ADEGUAMENTO PRIVACY SISTEMA DI PROTOCOLLO INFORMATICO E DI GESTIONE DOCUMENTALE P@DOC

contec aqs
AMBIENTE QUALITÀ SICUREZZA
gruppo contec

UNIONE EUROPEA
Fondo Sociale Europeo
Fondo Europeo di Sviluppo Regionale

Agenzia per la Coesione Territoriale

PON GOVERNANCE E CAPACITÀ ISTITUZIONALE 2014-2020

Indice generale

1. OBIETTIVO DEL DOCUMENTO 3
2. NORME E STANDARD DI RIFERIMENTO 3
3. DOCUMENTAZIONE E STRUMENTI ADOTTATI ALL'INTERNO DEL COMUNE DI PADOVA 4
4. ANALISI DEL CONTESTO E STAKEHOLDERS 5
5. ANALISI DELLE ENTITÀ DEL SISTEMA 9
6. LA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI – DATA PROTECTION IMPACT ASSESSMENT (DPIA) 10
7. ULTERIORI ANALISI FUNZIONALI ALLA CONFORMITÀ DEL SISTEMA 11
7.1. DATABASE P@DOC 11
7.2. IMPLEMENTAZIONE DELLA NORMA 11
8. CONCLUSIONI 12
8.1. DEFINIZIONE E IMPLEMENTAZIONE DI UNA CLASSIFICAZIONE DELLA RISERVATEZZA 13
8.2. GARANZIA DELL'ESERCIZIO DEI DIRITTI DELL'INTERESSATO 14
8.3. IMPLEMENTAZIONE SISTEMA DI PSEUDONIMIZZAZIONE O ANONIMIZZAZIONE - PARTIZIONAMENTO 15
8.4. INFORMATIVA AI DIPENDENTI 15
8.5. REDAZIONE E AGGIORNAMENTO DEL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO 15
8.6. AGGIORNAMENTO DEL REGOLAMENTO SULL'ACCESSO (anche per fini storici) 16
8.7. REDAZIONE E IMPLEMENTAZIONE DEL REGOLAMENTO PRIVACY E SICUREZZA 16
8.8. REVISIONE E AUDIT DEL SISTEMA DI GESTIONE DOCUMENTALE 16
8.9. VIGILANZA SULLA PROTEZIONE DEI DATI PERSONALI 16

1. OBIETTIVO DEL DOCUMENTO

Questo documento vuole descrivere lo stato di fatto, la documentazione, e le politiche adottate nell'ambito del sistema di protocollo informatico e di gestione documentale p@doc ed in particolar modo sulla protezione dei dati e sulla sicurezza. Si considera in particolare l'esperienza del Comune di Padova, in qualità di ente cedente all'interno del progetto PRODIGIO.

2. NORME E STANDARD DI RIFERIMENTO

Il seguente documento fa riferimento alle norme e agli standard nazionali ed internazionali in materia di amministrazione digitale e gestione documentale, tutela e conservazione degli archivi, protezione dei dati personali e sicurezza informatica. Nello specifico:

- Decreto del Presidente della Repubblica 20 dicembre 2000 n. 445 - *Testo unico delle* disposizioni legislative e regolamentari in materia di documentazione amministrativa
- Decreto legislativo 7 marzo 2005 n. 82 - *Codice dell'amministrazione digitale*
- Decreto Legislativo 22 gennaio 2004, n. 42 - *Codice dei beni culturali e del paesaggio*
- Decreto Legislativo 30 giugno 2003, n. 196 - *Codice in materia di protezione dei dati personali*
- Regolamento UE 679/2016 – General data protection regulation
- Legge 7 agosto 1990 n. 241 - *Nuove norme in materia di procedimento* amministrativo e di diritto di accesso ai documenti amministrativi
- ISO 31000:2010 - Risk management - Principles and guidelines
- ISO/IEC 29134:2017 - Information technology – Security techniques – Guidelines for privacy impact assessment
- ISO 27000:2018 – Information technology — Security techniques — Information security management systems — Overview and vocabulary
- ISO 15489-1:2016 - Information and documentation - Records management -- Part 1: Concepts and principles
- ISO 15489-2:2001 - Information and documentation - Records management -- Part 2: Guidelines

- MoReq2010 - Modular Requirement for Records Systems

3. DOCUMENTAZIONE E STRUMENTI ADOTTATI ALL'INTERNO DEL COMUNE DI PADOVA

La documentazione utilizzata nell'ambito del protocollo informatico e nella gestione documentale è la seguente:

Manuale di gestione dei documenti e dei flussi documentali del Comune di Padova: documento redatto ai sensi dell'art. 5, comma 1, del Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 - *Regole tecniche per il protocollo informatico* che "descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi".

