Capgemini EEA Human Resources Data Privacy *(Policy)*

Stato documento: Approvato

Riferimento: QMS/SI/P/18/73
Versione: 1.0
Data: 8 maggio 2018

CREAZIONE DOCUMENTO

DATA	AUTORE
Maggio 2018	M. Salza

REVISIONE E APPROVAZIONE

FUNZIONE	NOME	DATA	FIRMA
HR	A. Miata		
DPO	G. Branca		
BRM, CCM & Quality	A. Di Pasquale		

DISTRIBUZIONE

ENTE	FUNZIONE
Capgemini Italia e sue consociate	Tutto il personale

AGGIORNAMENTI

VER.	DATA	AUTORE	MODIFICHE

ABBREVIAZIONI

ABBREVIAZIONE	SIGNIFICATO
EEA	European Economic Area
BCR	Binding Corporate Rules
GDPR	General Data Protection Regulation Regolamento Generale sulla Protezione dei Dati
RPD	Responsabile della Protezione dei Dati
DPO	Data Protection Officer
C&B	Compensation & Benefit
DPA	Data Protection Authority

DOCUMENTI APPLICABILI E DI RIFERIMENTO

IDENTIFICATIVO	NOME	RIF.
---	Group Binding Corporate Rules	
QMS/GM/M/04/10	Codice Etico	
---	Global/Capgemini Data Privacy Policy	
	Cybersecurity Organization	
	Global Security Incident Response	
---	CySIP Incident Management Process	
QMS/DE/P/10/46	Procedura Gestione Incident	
---	Richiesta Esercizio dei Diritti degli Interessati	
---	GDPR – General Data Protection Regulation	
---	Capgemini Group – Information Security Policy	

INDICE

1. INTRODUZIONE

1.1 Conformemente a quanto stabilito dalle sue Binding Corporate Rules (Norme vincolanti d'impresa), Capgemini rispetta la privacy degli individui e soddisfa i requisiti previsti dalle normative in materia di tutela di Dati Personali, vigenti nei paesi in cui le società del Gruppo Capgemini svolgono attività. Inoltre, Capgemini tratta i Dati Personali in modo responsabile e limita la raccolta e l'accesso agli stessi al fine di proteggere la privacy delle persone, incluse quelle che lavorano per Capgemini.

1.2 In questo contesto Capgemini ha adottato la presente Policy (di seguito la "**Politica**") per istituire e mantenere alti standard globali di protezione riguardo ai Dati Personali dei propri Dipendenti che operano nell'ambito della EEA (European Economic Area).

1.3 In termini generali, la presente Politica descrive i Dati Personali che vengono trattati da Capgemini nell'ambito del rapporto di lavoro, il modo in cui vengono gestiti e quali sono i diritti dei Dipendenti in questo contesto. La presente Politica stabilisce inoltre, le regole che i Dipendenti di Capgemini devono rispettare quando trattano Dati Personali.

1.4 La presente Politica è in linea con le Binding Corporate Rules di Capgemini (BCR for Controller e BCR for Processor) e con il **Regolamento UE relativo alla tutela delle persone fisiche con riguardo al trattamento dei Dati Personali e alla libera circolazione di tali dati ("Regolamento Generale sulla Protezione dei Dati" o "GDPR")** ed è stata concepita per consentire alle società del Gruppo Capgemini che operano nella EEA di adempiere ai propri obblighi in qualità di "Controller" ai sensi del GDPR.

1.5 Nella presente Politica, i termini sotto riportati assumono la seguente accezione:

"**BCR**": Binding Corporate Rules (Norme Vincolanti d'impresa) applicabili a Capgemini sia in qualità di Titolare (Controller) che di Responsabile (Processor); le BCR sono allegate al presente documento come Appendice 1. Il testo delle BCR, è disponibile, nella sua versione più recente, all'indirizzo:

http://talent.capgemini.com/global/pages/hubs/global_functions/leg/data_privacy/

"**Capgemini**" o "**Gruppo**": l'intero Gruppo di società Capgemini controllate, direttamente o indirettamente, da Capgemini SE.

"**Società Capgemini**": una società del Gruppo Capgemini controllata direttamente o indirettamente da Capgemini SE.

"**Titolare del trattamento dei dati**" o "**Titolare del trattamento**": la Società Capgemini che stabilisce le finalità e i mezzi del trattamento dei Dati Personali del Dipendente.

"**Responsabile del trattamento dei dati**" o "**Responsabile del trattamento**": la società che provvede al trattamento dei Dati Personali per conto del Titolare del trattamento dei dati.

"**RPD**" o "**DPO**": Responsabile della Protezione dei Dati o Data Protection Officer.

"**Interessato"**: il Dipendente a cui si riferiscono i Dati Personali.

"**Dipendente/i**": un Dipendente attuale, passato o futuro di una Società del Gruppo Capgemini, nonché i lavoratori in regime di somministrazione.

"**EEA**: European Economic Area.

"**Dati Personali**": secondo quanto stabilito nell'articolo 4 del GDPR, 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.

2. A QUALI DATI PERSONALI SI APPLICA QUESTA POLITICA?

2.1 La presente Politica si applica ai Dati Personali dei Dipendenti (secondo la definizione sopra descritta) nonché dei candidati presso un Titolare del trattamento dei dati stabilito nella EEA, nella misura in cui i Dati Personali descritti nella sezione 4 vengono ricevuti da Capgemini.

2.2 La presente Politica non si applica ai Dati Personali di dipendenti e candidati presso Società del Gruppo Capgemini stabilite fuori dalla EEA. Tuttavia, i Dipendenti delle società del Gruppo Capgemini stabilite fuori dalla EEA sono tenuti a rispettare le disposizioni del capitolo 16 (**Responsabilità dei Dipendenti di Capgemini**) della presente Politica.

3. SU CHI RICADONO LE RESPONSABILITÀ AI SENSI DI QUESTA POLITICA?

3.1 Tutti coloro che in Capgemini vengono in contatto con Dati Personali devono rispettare le BCR e il capitolo 16 della presente Politica, (**Responsabilità dei Dipendenti di Capgemini**), che descrive più dettagliatamente le modalità con cui i Dipendenti devono trattare i Dati Personali nell'ambito del proprio ruolo.

3.2 Il mancato rispetto della presente Politica può esporre Capgemini a responsabilità giuridiche e può tradursi in provvedimenti disciplinari per il Dipendente.

4. QUALI SONO I DATI PERSONALI CHE CAPGEMINI DETIENE RIGUARDO AI PROPRI DIPENDENTI?

4.1 Capgemini può detenere varie tipologie di Dati Personali, in base alla natura del rapporto con i Dipendenti interessati dalla presente Politica e purché tale trattamento sia consentito dalle leggi applicabili nel paese in cui è stabilito il Titolare del trattamento dei dati. Questo può includere, a titolo non esaustivo:

- **Dati Personali** come nome e cognome, data di nascita, genere, età, indirizzo, numeri di telefono, indirizzi e-mail, numero di figli, cittadinanza, dettagli identificativi, dettagli relativi al visto, dettagli relativi al permesso di lavoro, dettagli relativi alle persone da contattare in caso di emergenza, dettagli relativi ai familiari a carico, stato civile, beneficiari dell'assicurazione vita, foto o immagini;
- **Informazioni finanziarie** relative al compenso, ai benefit e agli accordi pensionistici, quali ad esempio dettagli relativi a stipendio, conto corrente bancario, codice fiscale, spese di viaggio, stock option e piani per l'acquisto di azioni;
- **Informazioni relative all'assunzione**, ad esempio curriculum vitae, modulo di richiesta di assunzione, appunti dei colloqui di lavoro, referenze del richiedente (se registrate), qualifiche, risultati delle prove (eventuali);
- **Informazioni amministrative sull'impiego**, ad esempio cronologia degli impieghi e della carriera, grado lavorativo, dirigenti, dettagli dei contratti di lavoro, documentazione relativa alle assenze e documentazione relativa alla sicurezza, documentazione relativa alla salute, documentazione relativa a eventuali incidenti, analisi dello sviluppo personale, dettagli della patente automobilistica e documenti relativi, documentazione relativa alle competenze, numeri di identificazione rilasciati da enti statali;
- **Informazioni sull'esperienza professionale**, ad esempio curriculum vitae professionale, qualifiche, dettagli dei progetti su cui i Dipendenti hanno lavorato, resoconto della formazione, resoconto della mobilità;
- **Dettagli relativi all'ubicazione dei Dipendenti** nella sede Capgemini nella misura in cui sono registrati dai sistemi di accesso Capgemini tramite badge;
- **Dettagli relativi ai sistemi informatici e dati di connessione** agli stessi;
- **Fotografie.**

5. RACCOLTA DELLE INFORMAZIONI PERSONALI

5.1 Gran parte dei Dati Personali trattati da Capgemini e riguardanti i Dipendenti viene fornita direttamente dai Dipendenti durante la procedura di assunzione o dopo l'inizio del lavoro.

5.2 Il conferimento di determinate tipologie di Dati Personali, ad esempio nome, cognome, data di nascita e codice fiscale, è obbligatorio per la finalizzazione dei contratti di lavoro dei Dipendenti con Capgemini nonché per la tutela degli interessi legittimi di Capgemini.

Il conferimento di altre tipologie di Dati Personali, ad esempio i dettagli delle persone da contattare in caso di emergenza, può essere facoltativo.

5.3 Durante l'attività lavorativa del Dipendente presso Capgemini possono essere raccolte, dal Dipendente stesso e/o dal Mangagement, altre tipologie di Dati Personali come ad esempio dati relativi allo sviluppo professionale, documentazione inerente le competenze acquisite nel tempo e informazioni circa i progetti per cui il Dipendente ha lavorato. Tuttavia, a volte Capgemini riceve i Dati Personali da terzi, ad esempio da agenzie di somministrazione.

5.4 Talvolta Capgemini può chiedere ai Dipendenti di fornire Dati Personali riguardanti terzi, ad esempio i dettagli relativi alle persone che Capgemini deve contattare in caso di emergenza. I Dipendenti, prima di fornire Dati Personali relativi a terzi, devono accertarsi di aver comunicato a tutte le persone in questione che Capgemini tratterà i loro Dati Personali e dovranno fornire loro tutte le informazioni del caso in merito al trattamento dei loro Dati Personali da parte di Capgemini.

6. BASE GIURIDICA PER IL TRATTAMENTO DEI DATI PERSONALI DEI DIPENDENTI DA PARTE DI CAPGEMINI

6.1 Conformemente a quanto previsto dall'articolo 6 del GDPR, Capgemini raccoglie i Dati Personali soltanto in presenza di una chiara base giuridica per il trattamento degli stessi. In relazione ai trattamenti dei Dati Personali dei Dipendenti, la base giuridica è la seguente:

- Il trattamento è necessario per adempiere alle obbligazioni del contratto di lavoro stipulato tra le parti, o per ottemperare a tutti i requisiti previsti per l'assunzione di un candidato;
- Capgemini ha un chiaro e comprensibile legittimo interesse al trattamento dei dati dei sui Dipendenti connesso alle proprie attività d'impresa e al lavoro che il Dipendente svolge per conto della stessa Capgemini; fanno eccezione i casi in cui tali interessi sono superati dagli interessi, dai diritti e dalle libertà fondamentali del Dipendente che ha diritto alla tutela dei propri dati;
- Il trattamento è necessario per soddisfare un obbligo legale a cui Capgemini è soggetta;
- Il trattamento è necessario per proteggere gli interessi vitali del Dipendente o di un'altra persona.

