LG_DPO_v.1.0

Linea Guida di Governance “Privacy”

Approvata dal Consiglio di Amministrazione di Acea SpA con delibera n. 13 del 14 Marzo 2022

Indice

Versione	Data	Redatto da	Verificato da	Validato da	Approvato da	Motivo della revisione/aggiornamento
1.0	Marzo 2022	Responsabile Funzione Risk & Compliance	Responsabile Organizzazione e Process Governance Responsabile Unità Sistemi integrati di certificazione Responsabile Compliance Antitrust & Consumer Protection Responsabile Risk Governance & Compliance Data Protection Officer	AD	Consiglio di Amministrazione di Acea SpA	Review Corpus Procedurale Data Protection

Strumenti normativi annullati o sostituiti		
#	Nome strumento normativo	Data di emissione
1	LG_R&C01 - Versione 1.0 - Linee Guida Privacy by Design by Default	06/2018

Documento ad uso interno

Le informazioni contenute nel presente documento possono essere acquisite ed utilizzate dal personale aziendale con ordinaria diligenza per esclusive finalità lavorative, consapevole che queste costituiscono un bene da proteggere. È quindi vietato qualsiasi utilizzo delle stesse per finalità personali.

I documenti ad uso interno possono circolare liberamente nell'ambito del gruppo Acea ma non sono destinati alla diffusione.

L'eventuale divulgazione esterna può avvenire per finalità strettamente correlate agli interessi aziendali ed è subordinata all'autorizzazione rilasciata dal responsabile della redazione.

1 Introduzione

1.1 Scopo e campo di applicazione

Alla luce dell'evoluzione normativa in ambito trattamento dei dati personali, Acea SpA è impegnata nella realizzazione ed implementazione di politiche efficaci di tutela dei dati personali dei propri dipendenti, clienti, fornitori, azionisti, stakeholder, partner nonché delle persone i cui dati personali, a vario titolo, vengono trattati dalla Società (di seguito, anche "interessati").

In particolare, il presente documento ha lo scopo di definire le Linee Guida di gestione della Privacy del Gruppo Acea con l'obiettivo di:

- regolare le attività di indirizzo e controllo di Acea SpA ed illustrare obiettivi, principi ed attività afferenti alle tematiche Privacy;
- definire le regole generali per le attività trasversali al Modello di Governance Privacy.

La presente linea guida rientra all'interno del framework integrato adottato dal Gruppo Acea per l'applicazione del regolamento (UE) n. 2016/679 ("General Data Protection Regulation", di seguito "GDPR") relativo alla protezione delle persone fisiche e al trattamento dei dati personali, il quale abroga la direttiva n. 95/46/CE, e relativa regolamentazione locale per il recepimento dello stesso (di seguito, complessivamente, anche la "Normativa applicabile").

La presente Linea Guida si applica ad Acea SpA e alle Società Controllate dirette e indirette di Acea SpA (nel seguito anche "Società del Gruppo") e alle altre società che aderiscono al Modello di Governance Privacy del Gruppo (di seguito, anche "Modello") secondo le modalità indicate al par. 1.2, e che, in qualità di Titolari / Responsabili trattano dati personali e disciplina i ruoli, le responsabilità dei soggetti coinvolti e le attività di controllo relative all'applicazione del *framework* di compliance Privacy.

1.2 Recepimento, distribuzione e aggiornamento

Il presente documento, così come sue eventuali modifiche o integrazioni, è approvato dal Consiglio di Amministrazione della Holding e trasmesso alle Società del Gruppo per l'adozione, nelle rispettive sedi deliberative, da parte dei relativi organi amministrativi. Le disposizioni contenute nel presente documento sono da ritenersi comunque requisiti minimi da adottare; le Società del Gruppo possono prevedere requisiti maggiormente stringenti. Le Società del Gruppo devono comunicare alla Holding, tramite invio dell'apposita delibera, la data di adozione del presente documento.

Per le Società Partecipate, il documento è da considerarsi uno strumento di supporto alla definizione dei propri strumenti normativi. La Holding raccomanda l'esame e la valutazione del presente documento da parte gli organi di amministrazione delle stesse, a cui viene trasmesso da parte di Acea SpA.

La distribuzione avviene con la pubblicazione su rete intranet aziendale e/o con l'invio di comunicazioni tramite posta elettronica.

La Funzione Risk & Compliance è incaricata di fornire adeguato supporto nel processo di aggiornamento della presente Linea Guida e di mantenere aggiornate le eventuali procedure richiamate nella stessa. Gli aggiornamenti alla presente Linea Guida sono proposti all'AD per validazione.

2 Modello di Governance Privacy

Il presente capitolo riporta le linee guida generali volte ad esplicitare gli elementi essenziali del Modello di Governance Privacy Acea, nonché della relativa declinazione all'interno del Gruppo del relativo *framework* di compliance.