Censimento delle Istanze e dei documenti: survey che ha permesso la costituzione di una base informativa dei procedimenti esistenti all'interno dell'Ente. Si configura come uno strumento di rilevazione della produzione documentale dal punto di vista quantitativo e qualitativo (conformità alle regole tecniche e agli standard), che permette la definizione degli attori coinvolti nei processi, le responsabilità e gli strumenti di produzione utilizzati.

Registro del titolare e del responsabile del trattamento: registro istituito ai sensi dell'art. 30 del Regolamento UE 679/2016 che riporta le attività di trattamento svolte sotto la responsabilità di ogni titolare e responsabile del trattamento. Il registro è uno degli elementi funzionali per la definizione del quadro generale di accountability ed è istituito al fine di garantire un monitoraggio al titolare del trattamento e alle Autorità per garantire la cooperazione tra i due soggetti. Per la corretta formazione del Registro delle attività di trattamento il Comune di Padova ha implementato il database formato con l'attività del Censimento delle Istanze e dei documenti collegando i processi/procedimenti/attività dell'Ente con le informazioni minime definite dall'art. 30, paragrafo 1, che sono:

CAMPO	DESCRIZIONE
Finalità del trattamento	Descrive la finalità del trattamento
Tipologia di trattamento	Descrive il tipo di attività implicata nel trattamento
Categorie di soggetti interessati	Descrive i soggetti interessati al trattamento dei dati
Categorie di dati personali	Descrive le categorie di dati personali coinvolti nel trattamento comprese le categorie particolari di dati personali (ex. Art 9 del GDPR) e i dati relativi a condanne e reati (ex. Art. 10 del GDPR)

Categorie di soggetti destinatari	Descrive le categorie dei soggetti destinatari della comunicazione dei dati personali.
Trasferimento a soggetti extra UE	Indica se i dati sono trasferiti a soggetti extra UE e le eventuali garanzie richieste
Base giuridica del trattamento	Indica quale la base giuridica del trattamento al fine di rispondere al requisito di liceità del trattamento
Termini ultimi previsti per la cancellazione	Indica il periodo di conservazione del dato
Banche dati interne	Indica le eventuali banche dati interne utilizzate per il trattamento
Banche dati esterne	Indica le eventuali banche dati esterne utilizzate per il trattamento
Informativa del trattamento	Indica se è presente l'informativa per il trattamento dei dati personali
Contitolare del trattamento	Indica se è presente un contitolare del trattamento
Altri soggetti interni autorizzati al trattamento	Indica eventuali altri soggetti autorizzati al trattamento (altri settori, amministratori)
Responsabili esterni del trattamento	Indica se vi sono responsabili esterni del trattamento
Misure di sicurezza informatiche adottate	Indica le misure di sicurezza tecniche e informatiche adottate dall'Ente
Misure di sicurezza organizzative adottate	Indica le misure di sicurezza organizzative adottate dall'Ente
È necessaria una valutazione di impatto	In base ai campi selezionati precedentemente, si definisce in automatico se sia necessario effettuare una valutazione di impatto sul trattamento descritto
Valutazione dell'impatto	Definisce il valore di impatto e le soglie di rischio del trattamento
Note	Campo dove gli utenti possono inserire note e commenti al proprio trattamento.

4. ANALISI DEL CONTESTO E STAKEHOLDERS

Il sistema di protocollo informatico e di gestione documentale p@doc è lo strumento attraverso il quale l'organizzazione garantisce l'effettiva ricezione, trasmissione e gestione dei documenti informatici. Questo si serve di strumenti di gestione quali il titolario di classificazione, l'oggettario, l'organigramma, il repertorio dei fascicoli, il piano di fascicolazione e il piano di conservazione.

Oltre ad essere uno strumento di gestione documentale, il registro di protocollo si qualifica sia come **strumento giuridico**, in quanto attesta con certezza giuridica il momento dell'ingresso e dell'uscita dei documenti dall'organizzazione (atto pubblico di fede privilegiata) che come **strumento archivistico** in quanto descrive i documenti del soggetto produttore e determina, grazie agli strumenti di gestione sopracitati, la loro collocazione nell'archivio.

Valutando il sistema nell'ambito della protezione dei dati personali, il registro di protocollo va visto altresì come una banca dati contenente dati personali e categorie particolari di dati personali e dati personali relativi a condanne e reati (artt. 9-10 del Regolamento).