Generalmente, le finalità per cui Capgemini tratta i Dati Personali del Dipendente sono connesse al lavoro e potrebbero includere, a titolo non esaustivo, le seguenti:

- Assunzione, incluse la verifica delle referenze, nel rispetto della legge locale;

- Valutazione delle prestazioni e della formazione;
- Libro paga e amministrazione degli altri benefit legati al rapporto di lavoro (incluse stock option e piani per l'acquisto di azioni o altri piani o benefit aziendali);
- Attività di gestione corrente, ad esempio assegnazione a progetti, promozioni, attività disciplinari, gestione delle procedure di reclamo;
- Marketing dei servizi professionali di consulenti presso potenziali clienti di Capgemini (ad esempio fornendo i dettagli delle esperienze maturate su progetti precedenti);
- Amministrazione dei benefit correnti, inclusi il programma pensionistico del personale, il piano assicurazioni vita, il piano assicurazione sanitaria privata di Capgemini;
- Analisi del Dipendente, per esempio confrontando il successo di vari programmi di assunzione e/o fideliizzazione dei Dipendenti;
- Rispetto delle norme in materia di salute e sicurezza e degli altri obblighi legali che incombono su Capgemini in qualità di datore di lavoro;
- Se necessario, trattamento volto a consentire a Capgemini di esercitare i propri diritti legali e/o di adempiere ai propri obblighi giuridici in qualità di datore di lavoro, nella misura in cui ciò è richiesto dalla legge locale del paese in cui è stabilito il Titolare del trattamento dei dati;
- Gestione delle risorse umane, gestione della carriera e mobilità;
- Comunicazione interna ed esterna;
- Disaster Recovery Plan e gestione delle crisi;
- Gestione delle risorse aziendali;
- Audit e statistiche.

6.2 Se richiesto dal GDPR e dalle leggi locali del paese in cui è stabilito il Titolare del trattamento dei dati, Capgemini realizzerà una valutazione dell'impatto della protezione dei dati come richiesto ai sensi degli articoli 35 e 36 del GDPR e dalle leggi locali.

7. PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI PERSONALI DEI DIPENDENTI

7.1 Capgemini conserverà, utilizzerà e tratterà comunque i Dati Personali in maniera compatibile con la/le finalità per cui sono stati originariamente raccolti a meno che i Dipendenti non siano informati che i loro dati saranno trattati per una finalità diversa o a meno che l'uso per una finalità diversa sia consentito dalla legge locale.

7.2 Capgemini conserverà i Dati Personali per il tempo necessario al perseguimento della/delle finalità per cui sono stati raccolti. Dopodiché, i dati saranno cancellati o mantenuti in forma anonima, secondo quanto previsto dai requisiti della legge locale.

7.3 Capgemini adotterà le misure necessarie per garantire che i Dati Personali vengano mantenuti completi, accurati e aggiornati, tenuto conto della finalità per cui essi vengono trattati. Capgemini fa inoltre affidamento sui Dipendenti perché facciano in modo che tutti i Dati Personali

da essi comunicati siano corretti, accurati e aggiornati. I Dipendenti devono tenere aggiornata Capgemini su eventuali modifiche dei Dati Personali da essi forniti.

7.4 Più in generale, il trattamento dei Dati Personali da parte di Capgemini dovrà essere svolto in osservanza di quanto previsto dalle BCR e dai principi relativi al trattamento dei Dati Personali menzionati nell'articolo 5 del GDPR oltre che dai principi di privacy by design e privacy by default, secondo quanto previsto dall'articolo 25 del GDPR.

8. CATEGORIE PARTICOLARI DI DATI PERSONALI

8.1 In linea di massima, Capgemini non raccoglierà né tratterà Dati Personali così come definiti dall'articolo 9 del GDPR (dati sensibili) o informazioni relative alle condanne penali e ai reati (dati giudiziari).

8.2 In via eccezionale e se consentito ai sensi dell'articolo 9.2 o dell'articolo 10 del GDPR o dalle leggi del paese in cui è stabilito il Titolare del trattamento dei dati, Capgemini potrà raccogliere e trattare i suddetti Dati Personali.

9. PROFILAZIONE E DECISIONI AUTOMATIZZATE

9.1 Capgemini potrà trattare i Dati Personali dei Dipendenti nel contesto delle attività di profilazione così come definite nell'articolo 4 del GDPR. Il suddetto trattamento dovrà essere effettuato per le finalità elencate nell'articolo 6 della presente Politica e in conformità ai diritti degli Interessati, come definiti ai sensi dell'articolo 15 della presente Politica (**"Diritti degli Interessati"**).

9.2 In linea di massima, Capgemini non adotta alcuna decisione individuale che produca effetti giuridici o che incida in maniera significativa su un Interessato basandosi unicamente sul trattamento automatizzato, in conformità a quanto previsto dall'articolo 22 del GDPR.

10. CONTROLLI (VETTING) SUL PERSONALE

10.1 Nella misura consentita dalle leggi locali del paese in cui è stabilito il Titolare del trattamento dei dati e di volta in volta in relazione ad una particolare operazione commerciale, a Capgemini viene chiesto dai propri clienti di esaminare informazioni specifiche riguardo ai Dipendenti di Capgemini, per esempio di eseguire una verifica della solvibilità o un controllo della sicurezza per garantire che tutti i Dipendenti siano idonei per lavorare sugli argomenti sensibili

del cliente in questione; questa procedura viene definita "vetting". In linea di massima, quando a Capgemini viene richiesta l'esecuzione di una procedura di vetting, questa deve essere eseguita in conformità con le leggi applicabili. Nel caso in cui venga eseguita una procedura di vetting che li riguarda, i Dipendenti verranno informati in via preventiva.

11. CHI HA ACCESSO AI DATI PERSONALI ALL'INTERNO DI CAPGEMINI

11.1 I Dati Personali non sono a disposizione di chiunque all'interno di Capgemini. L'accesso ai Dati Personali è consentito soltanto a chi ha una chiara "necessità di conoscerli" (principio del "need to know") per motivi di lavoro o per motivi giuridici, come ad esempio, nel caso di ruoli manageriali o di appartenenza al Dipartimento risorse umane di Capgemini.

11.2 Inoltre, il grado di accesso ai dati di una persona fisica dipenderà dalla natura delle informazioni in questione. Per esempio, il nome e il cognome, la fotografia e i dettagli dei contatti lavorativi di un Dipendente sono disponibili attraverso l'Intranet di Capgemini per chiunque lavori in Capgemini, mentre altri Dati Personali, ad esempio i dettagli relativi al compenso del Dipendente, sono accessibili soltanto ai dirigenti di Capgemini che sono responsabili del suddetto Dipendente (ad esempio i superiori gerarchici del Dipendente e i dirigenti funzionali, che potrebbero anche essere stabiliti in altri paesi) e ai pertinenti membri del Dipartimento Risorse Umane di Capgemini. Qualora i Dipendenti presentino domanda per ricoprire un altro incarico o per essere trasferiti altrove all'interno di Capgemini, alcuni dei loro Dati Personali potrebbero anche essere messi a disposizione del dirigente che li assume o dei membri del Dipartimento Risorse Umane di Capgemini.

11.3 I Dipendenti devono tenere presente che quando esiste una "necessità di conoscere" i loro dati personali in relazione ad una determinata finalità, gli stessi dati potrebbero essere condivisi fra diverse società del Gruppo Capgemini, anche in diversi paesi.

12. CHI HA ACCESSO AI DATI PERSONALI ALL'ESTERNO DI CAPGEMINI

12.1 Capgemini non divulgherà i Dati Personali a terzi all'esterno di Capgemini a meno che non vi sia una importante motivazione aziendale o giuridica per farlo, ad esempio nei casi in cui Capgemini lo ritiene ragionevolmente necessario e quando ciò è consentito dalla legge applicabile al Titolare del trattamento dei dati. Generalmente, questi motivi sono legati al lavoro e possono includere, a titolo non esaustivo, le seguenti finalità:

- per proteggere gli interessi vitali dei Dipendenti;
- per la gestione dei sistemi informatici HR, incluso il payroll;

- per la gestione dell'attuale programma di benefici collettivi per i Dipendenti, tra cui il programma pensionistico personale, il piano assicurazioni vita, il piano assicurazione sanitaria privata del Gruppo Capgemini e gli eventuali altri benefici di volta in volta in vigore (o di un altro fornitore terzo di servizi connessi all'impiego);
- se richiesto dalla legge o da una ordinanza di tribunale, per esempio dalle autorità fiscali, dagli enti previdenziali o da altri enti statali o locali;
- per ottemperare ad una legittima richiesta di assistenza da parte della polizia o delle forze dell'ordine;
- per richiedere consulenza agli avvocati esterni di Capgemini e ad altri consulenti professionali;
- per gestire le relazioni con:
    - eventuali terze parti coinvolte in una controversia legale con Capgemini (inclusi gli avvocati delle suddette terze parti);
    - potenziali acquirenti e venditori nell'ambito di operazioni di cessione o acquisizione da parte di Capgemini di una società o dei relativi asset;
    - altre parti terze che forniscono a Capgemini servizi legati all'attività aziendale, ad esempio agenzie di viaggio, società di transito aeroportuale, fornitori di carte di credito, eccetera;
    - agenzie di somministrazione del personale;
- per fornire a parti terze (ad esempio potenziali clienti e fornitori) un mezzo per contattare Capgemini nel corso della normale attività di business, ad esempio fornendo i "dettagli di contatto" abitualmente riportati su un biglietto da visita;
- per intrattenere rapporti con clienti attuali e potenziali che richiedono dettagli relativi all'idoneità del Dipendente per un particolare progetto, ad esempio i dettagli relativi alle qualifiche e all'esperienza.

12.2 In ciascuno degli esempi che precedono, le tipologie dei Dati Personali rese note sono strettamente limitate a quelle necessarie e ragionevoli per il raggiungimento di uno degli obiettivi sopra elencati.

12.3 Talvolta, Capgemini può appaltare all'esterno determinati processi aziendali, ad esempio la manutenzione dei suoi sistemi informatici per le Risorse Umane, a terzi fornitori di servizi che agiscono per conto di Capgemini. Le suddette terze parti possono tecnicamente avere accesso ai Dati Personali nel corso dell'erogazione dei servizi ad essi appaltati, ma sono tenuti per contratto a trattare i Dati Personali soltanto in base alle istruzioni di Capgemini e in conformità con la presente Politica. Inoltre, Capgemini esegue preliminarmente un processo di due diligence sulle parti terze in merito al trattamento dei Dati Personali, che comprende la verifica dei requisiti di riservatezza dei dati personali trattati, di conformità alle istruzioni impartite da Capgemini e di adozione di misure tecniche ed organizzative appropriate per garantire che non venga eseguito alcun trattamento non autorizzato o illegittimo, e non avvengano accidentalmente eventi di perdita, distruzione o danneggiamento dei Dati Personali.Inoltre, con la parte terza in questione vengono sottoscritti opportuni contratti, come previsto dall'articolo 28 del GDPR.

13. TRASFERIMENTO INTERNAZIONALE DEI DATI PERSONALI

13.1 il Business di Capgemini e i suoi clienti sono sempre più globalizzati e fanno affidamento sulla comunicazione globale e sui sistemi informativi globali per funzionare con efficacia e in maniera competitiva. Questo significa che, potenzialmente, i Dati Personali potrebbero essere conservati, trattati e consultati (in ottemperanza al principio del "need to know") da Capgemini in qualunque parte del mondo nelle sue varie sedi.

13.2 Tutte le Società del Gruppo Capgemini in tutto il mondo sottoscriveranno gli accordi di adesione alle BCR, in modo da essere vincolate alle stesse; le BCR sono concepite, infatti, per regolamentare il trasferimento dei Dati Personali all'interno del Gruppo (inclusi i paesi situati fuori dalla EEA) in modo da consentire una libera e sicura circolazione dei Dati Personali fra le Società del Gruppo Capgemini.