Finalità

Il framework di Governance Privacy del Gruppo persegue le seguenti finalità:

- assicurare il rispetto delle vigenti disposizioni in materia di trattamento dei dati;
- definire ruoli e responsabilità delle figure coinvolte nell'applicazione del "Modello Organizzativo Privacy" di Acea di seguito rappresentato, nonché esplicitare il ruolo di indirizzo e controllo di quest'ultima all'interno del Gruppo;
- definire i principi di data protection che dovranno essere implementati ed efficacemente attuati;
- definire il framework di presidi di sicurezza che dovrà essere analizzato e declinato nei rapporti con soggetti (persone giuridiche o fisiche) che per conto di Acea trattano dati personali;
- definire le attività da espletare per l'analisi degli ambiti con potenziali impatti in materia di data protection;
- valutare il rischio e l'impatto sui diritti e le libertà delle persone fisiche connesso al trattamento dei dati personali;
- declinare i requisiti delle informative;
- mettere in atto le azioni necessarie per la tutela dei diritti degli interessati, garantendo la correttezza del processo di gestione e riscontro alle loro istanze;
- definire i requisiti delle reportistiche privacy e dei registri del trattamento dei dati personali;
- Esprimere l'architettura funzionale dei tool automatici di gestione dei sistemi privacy nelle Società.

Acea SpA, in qualità di Holding del Gruppo Acea, esercita una attività di direzione e coordinamento nei confronti delle Società controllate. Per il tramite della Funzione Risk & Compliance, Acea SpA definisce l'architettura del Modello di Governance Privacy del Gruppo e, attraverso l'unità data Protection & Privacy Security, si interfaccia con i Presidi Privacy di Funzione e di Società. Inoltre, l'unità Data Protection & Privacy Security assicura la corretta attuazione del presente Modello monitorando i livelli di rischio associati ai trattamenti effettuati e l'adeguatezza delle misure di protezione attuate, collaborando con i Process Owner nella definizione delle soluzioni di conformità di trattamenti afferenti processi complessi e/o trasversali e su progetti ad elevata complessità.

Di seguito si rappresenta il framework di Governance Privacy del Gruppo ACEA e trattato nel dettaglio nei paragrafi successivi:

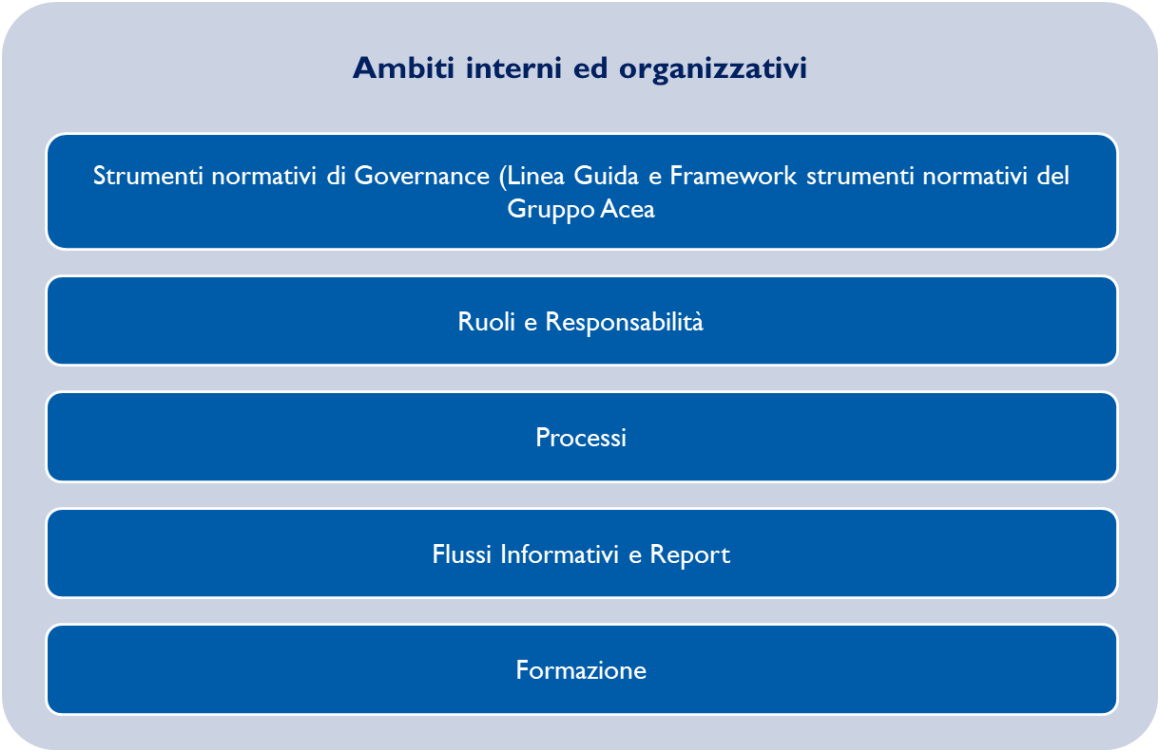

Figura 1: Framework Governance privacy

La presente linea guida, congiuntamente al più ampio *corpus normativo* interno (cfr. par. "Riferimenti interni") specificamente riferito agli "ambiti normativi" di cui alla tabella sopra esposta, è stato definito al fine di assicurare la tutela degli interessati ed il rispetto della normativa applicabile in materia.