Diviene utile eseguire una valutazione iniziale ai fini di quantificare i dati registrati all'interno del sistema di protocollo nell'anno 2018. Attualmente il sistema prevede la definizione di tre livelli di riservatezza da aggiornare al nuovo Regolamento UE 679/2016 :

- 1 – Privacy – D.lvo 196/2003, utilizzato per la registrazione di documenti contenenti dati sensibili e sensibilissimi così definiti dal Codice in materia di protezione dei dati, e riqualificati dal Regolamento UE come categorie particolari di dati personali e dati personali relativi a condanne e reati;
- 2 – Riservato – L.241/90 documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, potrebbero ostacolare il raggiungimento degli obiettivi prefissati o procurare pregiudizio a terzi o al buon andamento dell'attività amministrativa (tipologie documentarie definite dalla Legge 241/1990, art. 24);
- 3 – Sottratto all'accesso - Livello in disuso.

ANNO 2018	Protocolli E	Protocolli U	Protocolli I	Totale
0- Non riservato	277072	150012	48951	476035
1- Privacy – D.Lvo 196/2003	13045	9133	2287	24465
2- Riservato – L. 241/90	375	398	102	875
3- Sottratto all'accesso	22	31	1	54

In sintesi risulta che il 5,33% dei protocolli registrati (in entrata, uscita ed interni) presso l'Ente ha carattere di riservatezza. Ulteriori dati rilevanti sono riportati nella tabella che segue, nella quale si confronta il totale di protocolli registrati dai diversi settori dell'Ente con il totale dei protocolli riservati, riportando poi la percentuale dei riservati:

Denominazione Settore	totale_protocolli	protocolli_riservati	Percentuali
Settore Sicurezza, Salute, Prevenzione e Grandi eventi	5220	2630	50,38%
Settore Servizi Sociali	46066	16747	36,35%
Settore Risorse Umane	8259	506	6,13%
Settore Servizi Informatici e Telematici	2300	107	4,65%
Settore Urbanistica, Servizi Catastali e Mobilità	11436	515	4,50%
Settore Programmazione Controllo e Statistica	427	16	3,75%
Segreteria Direzione Generale	443	14	3,16%
Settore Servizi Istituzionali	67065	2056	3,07%
Settore Cultura, Turismo, Musei e Biblioteche	7667	159	2,07%
Settore Gabinetto del Sindaco	8981	174	1,94%
Settore Servizi Scolastici	20282	366	1,80%
Settore Risorse Finanziarie	1015	18	1,77%
Settore Ambiente e Territorio	6657	94	1,41%
Settore Verde, parchi e agricoltura urbana	1700	17	1,00%
Settore Lavori Pubblici- ex Opere Infrastrutturali	10585	101	0,95%
Settore Servizi Demografici e Cimiteriali. Decentramento	113677	1068	0,94%
Settore Tributi e Riscossione	20431	123	0,60%
Settore Servizi Sportivi	6351	36	0,57%
Settore Polizia Locale e Protezione Civile	84793	444	0,52%
Sportello unico attività produttive e attività economiche	22068	113	0,51%
Settore Patrimonio, Partecipazioni e Avvocatura	6910	25	0,36%
Settore Edilizia Privata	13093	42	0,32%
Settore Contratti Appalti e Provveditorato	27230	72	0,26%
Settore Lavori Pubblici- ex Edilizia Pubblica	6679	17	0,25%
Ed. Privata- Sportello front office	1329	0	0,00%
Presidente Consiglio Comunale	205	0	0,00%

Sono evidenziati i settori che svolgono un attività consistente all'interno del sistema distinguendo quelli che produco un maggior numero di protocolli (colore arancio), da quelli che producono una maggior numero / percentuale di protocolli riservati (colore verde).

Un ulteriore attività utile alla realizzazione del progetto (piano) di adeguamento è quella di identificare gli stakeholder, ossia le persone o le organizzazioni che possono influenzare, essere influenzate da, o percepire se stesse come influenzate dal sistema. Per ogni stakeholder individuato sarà definita la tipologia (interno o esterno), il contributo e/o l'interesse al progetto, definendo infine quali di questi debbano essere coinvolti per ottenere contributi e suggerimenti.

Stakeholders	Tipologia	Contributo	Interesse
Dipendenti	Interni	- Segnalazione delle criticità e delle necessità del sistema	- Tutela dei propri dati personali ed esercizio dei propri diritti.
Utenti del	Interni	- Corretto uso del sistema e degli	- Tutela della propria attività,