13.3 Inoltre, in caso di trasferimento internazionale dei Dati Personali a terzi al di fuori della EEA, Capgemini sottoscriverà con i suddetti terzi contratti appropriati garantendo che i dati vengano conservati e trattati in conformità alla legge applicabile.

14. SICUREZZA

14.1 Ai sensi dell'articolo 32 del GDPR, tenuto conto dello stato dell'arte, dei costi di attuazione nonchè della natura, dell'oggetto, del contesto e delle finalità del trattamento dei dati nonché dei rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, Capgemini applica e mantiene appropriate misure tecniche, fisiche e organizzative per la protezione dei Dati Personali e segue le prassi e gli standard di mercato adottando procedure e implementando sistemi concepiti per prevenire l'accesso non autorizzato ai Dati Personali ed evitare che gli stessi siano soggetti a perdita, danneggiamento o distruzione accidentale.

14.2 Tutte le Società e le Business Unit del Gruppo Capgemini hanno l'obbligo di rispettare le "Group Security baseline" minime, stabilite dal "Group Cybersecurity and Information Protection Officer" e monitorate all'interno delle Società e delle Business Unit del Gruppo Capgemini dai Security and Information Protection Officer che lavorano a stretto contatto con i RPD (DPO) quando necessario.

14.3 In base a quanto previsto dagli articoli 33 e 34 del GDPR e dalle leggi locali e tenuto conto del livello di rischio per i diritti e le libertà degli Interessati, Capgemini segnalerà le violazioni dei Dati Personali alle autorità e/o agli interessati, se dovesse venire a conoscenza del fatto che la sicurezza, la riservatezza o l'integrità dei Dati Personali sono state compromesse.

14.4 Allo stesso modo, tutti i Dipendenti sono tenuti a segnalare tutte le violazioni dei dati in conformità con il CySIP Incident Management Process.

15. DIRITTI DEGLI INTERESSATI - RECLAMI

15.1 Capgemini rispetterà i diritti degli Interessati come definiti dal capitolo III del GDPR e dalle leggi locali.

15.2 I Dipendenti hanno il diritto di ricevere informazioni relative al trattamento dei loro Dati Personali. Tali informazioni sono fornite nella presente Politica e nelle BCR nonché in specifiche informative laddove necesario.

15.3 I Dipendenti hanno diritto di accesso ai loro Dati Personali. I Dipendenti possono accedere online a gran parte dei loro Dati Personali usando varie applicazioni HR "self-service" implementate in Capgemini. Gli altri dati possono essere ottenuti presentando una richiesta di esercizio dei diritti degli Interessati. Tuttavia, il Dipendente non può avere accesso a determinate categorie di informazioni. Esse includono tipicamente i Dati Personali che vengono trattati nell'ambito dei piani definiti dal management (ad esempio la pianificazione delle promozioni), i Dati Personali riguardanti una parte terza (cioè un collega di lavoro) o i Dati Personali che vengono trattati nell'ambito di una consulenza legale. L'elenco che precede non è esaustivo.

15.4 I Dipendenti inoltre hanno diritto di rettifica, cancellazione, opposizione, portabilità e diritto alla limitazione del trattamento. L'esercizo dei suddetti diritti dipende dalla natura del trattamento, dalla necessità di proteggere informazioni riservate nonché dalla presenza di eventuali terze parti. L'elenco che precede non è esaustivo.

15.5 Per esercitare i suddetti diritti, il Dipendente deve prendere visione della "Richiesta di esercizio dei diritti degli interessati e procedura di reclamo" annessa alla presente Politica come Allegato 2 e rivolgersi al RPD (o DPO). Inoltre i Dipendenti possono inviare una richiesta di informazioni tramite e-mail al seguente indirizzo: dataprivacy.it@capgemini.com.

16. RESPONSABILITÀ DEI DIPENDENTI DI CAPGEMINI

I Dipendenti che lavorano per Capgemini hanno la responsabilità di garantire che Capgemini rispetti le leggi applicabili riguardanti la protezione dei dati, le BCR e la presente Politica.

16.1 Trattamento dei dati in conformità alla Politica

Durante la loro attività lavorativa, i Dipendenti possono avere accesso o venire in contatto con Dati Personali. A seconda del ruolo del Dipendente all'interno di Capgemini, i suddetti Dati Personali possono andare dal nome e cognome e numero di telefono di casa di una persona fisica ai Dati Personali più riservati, quali ad esempio il compenso del Dipendente o le sue coordinate bancarie. Può trattarsi anche dei Dati Personali di terzi, ad esempio Dati Personali trattati da Capgemini in qualità di Responsabile del trattamento dei dati per conto di un cliente che agisce

come Titolare del trattamento dei dati quando il Dipendente è coinvolto nell'erogazione di servizi al cliente. In questi casi il Dipendente può inoltre essere tenuto a conformarsi alle politiche del cliente applicabili al trattamento dei Dati Personali. I Dipendenti devono agire di concerto con i loro manager per comprendere le proprie responsabilità nel caso in cui le politiche del cliente siano in conflitto con la presente Politica.

Si ricorda ai Dipendenti che nell'ambito del loro contratto di lavoro, devono rispettare un obbligo di riservatezza che si applica a tutte le informazioni che essi ricevono o a cui hanno accesso in occasione delle loro attività lavorative. Il suddetto obbligo di riservatezza si applica ai Dati Personali, che il Dipendente deve trattare con discrezione e in ottemperanza alla presente Politica e alle BCR.

16.2 Sicurezza

In aggiunta agli obblighi generali di riservatezza e alle altre politiche e procedure di sicurezza interna logiche e fisiche di Capgemini, i Dipendenti devono in particolare:

- Evitare di lasciare incustoditi in luoghi accessibili a persone non autorizzate "supporti di memorizzazione dei dati" come documenti cartacei, CD-ROM, fogli stampati e altri dispositivi contenenti Dati Personali;
- Evitare di lasciare incustoditi in spazi aperti attrezzature periferiche come stampanti, PC e laptop;
- Mantenere riservati nome utente e password;
- Le regole sopra indicate si applicano anche all'uso dei dispositivi mobili personali utilizzati per accedere ai Dati Personali trasferiti dai server di Capgemini;
- Seguire le misure di tutela obbligatorie allegate al presente documento come appendice.

16.3 Richieste di Parti terze

Nel caso in cui al Dipendente venga chiesto di fornire Dati Personali riguardanti una persona fisica a chiunque all'esterno di Capgemini, il Dipendente dovrà rifiutarsi a meno che non si tratti di una persona autorizzata del Dipartimento Risorse Umane, anche se è convinto che la richiesta provenga dalla polizia o da un organismo governativo. In tali circostanze, i Dipendenti devono sottoporre la richiesta all'attenzione del management locale, il più rapidamente possibile.

16.4 Sensibilizzazione e formazione

I Manager devono garantire che i Dipendenti dei quali essi sono responsabili abbiano ricevuto una copia della presente Politica e, se opportuno, abbiano accettato quanto previsto dalla stessa o da una Politica equivalente nei paesi non appartenenti alla EEA. Inoltre, il Dipendente ha l'obbligo di seguire il corso obbligatorio in e-learning sulla sicurezza informatica e la protezione delle informazioni all'atto dell'assunzione nel Gruppo, nonché tutti i successivi eventi di formazione obbligatori in materia di Riservatezza dei Dati e Sicurezza.

16.5 Misure disciplinari

La mancata osservanza della presente Politica può esporre i Dipendenti e/o Capgemini a risarcimenti in sede civile, sanzioni pecuniarie di natura penale e altre penalità. Di conseguenza,

tutti i Dipendenti devono rispettare la presente Politica; qualsiasi violazione della stessa sarà seriamente valutata e potrebbe comportare provvedimenti disciplinari appropriati.

16.6 Segnalazioni

I Dipendenti devono segnalare eventuali dubbi in merito a possibili comportamenti non conformi, infrazioni e violazioni della presente Politica scrivendo a dataprivacy.it@capgemini.com.

17. AUDIT

17.1 Il rispetto della presente Politica e delle BCR in ogni country in cui si effettuano trattamenti di Dati Personali è soggetto all'audit interno da parte di Capgemini.

18. LEGGE APPLICABILE E FORO COMPETENTE

18.1 La presente Politica verrà interpretata in conformità alle leggi del paese di cui è stabilito il Titolare del trattamento dei dati.

18.2 Qualsiasi conflitto tra la presente Politica e una prescrizione legale vincolante in un'altra giurisdizione che impedisca o ostacoli il rispetto della presente Politica deve essere sottoposto all'attenzione del management locale al più presto possibile e in ogni caso prima di qualsiasi divulgazione dei Dati Personali a terzi.

19. IDENTITÀ DEL TITOLARE DEL TRATTAMENTO DEI DATI

19.1 Il Titolare del trattamento dei dati ai sensi della presente Politica è Capgemini Italia S.p.A., con sede legale in Roma, Via di Torre Spaccata, 140, nonché Capgemini BS S.r.l., con sede legale in Marcon (VE), Centro Direzionale Valecenter, Via E. Mattei 1/C.

19.2 Il RPD (o DPO) è ***Gaetano Branca*****.**

TRATTAMENTO DI DATI PERSONALI – MISURE DI TUTELA OBBLIGATORIE

1. REGOLE GENERALI IN CASO DI TRATTAMENTO DI DATI PERSONALI

1. Impara a identificare i dati personali. I Dati Personali comprendono qualsiasi informazione che consente l'identificazione diretta (es. il nome) o indiretta di un individuo;

2. Valuta sempre se non puoi raggiungere un obiettivo prefissato senza ricorrere al trattamento di dati personali;

3. Se devi effettuare un trattamento di dati personali, valuta la possibilità di criptare o anonimizzare i set di dati personali che possono identificare un individuo, salvo il caso in cui ciò non sia strettamente necessario;

4. Nel caso in cui debba fornire accesso a dati personali, limita il numero di persone che possono accedervi ai soli soggetti che ne hanno strettamente necessità per motivazioni di business, o legate a tematiche HR o di carattere legale;

5. Sii particolarmente attento in caso di trasmissioni di dati all'estero e chiedi consiglio agli enti preposti se sono presenti dati identificabili.

2. REGOLE SPECIFICHE PER I DATI IN AMBITO HR

1. Considera che in base alle leggi applicabili riguardanti la privacy e la sicurezza in alcuni paesi, i dati relativi al contesto HR sono considerati sensibili e richiedono attenzioni ulteriori legate al fatto che divulgazioni non autorizzate di tali dati potrebbero potenzialmente causare danni all'individuo;

2. Se hai necessità di condividere dati personali, per ottenere le appropriate autorizzazioni da parte del management, assicurati che i file contenenti i dati siano protetti da password;

3. I file possono essere condivisi solo nelle seguenti modalità:

- Mediante un accesso controllato su team room o su ambiente Sharepoint, a cui possono avere accesso i soli soggetti autorizzati (soluzione preferenziale); oppure
- Via email, con la password non trasmessa nella stessa mail;

4. Nel caso in cui debba sottoporre "non-VP pay files" all'approvazione del Gruppo, non inviare dati personali di dipendenti – il Gruppo richiede solo il foglio di riepilogo al fine di rivedere/ approvare la tua proposta;

5. Qualsiasi output prodotto come parte dei nostri processi di Compensation & Benefit (C&B) viene considerato una Company Confidential Information.

3. REGOLE GENERALI DI SICUREZZA

1. Controlla attentamente tutti i destinatari delle mail prima di inoltrarle – le feature di autocorrect e autosuggest possono essere utili, ma senza la dovuta attenzione è possibile che vengano referenziati destinatari esterni o destinatari interni non corretti.

2. Memorizza i dati personali sul tuo laptop o pc soltanto per quanto è necessario per completare il tuo lavoro e poi provvedi alla loro cancellazione. Raccomandiamo di controllare al più presto se sono presenti dati personali sul tuo PC originati da precedenti memorizzazioni e di provvedere alla loro cancellazione.