2.1 Ambiti interni ed organizzativi

2.1.1 Governance Privacy – Ruoli e Responsabilità

L'architettura di Governance privacy adottata da Acea SpA è definita come segue:

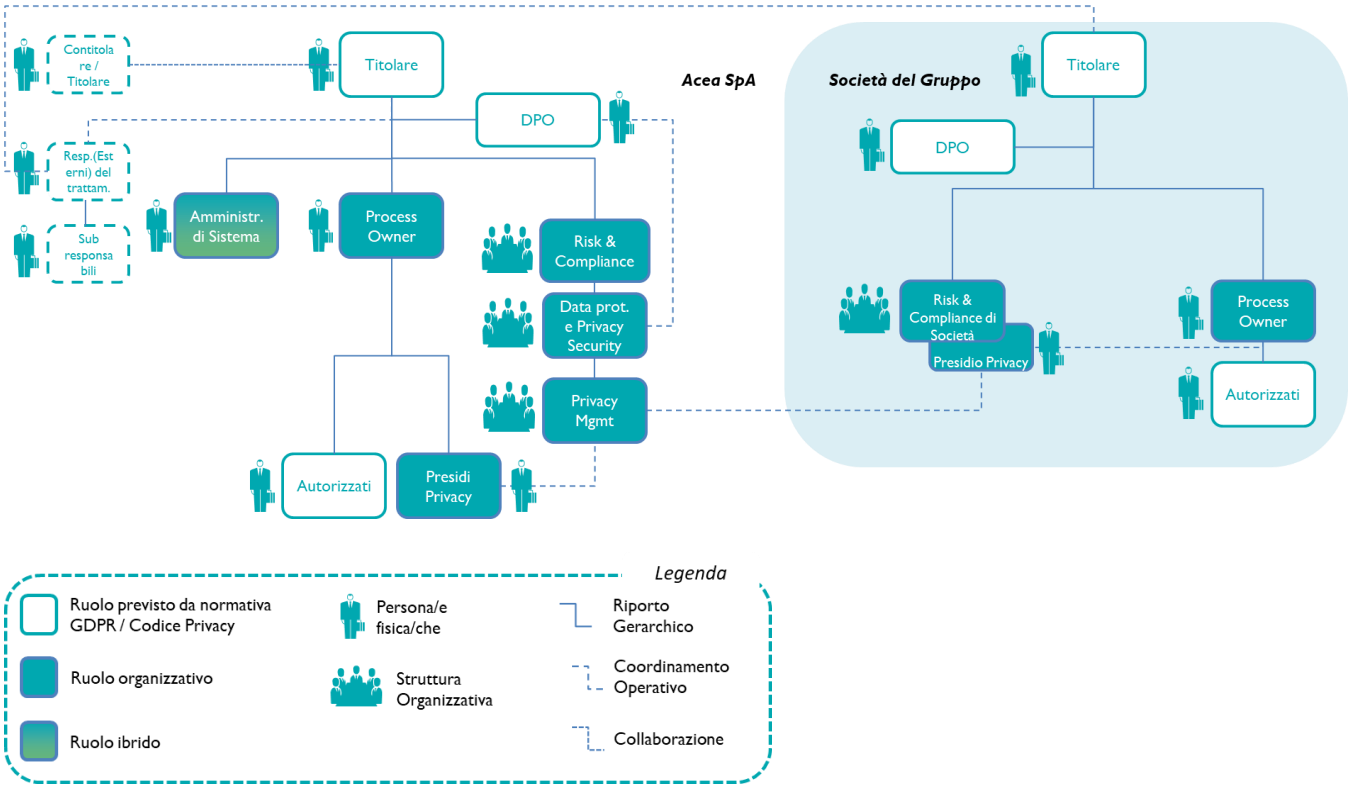

Figura 2: Struttura Governance privacy

In particolare, gli attori principali della struttura di Governance privacy sono:

- **Titolare del trattamento**[1]: La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali. Nel Gruppo Acea, coincide con la persona giuridica ovvero la Legal Entity che sarà responsabile di dare attuazione dei principi riportati all'interno della presente linea guida per il tramite degli strumenti di governance internamente previsti; si esprime per il tramite del rappresentante legali di vertice;
- **Consiglio di Amministrazione di Acea Holding:** Approva le presenti Linee Guida di Governance Privacy al fine di darne efficacia nel Gruppo Acea;