sistema		strumenti a corredo, segnalazione delle criticità e delle necessità del sistema - Segnalazione delle criticità e delle necessità del sistema rilevate dagli stakeholder esterni.	- Efficienza ed usabilità del sistema - Reperibilità delle informazioni.
Amministratori del sistema	Interni	- Amministrazione del sistema - coordinamento delle attività - definizione, condivisione e aggiornamento delle politiche di gestione del sistema e degli strumenti a corredo - monitoraggio e verifica - rilevazione delle criticità e delle necessità del sistema - formazione e supporto agli utenti del sistema.	- Tutela della propria attività, - efficienza ed usabilità del sistema, - garantire la riservatezza, l'integrità e la disponibilità informazioni, - garantire la conformità a leggi e regolamenti
Amministratori (Sindaco, Assessori, consiglieri)	Interni	- Approvazione del sistema e condivisione delle politiche di gestione del sistema	- Garantire la reputazione dell'organizzazione - garantire servizi ai cittadini e agli stakeholders esterni. - garantire la conformità a leggi e regolamenti
Rappresentanze sindacali	Interni	- segnalazione delle criticità e delle necessità del sistema rilevate dai dipendenti	- Garantire la tutela dei dati personali dei dipendenti e l'esercizio dei diritti.
Cittadini	Esterni	- Segnalazione delle criticità e delle necessità nell'uso dei servizi	- Tutela dei propri dati personali ed esercizio dei propri diritti. - Efficienza dei servizi resi dall'organizzazione - Tutela dei propri dei propri interessi economici
Istituzioni pubbliche centrali e locali	Esterni	- Condivisione delle politiche di gestione e degli strumenti a corredo	- Efficienza dei servizi resi dall'organizzazione - Garantire la reputazione dell'organizzazione
Associazioni	Esterni	- Segnalazione delle criticità e delle necessità nell'uso dei servizi	- Tutela dei dati personali ed esercizio dei diritti della propria categoria - Efficienza dei servizi resi dall'organizzazione - Tutela dei propri degli interessi economici propri o della categoria

			rappresentata
Fornitori di beni e servizi	Esterni	- Segnalazione delle criticità e delle necessità nell'uso dei servizi	- Tutela dei propri dati personali ed esercizio dei propri diritti. - Efficienza dei servizi resi dall'organizzazione - Tutela dei propri dei propri interessi economici
Imprese	Esterni	- Segnalazione delle criticità e delle necessità nell'uso dei servizi	- Tutela dei propri dati ed esercizio dei propri diritti. - Efficienza dei servizi resi dall'organizzazione - Tutela dei propri dei propri interessi economici
Mass Media	Esterni	- Segnalazione delle criticità e delle necessità nell'uso dei servizi	- Tutela dei propri dati ed esercizio dei propri diritti. - Efficienza dei servizi resi dall'organizzazione - Accessibilità ai dati e garanzia del diritto di cronaca e di libertà di manifestazione del pensiero
Gruppi informali	Esterni	- Segnalazione delle criticità e delle necessità nell'uso dei servizi	- Tutela dei propri dati ed esercizio dei propri diritti. - Efficienza dei servizi resi dall'organizzazione - Tutela dei propri dei propri interessi economici

Vista l'analisi dei dati e la mappatura dei principali stakeholder si ritiene opportuno coinvolgere nella valutazione di impatto gli amministratori del sistema gli utenti interni del sistema.

Tra gli amministratori del sistema si identificano le seguenti figure da coinvolgere:

- Responsabile della Gestione Documentale
- Referente informatico sistema p@doc

Per quanto riguarda gli utenti del sistema la scelta si baserà su due aspetti: il carico di lavoro e la percentuale dei protocolli riservati registrati. Saranno coinvolti nella valutazione di impatto il Settore Servizi Istituzionali (Ufficio Protocollo generale), Settore Servizi Sociali e Settore Risorse Umane.

Si ritiene opportuno aprire un dialogo con i settori evidenziati per comprendere le esigenze degli utenti del sistema e le eventuali segnalazioni pervenute dagli stakeholder esterni.