3. Segue tutte le regole interne riguardanti password, il blocco del laptop quando sei lontano dallo stesso, l'importanza di non visualizzare o lavorare su dati personali in posti non sicuri, es. durante viaggi.

4. Nel caso in cui si verifichi una violazione di dati personali o tu abbia il sospetto che possa essersi verificata, (es. a causa di un errore umano, a seguito della perdita di apparecchiature o dati, a seguito di divulgazioni di file contenenti password) o nel caso in cui il tuo PC sia stato compromesso, devi immediatamente avvertire il tuo manager di linea ed il tuo dipartimento di Data Protection/Legale di riferimento.

Per ulteriore supporto contatta il Data Protection Officer:

https://talent.capgemini.com/it/pages/funzioni_di_supporto/Facilities__Security/

CAPGEMINI BINDING CORPORATE RULES

Ultima revisione: maggio 2017

Si prega di consultare la pagina Talent > Data Privacy per reperire la versione più recente delle Public BCRs.

INTRODUZIONE

Tra le principali aziende mondiali di fornitura di servizi di consulenza, tecnologia e outsourcing per un ampio spettro di Clienti a livello mondiale, Capgemini è impegnata a proteggere la privacy e i dati personali affidatile. Come Gruppo Internazionale con aziende in più di 40 nazioni, Capgemini ha bisogno di assicurare che i dati personali circolino liberamente e in maniera sicura tra le aziende del Gruppo con un livello di protezione appropriato e uniforme.

La maggior parte dei paesi all'interno dei quali il Gruppo fornisce servizi dispone di Leggi riguardanti la protezione dei dati o la privacy, emanate per regolare la raccolta, l'utilizzo, il trasferimento, la conservazione e la distruzione dei dati personali. Come stabilito nel "Codice Etico" e nella "Data Privacy Policy" (Allegato 1), Capgemini è impegnata a garantire la conformità alle normative sulla protezione dei dati personali, vigenti negli Stati dove gli stessi vengono raccolti ed elaborati. Ciò include, il rispetto delle norme emanate dall'Unione Europea, sia attuali che future.

Inoltre, i Clienti che affidano i propri dati personali a Capgemini, confidano in una organizzazione che operi in modo efficace e competitivo a livello globale nella gestione dei loro dati personali. Ciò significa che, potenzialmente, sulla base di specifiche direttive del Cliente o al fine di soddisfare una sua legittima necessità, i dati personali del Cliente possono essere archiviati e trattati presso le sedi e i data center di Capgemini situati anche, al di fuori dell'"**European Economic Area**" (EEA).

Le Binding Corporate Rules di Capgemini e i relativi Allegati (complessivamente nel prosieguo referenziati come **"BCR"**) sono stati adottati per esprimere l'impegno di Capgemini nello stabilire e mantenere elevati standard di Gruppo per il trasferimento e il trattamento di dati personali da parte di tutte le società appartenenti al Gruppo Capgemini.

Le BCR sono state elaborate per proteggere i flussi di dati personali trasferiti all'interno del Gruppo Capgemini (comprese le sedi situate al di fuori dell'EEA) per le finalità di trattamento descritte nel presente documento, in modo da consentire una libera e sicura circolazione dei dati personali tra le società Capgemini. Le BCR si applicano ai trattamenti dei dati personali effettuati da Capgemini in qualità di "Data Controller" (**BCR-Controller**) nonché ai trattamenti di dati personali effettuati da Capgemini in qualità di "Data-Processor" (**BCR-Processor**).

Le BCR hanno anche lo scopo di sintetizzare le misure implementate da Capgemini, come espressione del più ampio impegno assunto dall'azienda nell'ambito della responsabilità sociale, per dimostrare che i trattamenti dei dati personali effettuati dalle società del Gruppo Capgemini sono condotti secondo quanto stabilito dalla normativa europea.

Per dare piena efficacia ai propri impegni, in aggiunta alle presenti BCR, Capgemini ha implementato un programma globale di "privacy compliance" che comprende (1) una "Global Data Privacy policy", (2) una "Cybersecurity Organization" che include un "global network" di Data Protection Officer, avvocati specializzati in privacy e professionisti della sicurezza, (3) programmi di conoscenza e di formazione in materia di privacy e sicurezza per i dipendenti; (4) meccanismi di monitoraggio del livello di conformità ai requisiti normativi e contrattuali in ambito privacy; e (5) piani di risposta agli incidenti di sicurezza.

1. Definizioni

Ai fini del presente documento, si riportano i seguenti termini da intendersi in conformità con quanto previsto dalla normativa Europea:

"**Legislazione applicabile**": si intende qualsiasi normativa in materia di privacy o di protezione dei dati, applicabile nel momento in cui vengono effettuati i trattamenti.

"**Business Contact**": si intende un fornitore di Capgemini, un sub-fornitore, cliente o partner, con cui Capgemini ha (ha avuto o potrebbe avere) rapporti commerciali.

"**Capgemini**" o "**Gruppo**": si intende l'intero Gruppo delle società Capgemini controllate, direttamente o indirettamente, da Capgemini SE.

"**Società Capgemini**": si intende una società all'interno di Capgemini che è controllata, direttamente o indirettamente, da Capgemini SE.

"**Capgemini Data Privacy Policy**": si intende la Politica emananata da Capgemini in materia di "Data privacy" che disciplina tutte le attività delle società del Gruppo Capgemini operanti in qualità di Data-Controller o di Data-Processor ed elencate nell'Allegato 1.

"**BCR-Controller**": si intende l'insieme di norme, presenti nel documento, che si applicano a Capgemini quando agisce come Data Controller.

"**Dati Personali oggetto di disciplina**": si intendono i dati personali inclusi nel campo di applicazione delle BCR.

"**Data Controller**" o "**Controller**"**:** si intende la società che determina le finalità e le modalità di trattamento dei dati personali.

"**Data Processor**" o "**Processor**": si intende la società che effettua trattamenti di dati personali per conto del Data Controller (se una società del Gruppo Capgemini agisce quale Data Processor, siamo nell'ipotesi di "**Internal Data Processor**", se invece "Data Processor" non è una società del Gruppo Capgemini, viene qualificata quale "**External Data Processor**"), e che può essere localizzata all'interno o al di fuori dell'EEA.

"**Data Subject**": si intende l'individuo (interessato) a cui si riferiscono i dati personali.

"**DPA**": si intende l'Autorità per la Protezione dei dati personali.

"**DPO**": si intende il Data Protection Officer.

"**EEA**": si intende l'European Economic Area.

"**Dipendente**": si intende un dipendente delle società Capgemini o lavoratori in regime di somministrazione.

"**Dati Personali dei Dipendenti**": si intendono i dati personali di un dipendente Capgemini attuale, ex o potenziale.

"**Normativa Europea**": si intende la direttiva 95/46/EC del Parlamento Europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione dei dati, nonché la Direttiva 2002/58/EC del Parlamento Europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e ogni successiva modifica alla legislazione dell'Unione Europea.

"BCR-Processor": si intende l'insieme di norme, presenti nel documento, che si applicano a Capgemini quando agisce come Data Processor.

"**Dato Personale**": si intende qualunque informazione relativa a una persona fisica identificata o identificabile ("**Data Subject**"). Una persona è identificabile quando può essere identificata, direttamente o indirettamente, da un numero di identificazione o da uno o più riferimenti riguardanti la propria identità fisica, fisiologica, psichica, economica, culturale o sociale. I Dati Personali sono intesi anche come Informazioni Identificative della Persona.

"**Trattamento**": include la raccolta, la registrazione, l'organizzazione, la conservazione, la modificazione, il ripristino, la consultazione, l'utilizzo e la divulgazione mediante comunicazione, o diffusione o in qualunque altro modo resi disponibili, il raffronto o l'associazione, il blocco, la cancellazione o la distruzione di dati personali.

"**Security Breach**": si intende qualsiasi azione che possa compremettere la sicurezza e che conduca alla accidentale o illegittima distruzione, perdita, alterazione, divulgazione non autorizzata o accesso a dati personali trasmessi, archiviati o altrimenti trattati.

"**Dati Personali Sensibili**": si intendono i dati personali che rivelano direttamente o indirettamente l'origine raziale e o etnica, le convinzioni politiche, filosofiche o religiose, i precedenti giudiziari, le adesioni ad organizzazioni sindacali, nonché i dati personali relativi allo stato di salute o alla vita sessuale.

"**Service Agreement**": si intende un accordo scritto tra il Data Controller e il Data Processor in cui si stabilisce che il Data Processor fornisce servizi al Data Controller e che ciò comporta il trattamento di dati personali da parte del Data Processor secondo le istruzioni impartite dal Data Controller.

"**SBU**": si intende una Business Unit Capgemini strategica a livello di Gruppo.

2. Ambito di applicazione delle BCR

2.1 Ambito di applicazione materiale

Le BCR regolamentano i trattamenti di dati personali effettuati da Capgemini in qualità di Data Controller (**BCR-Controller**) nonché quelli effettuati in qualità di Data Processor (**BCR-Processor**). Tali Dati Personali comprendono i Dati Personali dei Dipendenti trattati per finalità connesse al rapporto lavorativo, così come i Dati Personali dei Business Contact trattati per finalità di business. Quando si agisce come Data Processor possono essere oggetto di trattamento anche altre tipologie di Dati Personali in base a quanto richiesto dal Data Controller.

2.2 Ambito territoriale

Le BCR si applicano alle Società Capgemini nella misura in cui queste trattano Dati Personali oggetto della disciplina in qualità di Data Controller o di Data Processor. Per ulteriori informazioni sulle Società Capgemini presenti a livello mondiale è possibile cliccare qui.

Il trasferimento di dati personali oggetto della disciplina alle Società Capgemini situate al di fuori dell'"**EEA**" viene effettuato solo verso quelle società che hanno aderito alle BCR, sottoscrivendo uno specifico accordo.
Le BCR rispecchiano quanto previsto dalla Legislazione Europea e dalle Legislazioni nazionali dei paesi dell'**"EEA"** in tema di protezione dei dati. In alcuni paesi, la normativa nazionale potrebbe essere maggiormente restrittiva. Nella misura in cui queste leggi nazionali sono applicabili ai Dati Personali oggetto della disciplina, gli uffici legali locali dei paesi interessati, ove ritenuto opportuno, emetteranno specifiche linee guida o *policy* locali che si applicheranno in aggiunta alle BCR. Alcune *privacy policy* possono anche essere implementate nell'ambito di alcune Business Unit Capgemini o Società Capgemini. Tali *privacy policy* faranno riferimento alle BCR e terranno conto di ogni Legge locale o di regolamenti che prevedono requisiti ulteriori o maggiormente stringenti.

Le BCR-Controller si applicano solo ai dati personali oggetto della disciplina trasferiti dall'EEA verso il Gruppo Capgemini.
Per quanto concerne le **BCR-Processor**, il **"Controller"** può decidere di applicare le BCR 1) ai dati personali trattati da una società Capgemini per conto dello stesso **"Data Controller"** che è soggetto alla Legislazione Europea, o 2) ai dati personali trattati da una società Capgemini per conto del "**Data Controller**", qualunque sia l'origine di tali dati personali.

3. Attuazione delle BCR e della Capgemini Data Privacy Policy

Le BCR e la "**Capgemini Data Privacy Policy**" riportata nell'Allegato 1 saranno vincolanti per tutte le società Capgemini e i loro dipendenti. Il Management locale delle Società Capgemini e i relativi DPO saranno responsabili per l'attuazione delle BCR e della "**Capgemini Data Privacy Policy**".