[1] Art. 4. par. 1, n. 7 GDPR

- **Contitolare**[2]: Soggetto che determina congiuntamente al Titolare le finalità e gli strumenti del trattamento di dati personali. Affinché vi sia contitolarità è necessaria la partecipazione di entrambe le parti al trattamento, in modo che l'apporto di ciascuno sia inscindibile dall'altro. I rapporti e le responsabilità delle parti devo essere individuate tramite apposito accordo da rendere disponibile agli interessati;
- **DPO**[3]: Data Protection Officer, designato dal Titolare / Responsabile del trattamento e nominato formalmente mediante atto di nomina per ciascuna Società del Gruppo, ove applicabile, svolge una funzione di vigilanza e garanzia dell'osservanza del Regolamento e della conformità dei trattamenti attuati dai Titolari / Responsabili secondo quanto stabilito dalle presenti linee guida e, più in generale, dalla normativa applicabile, e la relativa attività di indirizzo, verifica e monitoraggio delle attività (es. valutazione dei rischi e DPIA). Il DPO deve assicurare l'indipendenza, la professionalità e la conoscenza specialistica della normativa e delle prassi in materia di protezione dei Dati, nonché della capacità di assolvere i compiti ad esso assegnati dalla Normativa applicabile, garantendo apposito supporto al Titolare anche con riferimento all'analisi degli input provenienti da parte delle Direzioni, Funzioni e Presidi. Il DPO funge, inoltre, da punto di contatto con l'Autorità Garante, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali (ivi incluse notifiche e comunicazioni ad essi inerenti) e contribuisce a definire le misure di sicurezza applicabili / integrabili ai trattamenti di dati personali effettuati all'interno del Gruppo Acea;
- **Funzione Risk & Compliance:** in relazione all'oggetto del presente documento, struttura organizzativa responsabile di progettare, implementare e monitorare le politiche di prevenzione dei rischi di non conformità alla disciplina in materia di protezione dei dati personali.
- **Presidio Privacy:** Persona/e fisica, generalmente individuata/e all'interno delle Unità Risk & Compliance o comunque struttura che svolga mansioni equivalenti, a supporto del Titolare / Process Owner; nella Capogruppo in ciascuna Funzione / Direzione si individua, di norma, un presidio. Coadiuvano Titolare / Process Owner nella realizzazione degli adempimenti privacy inerenti i trattamenti afferenti i processi, con particolare riferimento alle misure tecniche e organizzative di mitigazione dei rischi annessi, assicurando il costante monitoraggio dell'attuazione del trattamento;
- **Process Owner**: Il Process Owner è individuato dal Titolare del trattamento tra i soggetti che, per esperienza, capacità e affidabilità, forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati, ivi compreso il profilo relativo alla sicurezza. Rivestono in azienda il ruolo di Owner di specifici ambiti, individuati puntualmente nel modello organizzativo societario. Inoltre, i Process Owner possono avvalersi, nell'attuazione e gestione degli adempimenti

[2] Art. 26 GDPR.
[3] Artt. 37-39 GDPR.

privacy, del supporto operativo di risorse appartenenti alla propria struttura o ad altre Direzioni / Funzioni / Unità all'interno dell'organizzazione (es. i Presidi privacy);

- **Persona autorizzata al trattamento (c.d. Autorizzati)**[4]: Persona fisica sotto la diretta autorità del Titolare e del Responsabile (se nominato), che, dietro apposita autorizzazione, effettua materialmente le operazioni di trattamento sui dati. Nel Gruppo Acea si identificano in via generale con le persone appartenenti alle unità Organizzative a riporto del Process Owner che operano sulla scorta di istruzioni di contesto fornite dal Titolare del Trattamento come specificate dal Process Owner di riferimento. Pertanto, tutti coloro (dipendenti e collaboratori, etc.) che, a qualsiasi titolo, nell'ambito delle proprie prestazioni lavorative, svolgano operazioni in relazione ad uno o più Trattamenti di Dati, sono da considerarsi Autorizzati in relazione a tali Trattamenti.

  Nell'ambito di progetti e nuove iniziative, per la gestione di eventi di carattere eccezionale o comunque non ordinario ovvero per la realizzazione di trattamenti di dati personali che presentano profili di rischio medio-alti, possono essere individuate specifiche figure di Autorizzati anche non riferibili al Modello organizzativo di Gruppo / Società. In quei casi è opportuno che la designazione sia supportata da istruzioni ad hoc. Le modalità di individuazione / designazione dovranno essere individuate sulla base del modello organizzativo, il dimensionamento, la complessità e il dinamismo societario in essere, (es. lettere individuali; attribuzioni per ruolo; specifiche per progetto / ambito, ecc.);

- **Responsabile esterno del trattamento**[5]: Persona fisica o giuridica che tratta dati personali per conto del Titolare (es. terze parti con cui sussistono rapporti contrattuali per l'espletamento di attività che prevedono il trattamento di dati di interessati di cui Acea SpA / Società del Gruppo è Titolare). Il Titolare può ricorrere unicamente a Responsabili esterni del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative che risultino adeguate con riferimento ad attività di analisi di rischio in ambito. Tale controparte contrattuale (ad esempio fornitori, appaltatori, ecc.), con la quale risulta sottoscritto apposito Data Protection Agreement (DPA), dovrà rispettare i criteri, le finalità e le modalità di trattamento dei dati personali previsti dalla Normativa applicabile e da eventuali istruzioni impartite dal committente, nonché controlli e vigilanza specifica sulle attività del Responsabile esterno del Trattamento. Nel Gruppo Acea, i Responsabili esterni del trattamento possono essere anche Società del Gruppo, allorché eroghino servizi / prestazioni che comportano il trattamento dati Personali per conto della Società Titolare. In tali casistiche tra Società Titolare e Società Responsabile deve essere sottoscritto apposito contratto di Servizio con annesso specifico DPA;

[4] art. 4, n. 10 e 29 GDPR, (Codice Privacy novellato dal D.lgs. 101/2018, art. 2 *quaterdecies*).
[5] Artt. 4, n° 8) e 28 GDPR.