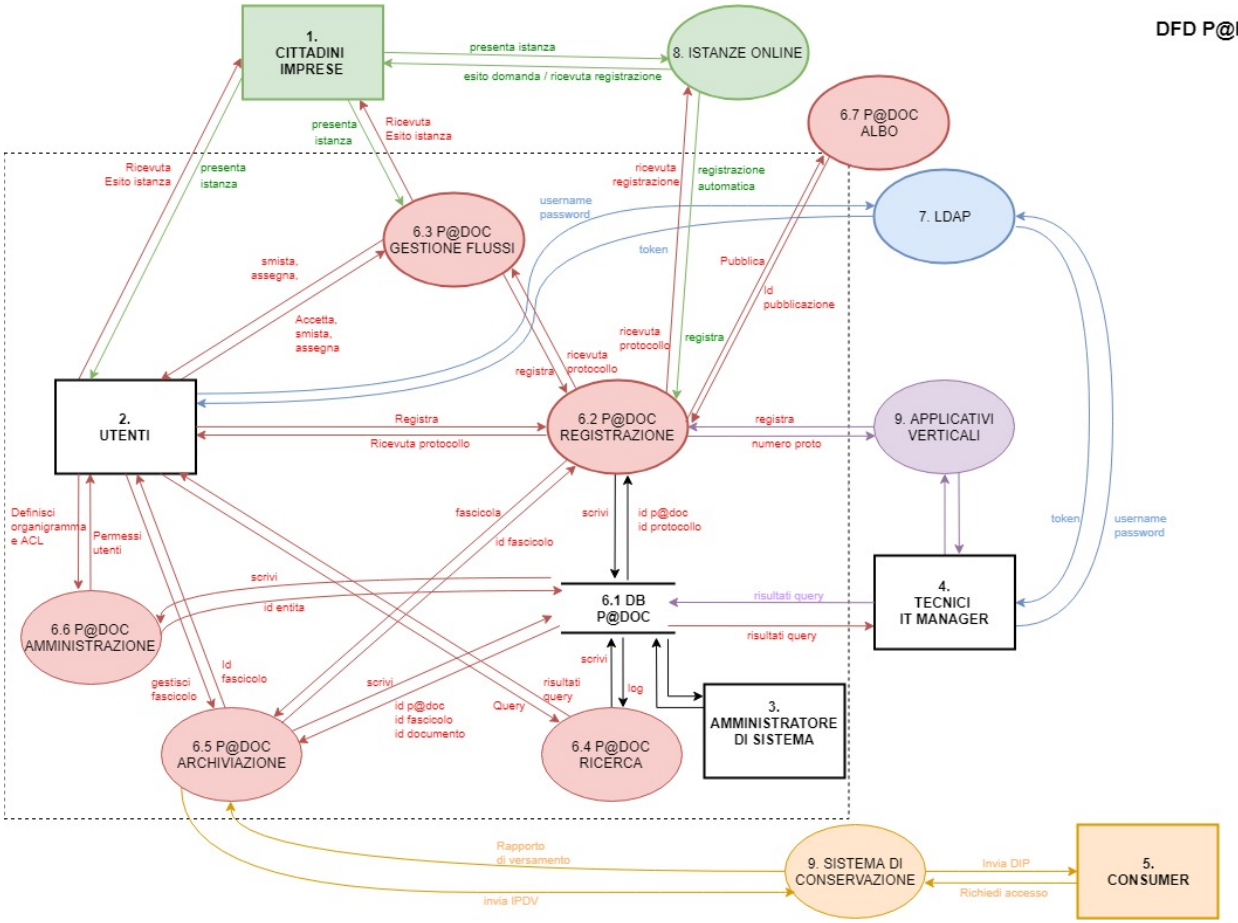
Per quanto riguarda il sistema privacy dell'ente si coinvolgono invece le figure del referente Privacy dell'organizzazione e quella del Data Protection Officer.

5. ANALISI DELLE ENTITÀ DEL SISTEMA

La metodologia utilizzata per l'analisi delle entità del sistema si basa sulle indicazioni fornite dalle "Linee guida per lo sviluppo del software sicuro nella Pubblica amministrazione" pubblicate da Agid nel dicembre 2017, con particolare riferimento alle "Linee guida per la modellazione delle minacce ed individuazione delle azioni di mitigazioni conformi ai principi del Secure/Privacy by design".
Il citato documento suggerisce diverse tecniche di modellazione e individuazione delle minacce finalizzate alla privacy by design e nell'ambito del sistema p@doc si è scelto di utilizzare, per quanto riguarda la sola parte di analisi del sistema, la metodologia LINDUNN *a privacy threat analysis framework.* LINDUNN è un nome mnemonico che tratta le violazione delle seguenti proprietà sulla privacy:

- Collegabilità (Linkability);
- Identificabilità (Identifiability);
- Non ripudio (Non Repudiation);
- Rilevabilità (Detectability);
- Divulgazione di informazioni (Disclosure of information);
- Inconsapevolezza sul contenuto (Content Unawareness);
- Inaderenza alla politica sul consenso (Policy and consent Non-compliance).

Di questa metodologia sarà utilizzata esclusivamente la parte relativa all'analisi nella quale si suggerisce la rappresentazione del sistema attraverso un diagramma di flusso dei dati (DFD-Data flow diagram) che Identifica le entità (utenti interni ed esterni al sistema), dei processi (moduli e applicativi interni ed esterni al sistema), dei database e dei flussi di dati.
Per la valutazione di impatto ed il piano di trattamento del rischio si farà invece riferimento allo standard ISO/IEC 29134:2017 - Information technology – Security techniques – Guidelines for privacy impact assessment, e nello specifico sarà utilizzato lo strumento fornito dall'Autorità Garante per la protezione dei dati personali PIA Assessment (sviluppato dal CNIL – Autorità garante francese). La valutazione avrà come oggetto i processi identificati nel diagramma di flusso.