La "**Capgemini Data Privacy Policy**" e una versione pubblica delle BCR (tradotta in lingua nazionale, laddove richiesto) sono disponibili nella Intranet Capgemini o nel sito web di Capgemini.
La "**Capgemini Data Privacy Policy**" incorpora i principi che governano il trattamento dei dati nell'ambito del Gruppo Capgemini, principi basati sugli articoli 6 e 7 della Direttiva 95/46/EC del Parlamento Europeo e del Consiglio del 24 ottobre 1995 sulla protezione degli individui in relazione al trattamento di dati personali ed alla libera circolazione di tali dati.

Questi principi verranno sviluppati qui di seguito.

3.1 Capgemini tratta i dati personali in modo leale, trasparente e conforme alla Legge

Quando opera come Data Controller, Capgemini tratta i dati personali in conformità alla **"Legislazione Applicabile"**, fornendo tutte le informazioni necessarie al **"Data Subject"** (interessato) e consentendo l'accesso ai propri dati personali come previsto dalla "**Legislazione**

Applicabile" e in accordo con le procedure di Capgemini applicabili. Quanto sopra descritto comporta che i trattamenti di dati personali siano adeguati, pertineti e non eccedenti rispetto alle finalità della raccolta, e che l'aggiornamento, la correzione o la cancellazione dei dati personali siano accurate e mantenute costantemente aggiornate.

Quando opera come Data Processor, Capgemini tratta i dati personali in conformità alla **"Legislazione Applicabile"** ed alle istruzioni del "**Data Controller**" nel pieno rispetto dagli obblighi contrattuali riportati nel "**Service Agreement**". Capgemini supporterà il "**Data Controller**", per quanto ragionevolmente necessario, per il raggiungimento della conformità alla normativa sulla protezione dei dati ed ai principi di qualità dei dati, correttezza delle elaborazioni e trasparenza degli stessi. Capgemini prontamente offrirà la propria collaborazione e assistenza al "**Data Controller**", entro un termine ragionevolmente possibile. Ciò potrà includere l'aggiornamento, la rettifica o la cancellazione dei Dati Personali e la comunicazione ad altri "**Data Processor**" in base alle richieste dei Data Subject o del Data Controller, in maniera che le informazioni siano accurate e aggiornate. Ciò potrà, altresì, includere, la comunicazione al "**Data Controller**", di qualsiasi informazione utile che possa faciliatere l'esercizio dei diritti dell'interessato, la gestione dei reclami o la risposta ad investigazioni o la risposta alle richieste di chiarimento o di approfondimento da parte delle DPA.

3.2 Capgemini tratta dati personali per finalità circoscritte e definite

Quando opera come Data Controller, Capgemini tratta dati personali solo per finalità determinate, esplicite e legittime e in conformità con gli scopi per i quali i dati sono stati orginariamente raccolti, nel rispetto della **"Legislazione Applicabile"**. Capgemini tratta dati personali (i) con il consenso esplicito del **"Data Subject"** (interessato) o (ii) per l'adempimento di un contratto di cui l'interessato è parte o al fine di adottare le necessarie misure a seguito di una richiesta dell'interessato prima di stipulare un contratto, o (iii) per adempiere a un obbligo di Legge a cui il Data Controller è soggetto, o (iv) per proteggere gli interessi vitali dell'interessato, o (v) quando il trattamento è necessario per le finalità legate ai legittimi interessi di Capgemini o di terze parti a cui i dati sono stati comunicati, eccetto i casi in cui su tali finalità prevalgono i diritti e le libertà fondamentali e le libertà dell'interessato. I Dati Personali sono comunicati solo per finalità legittime e pertinenti nel rispetto del principo del "*need to know*" per ragioni di business o legali. In ogni caso, qualsiasi comunicazione di dati personali è strettamente limitata a quanto sia necessario e ragionevole per assicurare le finalità di trattamento. Fatti salvi i casi di acquisizione di business o cessioni, Capgemini non vende o commercializza dati personali. In aggiunta, e in conformità con quanto previsto dalla "**Legislazione Applicabile**", i "**dati personali sensibili**" vengono trattati da Capgemini (i) se l'interessato ha fornito un consenso esplicito, o (ii) se il trattamento è necessario per adempiere agli obblighi in materia di legislazione del lavoro, o (iii) se il trattamento è necessario per proteggere gli interessi vitali dei "**Data Subjects**" (interessati) o di un'altra persona nel caso in cui il "**Data Subject**" si trovi nell'incapacità fisica o giuridica di fornire il proprio consenso, o (iv) se il trattamento riguarda dati che sono, in maniera manifesta, resi pubblici da parte del "**Data Subject**" o se sono necessari per costituire, esercitare o difendere un diritto per via giudiziaria.

Quando opera come Data Processor, Capgemini tratta dati personali nel rispetto delle istruzioni impartite del Data Controller e non effettua ulteriori trattamenti per un diverso cliente o per una differente finalità, salvo il caso in cui vi sia l'esplicito consenso del "**Data Controller**", e, in ogni caso, in base alla "**Legislazione applicabile**". Nel caso in cui Capgemini non possa trattare i

dati personali in conformità con quanto previsto dalle istruzioni del "**Data Controller**", ne informerà tempestivamente lo stesso; in tal caso il "**Data Controller**" avrà il diritto di interrompere il trasferimento di dati personali e risolvere il rapporto contrattuale, per quanto concerne il trattamento di dati personali, in conformità con quanto previsto dal contratto e dalla "Legislazione applicabile". Allo stesso modo, qualora venissero modificate le condizioni di trattamento, Capgemini informerà il "**Data Controller**" in maniera tempestiva in modo che questi abbia la possibilità di opporsi alla modifica o di recedere dal contratto prima della realizzazione del cambiamento stesso.

Quando svolge trattamenti di dati personali, Capgemini utilizza processi e tool che integrano gli aspetti di privacy fin dal principio (*privacy by design*) e svolge attività di valutazione degli impatti attinenti quanto previsto in materia di privacy, così come richiesto dalla "**Legislazione Applicabile**".

3.3 Capgemini tratta dati personali per un tempo limitato

Quando opera come Data Controller, Capgemini conserva dati personali in una forma che permette l'identificazione del "**Data Subject**" (interessato) solo per il tempo necessario al raggiungimento delle finalità per le quali viene effettuato il trattamento, nel rispetto delle Leggi nazionali.

Quando opera come Data Processor, Capgemini tratta dati personali solo in conformità alle istruzioni del "**Data Controller**", compresi anche, gli aspetti di durata della conservazione. Ciò può includere l'esecuzione di un'attività necessaria per la tutela dell'interesse pubblico o nell'esercizio di un potere conferito a Capgemini o a una terza parte a cui i dati sono stati comunicati. Nel rispetto di tali requisiti, alla fine del trattamento, i dati personali e le relative copie possono essere restituite al "**Data Controller**", anonimizzate o possono essere distrutte in maniera appropriata e sicura, e le stesse istruzioni vengono comunicate agli altri "**Data Processor**". Allorquando Capgemini distrugga i dati personali, certificherà tale distruzione al "**Data Controller**" agendo sempre nel rispetto di quanto previsto dalla normativa nazionale e degli obblighi di sicurezza e *back-up*. Nel caso in cui la legislazione nazionale impedisca a Capgemini di restituire o distruggere in toto o parzialmente i dati personali, Capgemini ne informerà il "**Data Controller**" e garantirà l'impegno ad assicurare la riservatezza dei dati personali scambiati e che gli stessi non vengano più trattati.

3.4 Capgemini tratta dati personali in maniera sicura

Come regola generale, e salvo diversamente richiesto dal Cliente, Capgemini applica lo stesso livello di sicurezza ai dati personali che tratta sia come "**Data Processor**" che come "**Data Controller**".

Capgemini applica e mantiene appropriate misure tecniche, fisiche e organizzative per proteggere i dati personali, e si avvale di pratiche e specifici standard nell'adottare procedure e implementare sistemi progettati per prevenire accessi non autorizzati a dati personali ed evitare la loro perdita accidentale, danneggiamento o distruzione.

Capgemini riporterà le violazioni di sicurezza alle Autorità e/o ai "**Data Subjects**", in base a quanto previsto dalla "**Legislazione Applicabile**", nel caso in cui rilevi che la sicurezza, la riservatezza o l'integrità dei dati personali siano state compromesse.

Quando opera come Data Processor, Capgemini lavora in conformità alle misure organizzative e di sicurezza che soddisfano almeno, i requisiti della legislazione applicabile al "**Data Controller**" e le disposizioni previste nel "**Service Agreement**". Capgemini informerà tempestivamente il "**Data Controller**" di qualsiasi violazione di sicurezza e garantirà che i suoi "**Processor**" siano soggetti ad obblighi equivalenti.

3.5 Capgemini lavora con i *sub-processor* in modo responsabile

Capgemini utilizzerà "**Processors**" interni al Gruppo ma stabiliti al di fuori dell'**EEA**, soltanto qualora gli stessi abbiano sottoscritto le BCR e la "**Capgemini Data Privacy Policy**" e siano vincolati da un accordo *intercompany,* nonché da uno *statement of work*.

In caso di utilizzo di "**External Data Processors**", Capgemini stipulerà con gli stessi specifici accordi che prevedano modalità di trattamento e conservazione dei dati personali secondo quanto previsto dalla Legislazione Europea nonché dalle istruzioni del "**Data Controller**".

In caso di utilizzo di "**External Data Processors**" stabiliti al di fuori dell'**EEA**, Capgemini stipulerà con gli stessi accordi che prevedano clausole contrattuali standard per il trasferimento dei Dati Personali secondo quanto previsto dalla Direttiva 95/46/EC del Parlamento Europea e del Consiglio.

Allorquando operi come Data Processor, Capgemini assicurerà che i trattamenti di dati personali affidati a "**Processor**" Capgemini o a "**External Data Processors**", nel corso della fornitura dei servizi, siano effettuati con il consenso e sotto la direzione del "**Data Controller**" e siano strettamente pertineti alle attività di trattamento. Tali trattamenti saranno effettuati sulla base di specifici accordi che vincolino il suddetto "**External Data Processors**" ad obblighi equivalenti a quelli imposti al "**Data Processor**" in virtù di quanto previsto nei "**Service Agreement**", nonché ai principi enunciati nelle BCR. Inoltre, qualora vengano trasferiti dati personali verso *External Data Sub-Processors* situati al di fuori dell'**EEA**, Capgemini stipulerà con detti "**Data Processors**" accordi *ad-hoc* che prevedano modalità di trattatamento e conservazione dei dati personali in accordo alla Legislazione europea applicabile nonché alle istruzioni impartite del "**Data Controller**".

4. Struttura di governance per la tutela dei dati personali in Capgemini

Al fine di proteggere le informazioni proprie e quelle dei propri Clienti e per fronteggiare i rischi di sicurezza, Capgemini ha lanciato un programma globale di *Cybersecurity and Information Protection* (detto anche "CySIP") con l'obiettivo di stabilire un livello di sicurezza omogeneo e obbligatorio per tutte le entità del Gruppo Capgemini. La protezione dei dati, la *data privacy* e la riservatezza sono l'essenza del programma CySIP. Il programma CySIP di Gruppo è guidato dal *Group CySIP Officer* che riporta al *Group General Secretary*.

Quale parte del più ampio programma CySIP, relativamente alle tematiche di privacy, è stata predisposta una specifica struttura di *privacy governance*, guidata dal *Group DPO* che ha il compito di supervisionare l'intero programma di conformità alla privacy del Gruppo, svolgendo attività quali: fornire consulenza in merito a questioni di data privacy, monitorare l'applicazione

delle BCR e della "**Capgemini Data Privacy Policy**" da parte delle società del Gruppo Capgemini, organizzare delle campagne globali di sensibilizzazione e monitorarne l'attuazione. Il *local DPO* sovrintende all'implementazione locale delle BCR, della Capgemini Data Privacy Policy e di tutte le iniziative di sensibilizzazione collegate. Agisce come delegato locale del Group DPO e funge da unico punto di contatto verso la DPA locale.