- **Amministratore di Sistema[6]:** È designato Amministratore di Sistema (di seguito, anche "AdS") colui che configura e gestisce un sistema di elaborazione dati o sue componenti fisiche o virtuali, presso la sede o presso terzi. In particolare, lo stesso, è identificato come una figura professionale che, in ambito informatico, mantiene, configura e gestisce un sistema di elaborazione dati o sue componenti, ivi inclusi sistemi software complessi (e.g. i sistemi Enterprise Resource Planning - system administrator), ossia una base dati (database administrator), ovvero reti e apparati di telecomunicazione di sicurezza (network administrator). Tale figura, è chiamata, inoltre, a gestire specifiche fasi (attività tecniche come backup, recovery, manutenzione hardware, ecc.) che possono comportare elevate criticità rispetto alla protezione dei dati personali. Inoltre, l'attribuzione delle funzioni di AdS segue ad una previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, ivi compreso il profilo relativo alla sicurezza. Tale designazione deve indicare in maniera analitica gli ambiti di operatività consentiti al profilo assegnato e deve essere predisposta una lista degli amministratori di sistema e delle relative funzioni attribuite. È necessario, inoltre, che con cadenza almeno annuale, siano svolte attività di verifica circa il corretto operato degli amministratori di sistema. Sono infine adottati sistemi idonei a garantire la registrazione degli accessi logici ai sistemi di elaborazione / archivi elettronici che abbiano caratteristiche di completezza, inalterabilità ed integrità;
- **Unità Data Protection & Privacy Security:** Struttura organizzativa responsabile di fornire indirizzi attuativi in materia di privacy a tutte le Direzioni / Funzioni e Presidi aziendali (ivi inclusi i Process Owner e gli Autorizzati), attraverso il monitoraggio dei livelli di rischio e l'idoneità delle misure di sicurezza associate ai trattamenti dei dati, collaborando con i Process Owner nella definizione delle soluzioni di conformità di trattamenti afferenti processi complessi e/o trasversali e su progetti ad elevata complessità In tal contesto, coordina l'attività interna di compliance in tema di privacy, assicurandone l'uniformità e l'efficienza, e valuta le misure idonee per incorporare i requisiti normativi nei processi aziendali, sviluppando proposte e interventi per modifiche e aggiornamenti di Linee Guida, procedure, misure di sicurezza, ecc. Inoltre, assicura l'effettiva ed efficace attuazione delle politiche di governo dei rischi connessi con il trattamento dei dati personali in Acea SpA (es. privacy screening, verifica esecuzione di analisi dei rischi e valutazioni di impatto, rispetto dei requisiti di privacy by design e privacy by default, adeguamenti normativi, ecc.) e fornisce supporto alle attività in capo al DPO di Acea SpA;
- **Unità Privacy Management:** Struttura che interfaccia e coordina i Presìdi Privacy nella gestione delle attività del programma di compliance, dei relativi adempimenti normativi e contrattuali, declina

[6] Provvedimento Garante 27 novembre 2008

e/o attua operativamente gli indirizzi in materia di privacy per assicurare la compliance al Modello e alla normativa vigente, presidia il processo di gestione delle richieste provenienti da parte degli interessati per la Holding e le Società controllate.

2.1.2 Governance Privacy – Processi

In virtù della pervasività della materia trattata all'interno del presente documento, si ravvisa che ciascun processo aziendale potrebbe essere potenzialmente rilevante, qualora nell'ambito dello stesso si configuri un trattamento di dati personali.

2.1.3 Governance Privacy – Flussi informativi e report

I Presidi privacy di Società del Gruppo e quelli di Funzione / Direzione all'interno della Holding / Società del Gruppo – nello svolgimento delle attività finalizzate all'attuazione e implementazione del Modello di Governance Privacy – sono coordinati dall'unità Data Protection & Privacy Security che potrà adottare qualsiasi iniziativa che ritenga necessaria per assicurare l'efficace applicazione, l'aggiornamento e il miglioramento del Modello stesso.