6. LA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI – DATA PROTECTION IMPACT ASSESSMENT (DPIA)

La valutazione di impatto è uno strumento previsto dall'articolo 35 del Regolamento. Essendo p@doc un applicativo trasversale utilizzato da tutta l'organizzazione, si ritiene fondamentale eseguire una dettagliata analisi finalizzata alla definizione dei controlli e delle azioni da implementare per la conformità privacy. In questo caso particolare si esegue una valutazione di impatto in quanto il trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche ed in particolare sussiste un trattamento, su larga scala, di categorie particolari di dati personali di cui all'art. 9 e 10 del Regolamento. Il concetto di trattamento su larga scala viene definito dalle linee guida rilasciate dal WP 29 e si lega a

- Il territorio geografico (quanto ampio è il territorio all'interno del quale effettuo il trattamento);

- il volume e la tipologia dei dati trattati;
- La percentuale di interessati sul totale di una popolazione di riferimento;
- La durata del trattamento.

L'analisi delle entità del sistema effettuata precedentemente permette di valutare l'intero sistema considerando tutte le entità descritte. Lo strumento per la redazione della DPIA è quello messo a disposizione dal Garante per la protezione dei dati personali e sviluppato dal CNIL (Autorità garante francese) e tradotto per gli stati membri e disponibile all'indirizzo https://www.cnil.fr/en/pia-software-20-available-and-growth-pia-ecosystem.

Lo standard di riferimento è la norma ISO/IEC 29134:2017 - Information technology – Security techniques – Guidelines for privacy impact assessment.

Per accedere alla documentazione prodotta si allegano i seguenti documenti:

5.1_PIA_PADOC.json per l'importazione della PIA all'interno dello strumento opensource

5.2_p@doc – PIA - Privacy Impact Assessment.pdf per consultare la PIA in formato pdf.

7. ULTERIORI ANALISI FUNZIONALI ALLA CONFORMITÀ DEL SISTEMA

Le analisi che seguono si pongono come ulteriore strumento di controllo ed implementazione dei requisiti per la protezione dei dati personali.

7.1. DATABASE P@DOC

Questa analisi ha la finalità di identificare, all'interno del database postgreSQL del sistema di protocollo, le tabelle che contengono dati personali o che sono di supporto alla gestione della tutela del dato personale. Si allega il file 7.1_gestione tabelle riservatezza p@doc all'interno del quale è possibile identificare i dati personali trattati in ogni tabella e gli interessati (sia stakeholder interni che esterni).

Dall'analisi emerge la necessità di tutelare i dati personali non solo degli stakeholder esterni (cittadini, privati, imprese, etc) ma anche degli utenti all'interno del sistema.

7.2. IMPLEMENTAZIONE DELLA NORMA

A partire dalla Legge 7 agosto 1990 n. 241 - *Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi* fino al recente Regolamento UE 679/2016 – *General data protection regulation,* la norma nazionale ed internazionale ha dettato regole precise per la gestione delle informazioni valutando e definendo l'equilibrio tra la riservatezza e disponibilità dell'informazione.

Per ogni norma nazionale di riferimento nell'ambito della gestione documentale e della tenuta degli archivi, sono stati identificati gli articoli che definiscono la riservatezza e l'accessibilità delle informazioni. Ad ogni disposizione identificata si viene associato un ambito di applicazione così suddiviso:

- Tutela dell'interesse privato: la disposizione fa riferimento alla tutela degli interessati, dei loro dati e dei loro diritti di accesso.
- Tutela dell'interesse pubblico: la disposizione fa riferimento alla tutela delle informazioni dell'organizzazione.
- Conformità del sistema: la disposizione fa riferimento alla conformità del sistema di protocollo informatico e di gestione documentale p@doc
- Definizione delle politiche di accesso: la disposizione fa riferimento all'esercizio del diritto di accesso e conseguentemente alla definizione di tempi e disponibilità dell'informazione.

L'analisi si completa con la generazione di controlli che vanno ad impattare sia sul sistema stesso che sulle politiche di gestione documentale. In particolare, i controlli derivanti sono:

- DEFINIZIONE E IMPLEMENTAZIONE DI UNA CLASSIFICAZIONE DELLA RISERVATEZZA
- GARANTIRE L'ESERCIZIO DEI DIRITTI DELL'INTERESSATO
- IMPLEMENTAZIONE SISTEMA DI PSEUDONIMIZZAZIONE O ANONIMIZZAZIONE
- INFORMATIVA AI DIPENDENTI
- REDAZIONE E AGGIORNAMENTO DEL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO
- AGGIORNAMENTO DEL REGOLAMENTO SULL'ACCESSO
- REDAZIONE E IMPLEMENTAZIONE DEL REGOLAMENTO PRIVACY DELL'ORGANIZZAZIONE
- REVISIONE E AUDIT DEL SISTEMA DI GESTIONE DOCUMENTALE

8. CONCLUSIONI

Le analisi e le valutazioni effettuate restituiscono un piano di trattamento del sistema che definisce azioni volte al miglioramento o all'implementazione di politiche organizzative e degli strumenti tecnologici. Le seguenti azioni vanno viste all'interno dell'organizzazione e va valutata la fattibilità circa l'applicazione de