5. Diritti dei Data Subject (Interessati)

I "**Data Subjects**" possono esercitare i propri diritti secondo la procedura "Richiesta Esercizio dei Diritti degli Interessati" e sul sito *web* locale di Capgemini come ulteriormente dettagliato nell'**Allegato 2**. Qualora la "**Legislazione Applicabile**" contempli un livello di protezione più elevato, il *local DPO* si accerterà che venga applicato al "**Data Subject**" il livello di protezione più alto stabilito dalla Legge.

Eventuali richieste di informazioni sulle BCR, da parte dei "**Data Subjects**", dovrebbero essere indirizzate ai *local DPO* (e, se necessario, al *Group DPO*) che si attiverà affinché tali richieste ricevano risposte soddisfacenti e in ogni caso nel rispetto dei termini del "**Service Agreement**" quando Capgemini operi come "**Data Processor**".

I "**Data Subjects**" possono inoltrare le richieste scrivendo preferibilmente a mezzo mail a dataprivacy.it@capgemini.com.
Le informazioni di contatto sono disponibili sui siti web delle società Capgemini.

5.1 Procedura per l'esercizio dei diritti dei Data Subjects

All'interno del Gruppo, è presente una procedura specifica a livello locale e disponibile sulla intranet locale, per consentire ai "**Data Subjects**" (interessati), l'esercizio dei diritti di accesso, opposizione, rettifica e/o cancellazione dei dati. Ogni richiesta di esercizio dei diritti è gestita secondo la procedura locale in vigore. I *local DPO*, agendo di concerto con il *Group DPO*, saranno sempre a disposizione del "Data Controller" e del "**Data Subject**" (interessato) per fornire assistenza.

Allorquando Capgemini operi come Data Controller, il *local DPO* risponderà alla richiesta di un "**Data Subject**" (interessato) in un termine ragionevole, e comunque non oltre i due (2) mesi e sempre nel rispetto della "**Legislazione Applicabile**". Qualora la richiesta venisse respinta o qualora l'interessato non fosse soddisfatto della risposta, questi avrà il diritto di presentare un reclamo ai sensi dell'articolo 5.2 delle BCR.

Allorquando Capgemini operi come Data Processor, il *local DPO* agirà in conformità con quanto previsto dal **"Service Agreement"** stipulato con il "**Data Controller**". I **"Service Agreements"** in generale prevedono che il "**Data Controller**" si riservi il diritto di rispondere alle richieste di esercizio dei diritti dei "**Data Subjects**" (interessati) e di imporre che Capgemini inoltri ogni detta richiesta al "**Data Controller**", invece di rispondere direttamente ai "**Data Subjects**" (interessati). Nei casi in cui il **"Service Agreement"** non contenga alcuna disposizione in merito alla gestione dei diritti dei "**Data Subjects**", per impostazione predefinita, il *local DPO* inoltrerà la richiesta di esercizio dei diritti al "**Data Controller"**. Qualora Capgemini dovesse rispondere direttamente, fornirà una risposta al "**Data Subject"** entro un termine ragionevole e nel pieno rispetto della "**Legislazione applicabile**". Nel caso in cui la richiesta di

esercizio dei diritti venisse rifiutata o qualora il "**Data Subject"** non fosse soddisfatto della risposta ricevuta, questi avrà il diritto di presentare un reclamo ai sensi dell'articolo 5.2 delle BCR.

5.2 Procedura di gestione dei reclami

La procedura di gestione dei reclami si applicherà nel caso in cui il "**Data Subject**" ritenga che la procedura per l'esercizio dei diritti degli interessati non sia andata a buon fine o che i propri diritti di in materia di tutela dei dati siano stati violati.

I reclami saranno gestiti dal *local DPO*. Qualora venisse registrato un reclamo, lo stesso verrà gestito in un tempo ragionevole, ma non oltre i due (2) mesi ed in base alla "**Legislazione Applicabile**".

Qualora il *local DPO* non riuscisse a risolvere un reclamo presentato dal "**Data Subject**, a livello locale, quest'ultimo potrà presentare ricorso verso il *Group DPO*, che risponderà in un tempo ragionevole, ma non oltre i due (2) mesi ed in base alla "Legislazione Applicabile".

Alloquando Capgemini operi come Data Processor, il "**DPO**" gestirà un qualsiasi reclamo di un **"Data Subject"** (interessato) solo nel caso in cui quest'ultimo non sia in grado di portare il reclamo all'attenzione del **"Data Controller"** perché lo stesso abbia cessato di esistere giuridicamente o sia diventato insolvente e non vi siano entità successorie che abbiano assunto gli interi obblighi legali del precedente "**Data Controller**" per contratto o per esercizio di Legge. La risoluzione di un reclamo è sempre soggetta a vincoli tecnici ed alle disposizioni dei "**Service Agreements**" stipulati con il "**Data Controller**". Qualora il "**Service Agreement**" non contenesse alcuna disposizione relativa alla gestione dei reclami, per impostazione predefinita, il *local DPO* riporterà, gli stessi, senza ritardi, al "**Data Controller**".

6. Responsabilità

6.1 Responsabilità verso i Data Subjects

Le BCR conferiscono diritti ai "**Data Subjects,** al fine di rafforzarne la tutela. Nel caso in cui il "**Data Subject**" abbia subito un danno causato da una società Capgemini a seguito della non osservanza delle BCR, lo stesso ha il diritto di portare il caso all'attenzione della "**DPA**" o rivolgersi alle Autorità giurisdizionali dell'**EEA** territorialmente competenti o dinanzi alle Autorità giurisdizionali del paese nel quale ha sede il "**Data Controller**" o dinanzi alle Autorità Giudiziarie nell'**EEA** dove ha sede la società capogruppo di Capgemini (Francia).

In ogni caso, qualora una società Capgemini fosse cessata e le sue responsabilità non fossero assunte da altra entità, la "**DPA**" e le Autorità giudiziarie di riferimento saranno quelle del paese dell'**EEA** presso cui il "**Data Processor**" o la sua sede principale siano localizzate. Qualora la seconda soluzione non fosse applicabile, saranno competenti la "**DPA**" e le Autorità giudiziarie del paese di residenza del "**Data Subject**".

Nel caso in cui il "Data Subject" sia in grado di dimostrare fatti che confermino di avere subito un danno generato esclusivamente dalla violazione delle BCR, la società Capgemini che abbia originato il trasferimento dei dati personali verso una società Capgemini stabilita al di fuori dell'**EEA** si assumerà l'onere di provare che la società Capgemini situata al di fuori dell'**EEA** non sia responsabile per la violazione delle BCR che hanno dato orgine a tali danni. Qualora possa essere fornita tale prova, la società sarà automaticamente sollevata dalla propria responsabilità.

La società Capgemini che abbia trasferito i dati personali al di fuori dell'**EEA** compirà le azioni ragionevoli e necessarie per porre rimedio alle violazioni delle BCR commesse dalla società Capgemini sita al di fuori dell'EEA e per risarcire esclusivamente i danni derivanti da tale violazione.

Allorquando operi come Data Processor, la società Capgemini che abbia trasferito i dati personali al di fuori dell'**EEA** compirà le azioni ragionevoli e necessarie per porre rimedio alle violazioni commesse della società Capgemini sita al di fuori dell'**EEA** o dall' *External Sub Processor* sito al di fuori dell'**EEA**, in violazione delle **BCR-Processor,** e per risarcire esclusivamente i danni derivanti dalla presunta violazione.

Nel caso in cui il "**Data Controller**" abbia cessato le sue attività e le sue responsabilità non siano state acquisite da altra entità, la "**DPA**" e le Autorità giudiziarie di riferimento saranno quelle del paese dell'**EEA** presso cui è stabilita la società Capgemini o le Autorità Giudiziarie del paese dove ha sede la società Capogruppo di Capgemini (Francia). Qualora la seconda soluzione non fosse applicabile, saranno competenti la "**DPA**" e le Autorità giudiziarie del paese di residenza del "**Data Subject**".

La società Capgemini che ha sede nell'**EEA** non potrà fare affidamento suL fatto che tale violazione sia sata commessa da parte del *Sub-Processor* non appartenente all'**EEA**, per evitare la responsabilità che ha nei confronti dei "**Data Subjects**".

I diritti dei "**Data Subjects**" sono limitati ai seguenti obblighi del "**Data Processor**" in termini di conformità alle **BCR-Processor**: obbligo di rispettare le **BCR-Processor** e di consentire l'esercizio dei diritti dei "**Data Subjects**", responsabilità di risarcimento e ripristino della situazione causata dalle violazioni, onere della prova in capo al "**Data Processor**", accesso agevolato per l'interessato alle **BCR-Processor**, esistenza di una procedura di reclamo, obbligo di collaborare con la "**DPA**" e con il "**Data Controller**", descrizione dei principi di data privacy, predisposizione di un elenco delle entità sottoposte alle **BCR Processor**, obbligo di trasparenza nel caso in cui la legislazione nazionale non consenta al Gruppo di essere conforme alle **BCR-Processor**.

6.2 Responsabilità verso il Data Controller

Questo paragrafo è applicabile solo nell'ambito delle **BCR-Processor**. Le **BCR Processor** saranno incluse nel "**Service Agreement**" con il "**Data Controller**".

La società Capgemini che abbia trasferito i dati personali a un'altra società Capgemini o a un "**External Data Processor**", entrambi localizzati al di fuori dell'**EEA**, sarà responsabile verso il "**Data Controller**" per i danni diretti derivanti esclusivamente dalla violazione delle **BCR-Processor** in base alle disposizioni del "**Service Agreement**" nonché, da quanto segue.

La società Capgemini che abbia trasferito i dati personali al di fuori dell'**EEA** non potrà fare affidamento sul fatto che una violazione degli obblighi previsti sia stata commessa da parte della società Capgemini o di un "**External Data Processor**", entrambi localizzati al di fuori dell'**EEA**, per venir meno alle proprie responsabilità nei confronti del "**Data Controller**". Tutti i "**Data Controller**" avranno il diritto far rispettare le BCR verso qualsiasi società Capgemini in caso di violazioni delle stesse.

In tal caso, qualora il "**Data Controller**" sia in grado di dimostrare fatti che confermino di aver subito un danno derivante esclusivamente da una violazione delle **BCR Processor**, la società

Capgemini che abbia trasferito i dati personali al di fuori dell'**EEA** verso un'altra società Capgemini o verso un "**External Data Processor**", entrambi localizzati al di fuori dell'**EEA**, si assumerà l'onere di provare il fatto contrario e di provare che il "**External Data Processor**", non sia responsabile per la violazione delle **BCR Processor** che ha originato tali danni.

Nel caso in cui Capgemini riesca a fornire la suddetta prova, sarà automaticamente sollevata dalla propria responsabilità.

Inoltre, la società Capgemini che abbia trasferito dati personali al di fuori dell'**EEA** a un'altra società o a un "**External Data Processor**", entrambi localizzati al di fuori dell'**EEA**, adotterà tutte le azioni necessarie affiché i comportamenti che hanno dato origine alle violazioni delle **BCR-Processor** siano risolti da parte dei su citati soggetti.

7. Audit

Quando richiesto dalla "**Legislazione Applicabile**" o da una "**DPA**", Capgemini concorda che gli audit possano essere effettuati direttamente dalle "**DPA**" e si impegna a collaborare con le stesse.

8. Responsabilità dei dipendenti Capgemini – Sensibilizzazione e Formazione

Ogni dipendente Capgemini dovrà operare in conformità alle disposizioni delle BCR.

I dipendenti sono informati che, ogni qual volta si trovino a trattare dati personali, hanno la responsabilità di agire in conformità alla "**Legislazione Applicabile**" in materia di data privacy, nonché alle BCR e alla "**Capgemini Data Privacy Policy**".