I Presidi privacy, in via esemplificativa e non esaustiva:

- assicurano con cadenza almeno semestrale una comunicazione formale verso l'unità Data Protection & Privacy Security sullo stato di maturità della compliance privacy relativa ai processi da loro presidiati;
- forniscono insieme alla comunicazione presentata al punto precedente la documentazione esplicativa volta a comprovare lo stato di conformità dichiarato;
- possono ingaggiare l'unità Data Protection & Privacy Security per le attività con impatto privacy che ritengono maggiormente rischiose al fine di ottenere uno specifico indirizzo di compliance;
- informano l'unità Data Protection & Privacy Security di qualsiasi evento potenzialmente rilevante ai sensi della compliance privacy e ai fini dell'applicazione del Modello (ad es.: violazioni dei dati personali; sviluppo di nuove iniziative secondo le logiche di privacy by design e by default; gestione delle richieste degli interessati; analisi dei rischi svolte sui trattamenti; avanzamento delle azioni di rientro definite; eventuali violazioni o potenziali criticità del Modello; pareri interni rilasciati a Direzioni / Uffici interni della Società/struttura in merito alla conformità di specifiche condotte con la compliance GDPR);
- informano l'unità Data Protection & Privacy Security circa l'introduzione delle misure migliorative, correttive e/o di aggiornamento del Modello (ad esempio, adozione di Policy / Linee Guida, previsione

di specifici presidi di controllo all'interno dei processi maggiormente esposti a rischi privacy; aggiornamento periodico della formazione per il personale della Società o a seguito di nuove assunzioni e/o di mutamenti significativi negli organici interni che incidano sul profilo / area di rischio del personale; aggiornamento su novità normative e/o giurisprudenziali aventi un significativo impatto sull'attività della Società).

Il DPO riferisce in merito allo stato di aggiornamento della compliance GDPR con cadenza annuale, salvo esigenze specifiche, ai seguenti organi: Titolare del trattamento, Comitato controlli e rischi, Collegio sindacale e Organismo di Vigilanza.

2.1.4 Governance Privacy – Formazione

In linea con quanto disposto dalla normativa vigente, il DPO di Società del Gruppo è impegnato nella sensibilizzazione e nella formazione del personale che partecipa ai trattamenti di dati personali ed alle connesse attività di controllo. In tal contesto, al fine di diffondere, all'interno dell'azienda, una cultura della privacy e fornire gli strumenti adeguati per assicurare il rispetto della normativa in materia, le competenti strutture di Società del Gruppo hanno sviluppato, dietro input e sotto il coordinamento del DPO di Società del Gruppo, campagne di formazione e iniziative specifiche sui temi principali e più rilevanti in materia di privacy.

2.2 Ambiti Normativi

2.2.1 Gestione dell'informativa e del consenso

Informative agli interessati

Il GDPR riprende e rafforza il diritto alla trasparenza del trattamento, prescrivendo ai Titolari di fornire agli interessati informazioni rapide, esatte, chiare e semplici, intelligibili e facilmente accessibili, sia prima del trattamento, con l'informativa, che successivamente, qualora gli interessati si rivolgano al Titolare per far valere i propri ulteriori diritti specificati dalla normativa applicabile.

Il Gruppo Acea, pertanto, attua le seguenti attività:

- garantisce che gli interessati siano informati, in modo preventivo, consapevole e trasparente dei trattamenti relativi ai propri dati personali;
- indica, all'interno della informativa sul trattamento le finalità del trattamento, le modalità esecutive dello stesso, la tipologia di dati trattati, le categorie di soggetti interni ed esterni alla Società abilitati ad accedere ai dati dell'interessato, il tempo di conservazione (*retention*) dei dati, gli estremi identificativi del Titolare (Acea SpA o altre Società del Gruppo Acea), indicazione di eventuali trasferimenti verso Paesi Terzi (extra SEE – Spazio Economico Europeo), nonché i diritti degli interessati e i dati di contatto del DPO, ove nominato. L'Informativa deve essere fornita nel momento in cui i dati sono raccolti, se i dati sono raccolti presso l'interessato (rif. Art. 13 GDPR) e prima dell'espressione del relativo consenso (ove richiesto), nonché, nel caso di raccolta presso terzi (rif. Art. 14 GDPR), entro un termine ragionevole dall'ottenimento degli stessi, ma al più tardi entro un mese, ovvero al primo contatto utile con l'interessato.

Istruzioni e consenso

Nel rispetto di quanto previsto dalla Normativa applicabile, che riconosce tra i presupposti giuridici che rendono lecito il trattamento di dati personali il consenso espresso dell'interessato, il Gruppo Acea osserva che lo stesso debba avere le caratteristiche di una manifestazione:

I. ***libera***, quindi non condizionato da situazioni che potrebbero obbligare l'interessato a fornire dati personali;
II. ***specifica***, ovvero riferita alle singole e specifiche modalità e finalità del trattamento per cui la legge impone la richiesta del consenso;
III. ***informata***, ovvero che avvenga a seguito di una informativa chiara;
IV. ***inequivocabile***, verificabile e revocabile.

