suddetta comunicazione viene inviata dalla casella PEC del CERT Sogei (cert@pec.sogei.it) verso le caselle PEC dell'Amministrazione Titolare, del Responsabile del Trattamento e dei rispettivi RPD o, laddove non disponibili, verso le caselle di posta elettronica ordinaria di questi ultimi.

- l'Amministrazione Titolare, ricevuta la notifica di *Data Breach* e sentito il proprio RPD, valuta, anche mediante l'eventuale supporto del Responsabile del Trattamento, il livello di gravità della "violazione di dati personali" proposto da Sogei. Nel caso in cui la "violazione di dati personali" comporti un rischio per i diritti e le libertà delle persone fisiche, l'Amministrazione Titolare provvede a completare la notifica con le informazioni di propria competenza e ad inviare la stessa all'Autorità di Controllo entro 72 ore dalla conoscenza dell'avvenuta compromissione dei dati personali, dandone contestualmente riscontro al Responsabile del Trattamento, al CERT Sogei e ai rispettivi RPD. Qualora la notifica all'Autorità di Controllo non sia effettuata entro 72 ore, l'Amministrazione Titolare provvede, altresì, a corredarla con le motivazioni del ritardo.

Eventuali richieste di ulteriori informazioni o modifiche alla notifica all'Autorità di Controllo, necessarie durante le attività di risoluzione dell'incidente, saranno concordate tra l'Amministrazione Titolare, il Responsabile del Trattamento, il CERT Sogei e i rispettivi RPD.

Il CERT Sogei dovrà mantenere un'accurata documentazione di tutte le "violazioni di dati personali" registrate, comprese le circostanze ad esse relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione sarà integrata con le eventuali azioni intraprese dall'Amministrazione Titolare e/o dal Responsabile del Trattamento e opportunamente comunicate al CERT Sogei.

2. CONTENUTI DELLA NOTIFICA DI DATA BREACH ALL'AMMINISTRAZIONE TITOLARE

Le informazioni previste dal RGPD saranno raccolte e riportate nella notifica di avvenuto *Data Breach*.

Il CERT Sogei utilizzerà il modulo disponibile sul sito dell'Autorità di Controllo per fornire le informazioni necessarie all'Amministrazione Titolare, comprendenti almeno le seguenti:

- tipologia di incidente;
- descrizione del servizio impattato e/o della banca/banche dati oggetto di violazione di dati personali;
- intervallo temporale dell'incidente;
- luogo dell'incidente;
- misure tecniche di sicurezza applicate ai dati violati;
- misure attivate per il contenimento e la prevenzione;

- descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- descrizione della probabile conseguenza della violazione dei dati personali;
- descrizione delle misure di sicurezza adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione di dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

LA PRESENTE COPIA E' CONFORME ALL'ORIGINALE DEPOSITATO.
Elenco firme associate al file con impronta SHA1 (hex):

D3-3B-41-4D-68-81-D7-09-DF-F2-96-A2-AE-43-DF-FF-54-82-AB-AF

PAdES 1 di 3 del 20/06/2022 08:42:52

Soggetto: MINENNA MAURO TINIT-MNNMRA69S15A662R



Validità certificato dal 08/04/2021 06:23:34 al 07/04/2024 06:23:34

Rilasciato da Poste Italiane S.p.A. con S.N. 18311381

PAdES 2 di 3 del 21/06/2022 21:51:40

Soggetto: LEONARDI GIOVANNI TINIT-LNRGNM63L09C351R



Validità certificato dal 26/09/2019 14:37:00 al 24/09/2022 22:00:00

Rilasciato da Namirial S.p.A./02046570426 con S.N. 7BC35F7F

PAdES 3 di 3 del 24/06/2022 09:30:09

Soggetto: ANDREA QUACIVI TINIT-QCVNDR70M14H501Q



Validità certificato dal 14/12/2020 11:41:37 al 14/12/2023 00:00:00

Rilasciato da INFOCERT SPA con S.N. 145845D