Possono essere previste ulteriori iniziative locali al fine di assicurare che i dipendenti ricevano tutte le informazioni e gli aggiornamenti necessari.

Il mancato rispetto delle BCR e della "**Capgemini Data Privacy Policy**" può esporre sia i Dipendenti che le stesse Società del Gruppo Capgemini a rischi di ingenti danni, conseguenze di carattere penale e altre penali. Pertanto ci si aspetta che tutti i Dipendenti operino nel rispetto delle BCR e della "**Capgemini Data Privacy Policy**". I Dipendenti sono informati che qualsiasi non conformità a queste policy sarà valutata in maniera molto seria e potrà portare ad appropriate azioni disciplinari, in accordo a quanto previsto dalle leggi locali.

9. Legislazione applicabile – Conflitti di regole

Le Società Capgemini tratteranno i dati personali disciplinati in accordo alle BCR e alla "Legislazione Applicabile". Le BCR saranno interpretate in accordo con la Legislazione dell'Unione Europea e con le leggi dello stato dove la società Capgemini responsabile per il trasferimento di dati personali è stabilita.

Qualsiasi conflitto tra le BCR e i requisiti legali vincolanti in un'altra giurisdizione che impediscano o ostacolino la conformità alle stesse dovrà essere portato, nel più breve termine possibile, all'attenzione del *Group DPO*, il quale prenderà una decisione dopo aver consultato la "**DPA**" di riferimento, se necessario.

In base a quanto previsto nelle **BCR-Processor**, qualora una società Capgemini abbia ragioni per credere che la legislazione ad essa applicabile esistente o futura possa impedire l'adempimento delle istruzioni ricevute dal "**Data Controller**" o dei suoi obblighi previsti dalle BCR o dal "**Service Agreement"**, questa notificherà tempestivamente tali questioni al Data Controller, il quale ha il diritto di sospendere il trasferimento di dati e/o concludere il "**Service Agreement"**, nonché alla società Capgemini responsabile per il trasferimento di dati personali e alla "**DPA**" competente per il "**Data Controller**".

Qualsiasi richiesta legalmente vincolante di divulgazione di dati personali proveniente da parte di un'autorità di polizia sarà comunicata al "**Data Controller**". In ogni caso, tale richiesta sarà tenuta in sospeso e la "**DPA**" competente per il "**Data Controller**" nonché la *lead DPA* per le BCR ne saranno chiaramente informate. Ad ogni modo, se in casi specifici la sospensione e/o la notifica non fossero consentiti, la società Capgemini si adopererà per opporsi a tale divieto al fine di comunicare il maggior numero di informazioni possibile nel più breve termine, ed essere in grado di dimostrare quanto fatto. Qualora la società Capgemini, nonostante si sia adoperata in tal senso, non sia nella posizione di effettuare la notifica alla "**DPA**" competente, fornirà annualmente informazioni generali sulle richieste di divulgazione dei dati personali da parte dell'autorità di polizia alle "DPA" competenti.

10. Collaborazione con le Autorità per la Protezione dei dati

Capgemini collaborerà con le "**DPA**" e si impegna a rispondere alle stesse su qualsiasi richiesta attinente le BCR e la loro implementazione in un termine ragionevole. Come previsto dalle **BCR Processor**, Capgemini collaborerà con le "**DPA**" del "**Data Controller**". Le società Capgemini collaboreranno tra di loro per quanto necessario, per rispondere alle richieste delle "**DPA**".

Le società Capgemini si conformeranno ai suggerimenti delle "**DPA**" su questioni legate alla interpretazione delle BCR.

Allegato 1: Capgemini Data Privacy Policy

Tra le principali aziende mondiali di fornitura di servizi di consulenza, tecnologia e outsourcing per un ampio spettro di Clienti a livello mondiale e presente in più di 40 paesi, Capgemini è impegnata a proteggere la privacy e i dati personali affidatile, sia quando agisce come "Data Controller" che quale "Data Processor" (si vedano le definizioni riportate alla fine del documento).

La maggior parte dei paesi all'interno dei quali Capgemini fornisce servizi dispone di Leggi riguardanti la protezione dei dati o la privacy, emanate per regolare la raccolta, l'utilizzo, il trasferimento, la conservazione e la distruzione dei dati personali. Come stabilito nel "Code of Business Ethics", Capgemini è impegnata a garantire la conformità alle normative sulla protezione dei dati personali vigenti negli Stati dove gli stessi vengono raccolti ed elaborati.

Al fine di dare piena efficacia ai suoi impegni, Capgemini sta implementando un programma globale di *privacy compliance* in aggiunta alla presente Capgemini Data Privacy Policy, che comprende i seguenti elementi:

- Organizzazione globale di Cybersecurity e protezione delle informazioni, che include:
  - Data Protection Officer;
  - Avvocati in ambito privacy;
  - Professionisti della cyber security.

- Sensibilizzazione in materia di privacy e formazione:
  - Formazione in ambito privacy e sicurezza per i dipendenti;
  - Continui *reminder* in materia di riservatezza per i dipendenti;
  - Formazione privacy per profili specifici;
  - Gruppi di lavoro o attività di sensibilizzazione privacy e sicurezza per specifici ambiti;
  - Interventi periodici per la sensibilizzazione in ambito privacy e sicurezza.

- Monitoraggio della conformità ai requisiti normativi e contrattuali in materia di privacy:
  - Audit interni;
  - Audit di Clienti;
  - Conformità ai framework degli standard che costituiscono *best practice* (come ad esempio gli standard ISO);
  - Revisioni di qualità dei Data Protection Officer.
- Un processo di *Global Security Incident Response* e piani di risposta agli incidenti specifici per il cliente;
- Binding Corporate Rules per i ruoli di "Data Controller" e "Data Processor".

La Capgemini Data Privacy Policy raccoglie i principi che disciplinano il trattamento dei dati personali per l'intero Gruppo. Il rispetto di tale Politica è obbligatorio per tutte le società Capgemini, Business Unit e dipendenti che raccolgono e/o trattano dati personali.

La presente Policy si applica a tutte le attività di trattamento dati personali effettuate da Capgemini, in qualità sia di "Data Controller" che di "Data Processor".

1 Capgemini tratta i dati personali in modo leale, trasparente e conforme alla Legge

Capgemini tratta dati personali in conformità alla "Legislazione Applicabile" e le istruzioni del "Data Controller" (laddove applicabile).

Allorquando agisca come "Data Controller", in base alla "Legislazione Applicabile", Capgemini fornirà tutte le informazioni rilevanti all'interessato nel rispetto dei principi di equità e trasparenza.

Allorquando agisca come "Data Processor", Capgemini assisterà il "Data Controller" nell'adempimento della propria funzione.

Ciò include il rispetto dei diritti di aggiornamento, la correzione o la cancellazione dei dati personali in modo che il trattamento sia accurato e ove necessario mantenuto aggiornato in accordo alla procedura applicabile di Capgemini.

2 Capgemini tratta dati personali per finalità circoscritte e definite

Capgemini tratta solo dati personali in conformità con le finalità per le quali, gi stessi, sono stati originariamente raccolti e nonché in conformità con le istruzioni del "Data Controller" (se applicabile).

Capgemini, nel rispetto della "Legislazione Applicabile", non tratterà dati personali per finalità diverse, eccetto il caso in cui vi sia il consenso dell'interessato o del "Data Controller".

I dati personali sono comunicati soltanto per scopi legittimi e finalità di tipo "*need to know*", per ragioni di business o di natura legale. In ogni caso, qualsiasi divulgazione dei dati personali è strettamente limitata a quanto necessario e ragionevole per garantire le finalità del trattamento.

Capgemini è impegnata ad utilizzare processi e strumenti che integrano la privacy fin dal principio (*privacy by design*).

3 Capgemini tratta dati personali per un tempo limitato

In accordo con la "Legislazione Applicabile", le regole interne di Capgemini e le istruzioni del "Data Controller" (laddove presenti), Capgemini tratta dati personali solo per l'intervallo di tempo strettamente necessario al raggiungimento degli scopi per i quali, i trattamenti vengono effettuati.

Al termine del trattamento, Capgemini archivierà, anonimizzerà o distruggerà i dati personali, e altrimenti seguirà le istruzioni del Data Controller (laddove applicabile).

4 Capgemini tratta dati personali in maniera sicura

Come regola generale, e salvo diversamente richiesto dal Cliente, Capgemini applica lo stesso livello di sicurezza ai dati personali che tratta sia come "**Data Processor**" che come "**Data Controller**".

Capgemini applica e mantiene appropriate misure tecniche, fisiche e organizzative per proteggere i dati personali da accessi non autorizzati ed evitare la loro perdita accidentale, il danneggiamento, la distruzione o altre forme illegittime di trattamento.

Tali misure seguono quanto previsto da standard di settore e sono finalizzate a stabilire un livello di sicurezza appropriato rispetto ai rischi derivanti dal trattamento e dalla natura dei dati personali da proteggere.

Capgemini riporterà qualsiasi violazione di sicurezza alle Autorità e/o all'interessato e/o al "Data Controller", secondo quanto previsto dalla "Legislazione Applicabile" o dalle disposizioni contrattuali, qualora raggiunga la consapevolezza che la sicurezza, la riservatezza o l'integrità dei dati personali siano state compromesse.

5 Capgemini lavora con i *Data Processor* in modo responsabile

In base alla legislazione applicabile, allorquando vengano utilizzati "Internal" o "External Data Processor", Capgemini stipulerà, con gli stessi, appropriati accordi nei quali si richiede che i dati personali siano conservati e trattati in conformità alla "Legge Applicabile", includendo l'applicazione di adeguate misure di sicurezza.

Quanto sopra si applicherà anche nel caso in cui Capgemini agisca come "Data Processor", includendo quanto previsto dalle istruzioni del Data Controller.

Definizioni della Capgemini Data Privacy Policy

"**Legislazione applicabile**": si intende qualsiasi normativa in materia di privacy o di protezione dei dati, applicabile nel momento in cui vengono effettuati i trattamenti.

"**Capgemini Business Unit**": si intende un'unità organizzativa di *business* di Capgemini. Una Business Unit di Capgemini può essere parte di una società Capgemini o estendersi su diverse società Capgemini localizzate in Stati differenti, all'interno e/o al di fuori dell'EEA.

"**Capgemini**" o "**Gruppo**": si intende l'intero Gruppo delle società di Capgemini controllate, direttamente o indirettamente da Capgemini SE.

"**Società Capgemini**": si intende una società all'interno di Capgemini che è controllata direttamente o indirettamente, da Capgemini SE.

"**Data Controller**": si intende la società che determina le finalità e le modalità di trattamento dei dati personali.

"**Data Processor**": si intende la società che effettua i trattamenti di dati personali per conto del Data Controller (se una società del Gruppo Capgemini agisce quale "Data Processor", siamo nell'impotesi di "Internal Data Processor", se invece "Data Processor" non è una società del Gruppo Capgemini, viene qualificata quale "External Data Processor") e che può essere localizzato all'interno o al di fuori dell'EEA.

"**Data Subject**": si intende l'individuo (interessato) a cui si riferiscono i dati personali.

"**Dipendente**": si intende un dipendente delle società Capgemini o lavoratori in regime di somministrazione.

"**Dato Personale**" si intende qualsiasi informazione relativa ad una persona fisica identificata o identificabile ("**Data Subject**"). Una persona è identificabile quando può essere identificata, direttamente o indirettamente, da un numero di identificazione o da uno o più riferimenti riguardanti la propria identità fisica, fisiologica, mentale, economica, culturale o sociale. I dati personali sono intesi anche, come Informazioni Idetificative della Persona.