Inoltre, la Normativa applicabile (rif. Art. 6 – Liceità del trattamento - GDPR) dispone che il Titolare possa trattare senza la raccolta del consenso dell'interessato dati personali al sussistere delle seguenti ulteriori basi giuridiche diverse dal consenso:

- trattamento necessario per adempiere a un obbligo contrattuale ovvero ad un obbligo di legge e/o regolamentare;
- legittimo interesse del Titolare;
- difesa di un diritto in giudizio o nelle fasi di precontenzioso;
- dati pubblici e/o liberamente accessibili purché utilizzati dal Titolare per gli stessi scopi per cui sono stati pubblicati.

Diritti degli Interessati

Il Gruppo Acea assicura il rispetto dei Diritti degli Interessati, implementando le azioni necessarie per garantire agli stessi l'esercizio effettivo ed agevole dei relativi diritti.

Qualora un interessato proceda ad esercitare i propri diritti, mediante apposita istanza / richiesta, la figura preposta all'espletamento di tale attività è tenuta a dare tempestivamente seguito alla stessa.

Rilevato che tra i diritti dell'interessato rientra anche quello di Revoca del consenso, il GDPR, con gli articoli dal 15 al 22 (a cui si rimanda per gli aspetti di dettaglio), si dedica specificamente alla illustrazione degli ulteriori diritti dell'interessato e delle modalità con le quali i diritti possono essere esercitati.

In particolare, i diritti riconosciuti agli Interessati sono i seguenti:

- *Diritto di accesso;*
- *Diritto di rettifica;*
- *Diritto alla cancellazione;*
- *Diritto di limitazione del trattamento;*
- *Obbligo di notifica in caso di rettifica, cancellazione o limitazione;*
- *Diritto alla portabilità dei dati;*
- *Diritto di opposizione;*
- *Diritto di essere informato (ed eventualmente opporsi) della sussistenza di un processo decisionale automatizzato (compresa la profilazione).*

Anche al fine di permettere agli Interessati di poter esercitare i propri diritti in ambito, il Gruppo Acea ha definito e formalizzato uno specifico processo di gestione delle richieste provenienti da parte degli interessati stessi, in modo tale da garantire agli interessati un canale dedicato alle loro istanze e l'accesso diretto al DPO, ove nominato.

Per il dettaglio delle modalità operative, dei ruoli e delle responsabilità con cui tali richieste siano evase, si rimanda alla specifica procedura.

2.2.2 Gestione degli eventi di data breach

Il Gruppo Acea, ai sensi della normativa applicabile, è tenuto a porre in essere tutte le misure tecniche ed organizzative volte ad assicurare la protezione dei dati personali contro potenziali violazioni e conseguente perdita, distruzione o danneggiamento dei dati stessi (Data Breach).
In particolare, gli eventi di Data Breach, o violazione dei dati, possono essere suddivisi in tre principali categorie:

- *violazione di confidenzialità*, ossia una divulgazione non autorizzata / accidentale di dati o accesso agli stessi da parte di soggetti privi di autorizzazione;
- *violazione di integrità*, ossia una alterazione non autorizzata o accidentale di dati;
- *violazione di disponibilità*, ossia una perdita della possibilità di accesso o una distruzione, accidentale o non autorizzata, di dati.

Pertanto, il Gruppo Acea prevede che i soggetti coinvolti nel trattamento dei dati personali nell'espletamento delle proprie mansioni, agiscano con la massima diligenza al fine di prevenire episodi di violazione dei dati personali, configurabili in:

- violazioni involontarie od accidentali, quali, ad esempio: smarrimento di un supporto elettronico (es. chiavetta USB) o cartaceo (es. documento), distruzione accidentale di documenti, fornitura dati a persona diversa da contraente / cliente;
- violazioni volontarie, quali, ad esempio: furto di supporti elettronici o cartacei contenenti dati personali, accesso ai dati ed utilizzo illecito da parte di un dipendente o soggetto interno all'organizzazione autorizzato, alterazione dei dati da parte di soggetti non autorizzati.

Inoltre, dal momento che la violazione dei dati personali può avvenire anche a seguito di eventi accidentali, il Gruppo Acea garantisce, oltre al rilascio di apposite istruzioni in ambito, l'erogazione di apposita attività di formazione e *awareness* per una corretta gestione dei dati personali e la tempestiva segnalazione qualora se ne riscontrasse una violazione.

Nell'ambito dell'attività di prevenzione e gestione degli eventi anomali, degli incidenti e degli attacchi informatici, il Gruppo Acea definisce e implementa processi, procedure e strumenti operativi allo scopo di individuare chiaramente ruoli e responsabilità e prevedere un efficace sistema di comunicazione fra tutte le strutture coinvolte al fine di ripristinare la normale operatività di un servizio il più velocemente possibile,

minimizzando l'impatto degli eventi dannosi sull'operatività del business e assicurando livelli di servizio minimi. A tali obiettivi di continuità del servizio si aggiunge il rispetto dei principi fondamentali della sicurezza delle informazioni quali la confidenzialità, l'integrità e la disponibilità.

Per ottemperare alle finalità sopra riportate, il Gruppo Acea identifica attività di prevenzione, individuazione degli eventi anomali e di reazione agli incidenti, di monitoraggio e reportistica e di formazione in materia di sicurezza, tenendo conto di quanto emerso periodicamente dai report sugli eventi anomali, sugli incidenti e attacchi.