8.1. DEFINIZIONE E IMPLEMENTAZIONE DI UNA CLASSIFICAZIONE DELLA RISERVATEZZA

Obiettivo: Definire una classificazione della riservatezza

Azione: Definire una classificazione della riservatezza tenendo conto sia della tutela dei dati personali (privacy) che quelli di pubblico interesse (riservatezza dell'organizzazione)

Output: Implementazione all'interno del sistema p@doc della nuova classificazione della riservatezza. La classificazione dovrà essere implementata nei processi 6.2 P@doc Registrazione e 6.5 P@doc Archiviazione (vedi capitolo 5) ossia nella registrazione delle unità documentarie e nella loro fascicolazione.

Una proposta di classificazione per la protezione dei dati personali può essere:

ID	Nome Campo	Descrizione
1	Dati personali	dati Anagrafici (Nome, Cognome, Indirizzo, Data di nascita/morte, cittadinanza, stato civile, professione Codice fiscale Identificativi di documenti d'identità (numero patente/CI/Passaporto) Dati di contatto (e.mail, contatti telefonici) Coordinate bancarie Dati economico-finanziari, reddituali Numero di targa del veicolo Credenziali di autenticazione Codice identificazione personale (CID) numero di carta di credito Transazioni Carta di credito Indirizzo IP (quando collegato ad altri dati)
2	Dati personali particolari - 1	Relativi a origine razziale od etnica, convinzioni religiose, filosofiche, opinioni politiche, appartenenza sindacale. Rientrano in questa categoria anche i dati genetici e i dati biometrici (impronta digitale, scansione iride, immagine identificativa).

3	Dati personali particolari - 2	Dati relativi alla salute, alla vita o all'orientamento sessuale, rapporti riservati riservati di tipo familiare, l'appartenenza a categorie protette
4	Dati giudiziari	dati cosidetti giudiziari, cioè quelli che possono rilevare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato

I dati personali particolari vengono divisi in due diverse categorie per garantire la limitazione alla consultabilità per quarant'anni nel caso di dati personali particolari - 1, e settanta nel caso dei dati personali particolari – 2.

Una proposta di classificazione per la protezione dei dati di pubblico interesse può essere:

ID	Nome Campo	Descrizione
1	Dati confidenziali	- libertà e segretezza della corrispondenza, interessi economici e - commerciali di una persona fisica o giuridica, ivi compresa la proprietà intellettuale, il diritto d'autore e i segreti commerciali (E.G. risposte tecniche e offerte economiche da parte dei fornitori) - Dati che possono essere divulgati ad un elenco limitato e predefinito di personale interno alla PA e ad altre entità (es. cittadini, imprese, altre PA) che hanno sottoscritto un contratto per la fornitura di un servizio o un Accordo di non divulgazione (NDA – Non Disclusure Agreement). Esempi di dati sono: Codice applicativo, valutazioni delle performance dei servizi erogati, accordi strategici, log di accesso, contratti di servizio, dati di profilazione, elementi segreti per l'accesso ai sistemi informatici (PIN,Password), rapporti di verifiche ispettive interne, Dati relativi a gare (dati relativi a budget, report di analisi dei rischi).
2	Dati a uso interno	Dati che possono essere divulgati a tutto il personale interno alla PA e alle terze parti che hanno in corso un rapporto di lavoro o fornitura o hanno sottoscritto un accordo di non divulgazione (NDA). Esempi di dati sono: policy e procedure e processi della PA, materiali di formazione.
3	Dati riservati	Per quanto riguarda la tutela dell'interesse pubblico possiamo definire le seguenti classi: segreto di stato sicurezza pubblica e ordine pubblico (strutture, mezzi, dotazioni, personale e azioni strumentali) sicurezza nazionale difesa e questioni militari relazioni internazionali politica e stabilità finanziaria ed economica dello Stato indagine su reati e loro perseguimento

		svolgimento delle attività ispettive declaratoria di riservatezza (art. 125 del Codice dei beni culturali)
4	Dati gestione del personale	Dati relativi alla gestione del rapporto di lavoro del personale dell'organizzazione (provvedimenti disciplinari, medicina preventiva, sequestro stipendio)

8.2. GARANZIA DELL'ESERCIZIO DEI DIRITTI DELL'INTERESSATO

Obiettivo: Integrazione nel sistema p@doc di una corretta gestione dell'esercizio dei diritti degli interessati

Azione: La documentazione relativa all'esercizio dei diritti degli interessati (art. 15-22 del GDPR) deve essere allegata/associata ai documenti o ai fascicoli relativi alla persona (interessato). I diritti esercitati possono influenzare l'accessibilità alla documentazione (blocco dei dati che non siano di rilevante tutela dell'interesse pubblico). [art. 126 comma 1-2, D.LGS 42/2004 – Codice dei beni culturali e del paesaggio]

Output: Documento di analisi per l'implementazione a sistema dell'esercizio dei diritti dell'interessato

8.3. IMPLEMENTAZIONE SISTEMA DI PSEUDONIMIZZAZIONE O ANONIMIZZAZIONE - PARTIZIONAMENTO

Obiettivo: Definire delle modalità operative o dei sistemi automatici per rendere i dati personali intellegibili, oscurabili o per sottrarli temporaneamente.