"**Trattamento**" include la raccolta, la registrazione, l'organizzazione, la conservazione, la modificazione, il ripristino, la consultazione, l'utilizzo e la divulgazione mediante comunicazione o diffusione o in qualunque altro modo resi disponibili, il raffronto o l'associazione, il blocco, la cancellazione o la distruzione di dati personali.

"**Security Breach**": si intende qualsiasi azione che possa compromettere la sicurezza e che conduca accidentale o illegittima distruzione, perdita, alterazione, divulgazione non autorizzata o accesso a dati personali trasmessi, archiviati o altrimenti trattati.

Per qualsiasi domanda si prega di contattare Nathalie Laneret, Group Data Officer, al seguente indirizzo e-mail: nathalie.laneret@capgemini.com

Allegato 2: Richiesta di esercizio dei diritti degli interessati e procedura di reclamo

Annoverata tra le principali aziende mondiali di fornitura di servizi di consulenza, tecnologia e outsourcing ad un ampio spettro di clienti a livello mondiale, somministrando servizi in più di 40 paesi, Capgemini ("**Noi**") è impegnata a proteggere la privacy e i dati personali alla stessa affidati, sia quando opera come Data Controller sia quando opera come Data Processor (si vedano le Definizioni alla fine del documento). La finalità di questa procedura inerente l'esercizio dei diritti dell'interessato e la gestione dei reclami ("**Procedura**") è quella di descrivere il processo con il quale un interessato ("**Tu**") possa avanzare una richiesta di esercizio dei diritti dell'interessato riguardante i propri dati personali che vengono trattati da Capgemini o presentare un reclamo avente ad oggetto il trattamento dei propri dati personali. In ogni caso l'interessato può anche contattare direttamente l'Autorità Locale per la Protezione dei dati personali o la corte giudiziaria competente.

1. Quali sono i diritti di un interessato?

In base alla Legge Applicabile e fatte salve eventuali deroghe, l'interessato ha il diritto di accedere ai suoi Dati Personali, il diritto di ottenere la loro rettifica, il diritto di opporsi al trattamento o il diritto di ottenere la loro distruzione e la conseguente cessazione del loro trattamento. Se si desidera esercitare questi diritti l'interessato può presentare una richiesta secondo i due procedimenti descritti qui di seguito.

1.1 **La Procedura di esercizio dei diritti dell'interessato:** se l'interessato ha un qualsiasi interesse o una qualsiasi domanda riguardante i suoi Dati Personali.

1.2 **La Procedura di reclamo dell'interessato:** se l'interessato non è soddisfatto della replica di Capgemini in merito alla sua richiesta di esercizio dei diritti o di ogni altra questione riguardante il trattamento dei propri dati personali.

Capgemini si impegna a gestire tutte le richieste sempre con il più alto livello di qualità e ad agire attivamente per risolvere in maniera soddisfacente qualsiasi richiesta.

2. Chi è autorizzato a presentare la domanda?

2.1. **Domanda diretta**: l'interessato a cui i dati personali si riferiscono può presentare una domanda a Capgemini, ad esempio un dipendente in organico o un ex dipendente, un cliente o un azionista di Capgemini.

2.2. **Domanda indiretta**: l'interessato può avanzare una richiesta per il tramite di un terzo soggetto che agisce in qualità di suo procuratore. In questo caso, l'interessato deve provare che la terza parte che sta effettuando la richiesta è autorizzata ad agire per suo conto, in base alla Legislazione Applicabile.

Attenzione – Tentare di ottenere Dati Personali per i quali non si è autorizzati potrebbe essere illegale nell'ambito della Legislazione Applicabile

3. Qual è l'ambito dei dati personali disciplinati?

I dati personali interessati da questa procedura includono tutti i dati personali trattati quando una Società Capgemini opera come Data Controller (sia quando tali Dati Personali sono trattati

internamente da una società Capgemini che agisce come Data Processor sia quando tali Dati Personali sono trattati da un External Data Processor).

Quando opera come Data Processor, Capgemini tratta solo i Dati Personali sulla base delle istruzioni contrattualmente specificate dal Data Controller. In questi casi, solo il Data Controller è in grado di rispondere alle richieste di esercizio dei diritti dell'interessato o di reclamo dell'interessato.

4. Quali sono le verifiche preliminari?

4.1. **Verifica dell'identità dell'interessato**: al fine di salvaguardare i dati Personali dell'interessato da accessi non autorizzati, prima di elaborare la suddetta domanda, sarà richiesto all'interessato di fornire a Capgemini un documento ufficiale di identificazione (es. passaporto, patente di guida, ecc.) per verificare la sua identità in base alla Legislazione Applicabile. Senza una appropriata identificazione la domanda non può essere elaborata.

4.2. **Verifica della completezza della domanda**: le domande incomplete o non accurate e/o per le quali l'identificazione non è stata possibile, saranno messe in attesa fino a quando l'interessato non sarà in grado di fornire a Capgemini le informazioni richieste.

Attenzione – Per facilitare la ricerca dei Dati Personali dell'interessato, si prega di specificare e di precisare il più possibile la domanda. In alcuni casi, Capgemini può addebitare costi per coprire le spese amministrative.

5. Saranno addebitati all'interessato costi per la sua domanda?

In alcuni casi ed in base alla Legge Applicabile, Capgemini, in considerazione della complessità della domanda dell'interessato e dello sforzo richiesto per soddisfarla in maniera appropriata, può decidere di richiedere un corrispettivo. L'ammontare del corrispettivo sarà ragionevole, in base alla complessità della richiesta. Se viene richiesto un corrispettivo, saranno notificati all'interessato l'importo e le opzioni di pagamento.

6. Quando si riceverà una risposta alla domanda presentata?

In primo luogo, Capgemini comunicherà all'interessato l'avvenuto ricevimento della domanda e poi che la stessa è in corso di elaborazione. L'elaborazione della domanda e l'inoltro dei risultati avverrà entro due (2) mesi (o in un termine inferiore ai sensi della Legislaizone Applicabile) dalla data in cui la richiesta è stata completata.

7. Come si può presentare la domanda?

7.1. **Domanda riguardante l'esercizio dei diritti dell'interessato:** l'interessato può presentare la domanda di esercizio dei diritti preferibilmente in forma scritta online sul sito web di Capgemini, a mezzo mail all'indirizzo dataprivacy.it@capgemini.com o mediante posta ordinaria al seguente indirizzo: Via di Torre Spaccata 140, 00173, Roma.

7.2. **Domanda riguardante un reclamo da parte dell'interessato:** l'interessato può presentare reclamo preferibilmente in forma scritta al DPO locale a mezzo email all'indirizzo dataprivacy.it@capgemini.com o mediante posta ordinaria al seguente indirizzo: Via di Torre Spaccata 140, 00173, Roma.

8. Chi gestisce la domanda?

La domanda dell'interessato sarà gestita dal relativo DPO locale. Se l'interessato non ha fornito sufficienti informazioni tali da consentire di localizzare i suoi Dati Personali, il DPO locale informerà lo stesso delle ulteriori informazioni richieste per elaborare la domanda.

Attenzione – Affinché la richiesta possa essere gestita nel tempo dovuto, raccomandiamo all'interessato di presentare domanda solo al DPO locale della società Capgemini della nazione in cui vive.

9. Cosa può fare l'interessato se non è soddisfatto della risposta Capgemini?

Se l'interessato non è soddisfatto della risposta di Capgemini in merito al reclamo proposto, può presentare in forma scritta e mediante email un ricorso in appello al DPO di Gruppo. Una risposta al suddetto Appello sarà fornita dal DPO di Capgemini in un periodo di due (2) mesi (o in un termine più breve ai sensi della Legislazione Applicabile) dalla data in cui l'Appello è stato inoltrato.

Se l'interessato non è soddisfatto della risposta al suo Appello, può contattare l'Autorità Nazionale per la Protezione dei dati personali o la corte giudiziaria competente.

Definizioni relative alla domanda di esercizio dei diritti dell'interessato e alla procedura di reclamo

"**Appello**": si intende il processo di impugnazione di una risposta a un reclamo presentato dall'interessato.

"**Legislazione Applicabile**": si intende qualsiasi normativa in materia di privacy o di protezione dei dati applicabile nel momento in cui vengono effettuati i trattamenti.

"**BCR**": si intendono le regole vincolanti per il Gruppo Capgemini sia quando opera come Controller che come Processor.

"Capgemini" o "Gruppo": si intende l'intero Gruppo delle società Capgemini controllate, direttamente o indirettamente, da Capgemini SE.

"**Società Capgemini**": si intende una società all'interno di Capgemini che è controllata, direttamente o indirettamente, da Capemini SE.

"**Dati Personali oggetto di disciplina**": si intendono i dati personali che sono inclusi nel campo di applicazione delle BCR.

"**Data Controller**": si intende la società che determina le finalità e le modalità di trattamento dei dati personali.

"**Data Processor**": si intende la società che effettua trattamenti di dati personali per conto del Data Controller che può essere localizzata all'interno o al di fuori dell'EEA.

"**Data Subject**": si intende l'individuo (interessato) a cui si riferiscono i dati personali. Può essere un dipendente in forza presso Capgemini, un ex dipendente, un tirocinante, un candidato, un fornitore, un cliente, l'utente di un servizio gestito da Capgemini per conto di un cliente o qualsiasi individuo i cui dati personali sono trattati da Capgemini.

"**Reclamo dell'interessato":** si intende il diritto dell'interessato di presentare un reclamo, nel caso in cui ritenga che i diritti indicati nella "Legislazione Applicabile" e nelle "BCR" non siano stati rispettati.

"**Procedura di reclamo dell'interessato (Data Subject)**": si intende la procedura che consente all'interessato di presentare un reclamo quando questi ritiene che i diritti indicati nella "Legislazione Applicabile" e nelle "BCR" non siano stati rispettati.

"**Richiesta di esercizio dei diritti dell'interessato**": si riferisce al diritto dell'interessato di avanzare una richiesta di esercizio dei diritti per l'accesso ("Richiesta di Accesso"), la rettifica ("Richiesta di Rettifica"), il blocco ("Richiesta di Blocco") o la cancellazione ("Richiesta di cancellazione") dei dati personali, ai sensi delle "BCR" e della "Legislazione Applicabile".

"**Procedura di richiesta di esercizio dei diritti dell'interessato**": si intende la procedura che consente a un interessato di sottoporre una richiesta di esercizio dei diritti al fine di esercitare i diritti individuali garantiti dalla "Legislazione Applicabile" e dalle "BCR".

"**DPO**": si intende il Data Protection Officer.

"**EEA**": si intende l'Area Economica Europea formata dagli Stati membri dell'Unione Europea così come dalla Norvegia, l'Islanda e il Lichtenstein.

"**Dipendente**": si intende un dipendente delle società Capgemini o lavoratori in regime di somministrazione.

"**Normativa Europea**": si intende la direttiva 95/46/EC del Parlamento Europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione dei dati, nonché la Direttiva 2002/58/EC del Parlamento Europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e ogni successiva modifica alla legislazione dell'Unione Europea.

"**Domanda**": si intendono le richieste di esercizio dei diritti dell'interessato e/o i reclami dell'interessato.

"**Dato Personale**": si intende qualsiasi informazione relativa a una persona fisica identificata o identificabile ("**Data Subject**"). Una persona è identificabile quando può essere identificata, direttamente o indirettamente, da un numero di identificazione o da uno o più riferimenti riguardanti la propria identità fisica, fisiologica, mentale, economica, culturale o sociale. I dati personali sono intesi anche come Informazioni Idetificative della Persona.

"**Trattamento**": include la raccolta, la registrazione, l'organizzazione, la conservazione, la modificazione, il ripristino, la consultazione, l'utilizzo e la divulgazione mediante comunicazione o diffusione o in qualunque altro modo resi disponibili, il raffronto o l'associazione, il blocco, la cancellazione o la distruzione di dati personali.