Azione: Nell'ambito dell'accessibilità, della trasparenza e degli open data diviene fondamentale creare degli automatismi o descrivere delle modalità operative per adottare misure di sicurezza adeguate alla tutela dei dati personali. Nello specifico potrebbe essere utile prevedere un partizionamento dei dati descritti all'interno del campo "oggetto" dell'unità documentaria registrata, separando l'azione (istanza, segnalazione, dichiarazione) dall'interessato (cittadino, utente, libero professionista, etc..) rendendo logicamente separati i dati.

Output: Analisi di fattibilità partizionamento dati del campo oggetto.

8.4. INFORMATIVA AI DIPENDENTI

Obiettivo: Aggiornamento dell'Informativa sul trattamento dei dati dei dipendenti

Azione: Con l'entrata in vigore del GDPR deve essere rivista l'informativa sul trattamento dei dati personali dei dipendenti. Questi sono attualmente gestiti, archiviati e conservati all'interno di

appositi fascicoli all'interno del sistema p@doc, all'interno del quale sono registrate anche le operazioni effettuate dai vari utenti (dipendenti) del sistema.

Output: Nuova informativa ai dipendenti

8.5. REDAZIONE E AGGIORNAMENTO DEL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Obiettivo: Implementazione / aggiornamento del registro delle attività di trattamento

Azione: L'obbligo di tenuta del registro delle attività di trattamento è stato rispettato dal Comune di Padova. Data la natura dei dati trattati è fondamentale eseguire una verifica e aggiornamento periodici (semestrale) dei contenuti del registro.

Output: Registro delle attività di trattamento

8.6. AGGIORNAMENTO DEL REGOLAMENTO SULL'ACCESSO (anche per fini storici)

Obiettivo: Implementazione / aggiornamento del regolamento sull'accesso

Azione: Verificare che il regolamento sull'accesso adottato dall'organizzazione riporti i limiti alla consultazione e le eventuali modalità per di accesso per i documenti di carattere riservato (autorizzazione del Ministero dell'interno). Verificare che il regolamento riporti i tempi di limitazione all'accesso dei documenti contenenti categorie particolari di dati personali (art. 9 e 10).

Output: Regolamento sull'accesso

8.7. REDAZIONE E IMPLEMENTAZIONE DEL REGOLAMENTO PRIVACY E SICUREZZA

Obiettivo: redazione e adozione di un regolamento privacy e sicurezza

Azione: l'organizzazione dovrebbe adottare un regolamento privacy che descriva i ruoli coinvolti nel trattamento dei dati personali, i doveri del titolare del trattamento e dei responsabili del trattamento, le modalità di aggiornamento del registro delle attività di trattamento, le misure di sicurezza adottate dall'organizzazione , le modalità di utilizzo degli strumenti informatici, di gestione delle postazioni ed il controllo degli accessi logici (autenticazione, password, etc), le politiche di back-up e di business continuity, le modalità di gestione degli incidenti di sicurezza e delle violazioni dei dati personali con i relativi piani di reazione e caratterizzazione delle violazioni.

Output: Regolamento privacy e sicurezza

8.8. REVISIONE E AUDIT DEL SISTEMA DI GESTIONE DOCUMENTALE

Obiettivo: Adottare un sistema di audit per il sistema di gestione documentale p@doc

Azione: implementare delle procedure di audit del sistema con l'utilizzo di tool per l'analisi del rischio e conseguenti piani di trattamento

Output: Analisi di rischio e audit del sistema.

8.9. VIGILANZA SULLA PROTEZIONE DEI DATI PERSONALI

Obiettivo: Monitoraggio continuo sui trattamenti effettuati dal titolare

Azione: implementare una procedura di verifica attraverso la codifica dei procedimenti amministrativi, la codifica all'interno del protocollo (oggettario) e il registro delle attività di trattamento. Questa implementazione permette di rilevare se i trattamenti sono fatti in conformità alle regole definite dall'organizzazione, se le informazioni sono state raccolte correttamente e la quantificazione dei trattamenti censiti.

Output: Strumento di monitoraggio sui trattamenti all'interno di p@doc (Pentaho Data Integration – Kettle)