Inoltre, il Gruppo Acea ha implementato tecniche e sistemi di monitoraggio e allarmistica proattiva al fine di rilevare gli eventi anomali in maniera tempestiva e sulla base di una preventiva identificazione del perimetro dei sistemi sottoposti al controllo.

Il Gruppo Acea dispone che, nel caso in cui chiunque all'interno dell'Azienda venga a conoscenza direttamente e/o indirettamente (es. su indicazione di un Incaricato, di una Persona di Acea e/o di un terzo) di una possibile Violazione di Dati Personali (anche solo sospetta), tale soggetto comunichi tempestivamente alle strutture competenti tale evento.

A seguito della ricezione di una segnalazione di un avvenuto o potenziale *data breach*, le strutture competenti della Società si attivano per valutare se ricorrono i presupposti per considerare l'evento comunicato come Violazione di Dati Personali (o *data breach*) e porre in essere tutte le attività necessarie, tra cui la registrazione dello stesso nella documentazione apposita. La notifica deve essere presentata, a cura del Titolare del trattamento, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, al Garante per la protezione dei dati personali a meno che sia improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche.

Per il dettaglio delle modalità operative e dei ruoli e responsabilità con cui la valutazione degli eventi e le successive attività (es. notifica alle Autorità; notifica ai soggetti interessati ecc.) sono gestite si rimanda alla specifica procedura in ambito *pro tempore* vigente.

2.2.3 Gestione della Data Retention

I dati personali, come anche i documenti e le informazioni conservate dalle Società del Gruppo Acea, rappresentano un importante *asset* aziendale e richiedono una gestione appropriata e mirata, che preservi il loro valore nel tempo, ne garantisca la disponibilità e l'idoneità all'utilizzo dove e quando necessario e protegga gli interessi dei soggetti interessati, dell'azienda, dello *staff* e degli *stakeholder*.

Il Gruppo Acea garantisce l'adozione e la puntuale applicazione dei principi di riferimento in ambito *data retention* dettati dalla Normativa applicabile, al fine di garantire che l'identificazione degli Interessati sia consentita per un arco di tempo non superiore al conseguimento delle finalità per le quali i dati stessi sono raccolti e trattati. Di seguito sono sintetizzati i summenzionati principi:

- i dati personali raccolti devono essere adeguati, pertinenti e limitati a quanto necessario per le finalità per cui sono stati raccolti;
- i dati personali devono essere conservati per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati;
- i sistemi informativi e gli applicativi devono essere configurati riducendo al minimo l'utilizzo dei dati personali, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi o opportune modalità che permettano di identificare l'interessato solo in caso di necessità;
- i dati personali devono essere trattati in modo da garantirne un adeguato livello di sicurezza e riservatezza, impedendone l'accesso o l'utilizzo non autorizzato;
- al termine del periodo di conservazione consentito, i dati personali devono essere anonimizzati (o de-identificati) in maniera irreversibile o eliminati, a meno che sia stato raccolto il consenso espresso dell'interessato, ovvero la conservazione per tempi più lunghi sia ammissibile / richiesto da una norma di legge.

Al fine di rispettare i principi sopra descritti il Titolare del trattamento, eventualmente con il supporto delle competenti strutture in materia di *data protection*, deve declinare e definire i tempi di conservazione dei dati in considerazione delle finalità del relativo trattamento (cfr. All. B). La definizione del periodo di conservazione è indicata all'interno del relativo Registro dei Trattamenti.

2.2.4 Privacy by design e privacy by default

Il Regolamento UE 679/2016 definisce che la tutela dei dati personali nelle attività di trattamento debba essere considerata ex ante, e cioè "a monte" di ogni attività di trattamento, inserendosi nelle valutazioni preliminari di ogni attività / processo / progetto / servizio da avviare nell'operatività aziendale (principio di "*Privacy by Design* e *Privacy by Default*"). In tal contesto, la Società assicura la protezione dei dati fin dalla progettazione e per impostazione predefinita garantendo che, nell'ambito di qualsiasi iniziativa, i sistemi informativi utilizzati e i processi adottati soddisfino i suddetti principi.

Più in dettaglio, al momento di determinare i mezzi del trattamento dei dati e all'atto del trattamento stesso, è previsto che il Titolare metta in atto misure tecniche e organizzative adeguate volte ad attuare in modo

efficace i principi di protezione dei dati, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti della normativa applicabile in tale ambito, tutelare i diritti degli interessati ed agire conformemente al principio di *accountability*.

I principi summenzionati, che si applicano a qualsiasi iniziativa aziendale e ogniqualvolta occorrano modifiche a quanto già in essere all'interno dell'azienda, consistono nel garantire, per impostazione predefinita (*privacy by default* che il Titolare tratti solo i dati personali nella misura necessaria e sufficiente (*minimizzazione*) per le finalità previste e per il periodo strettamente necessario a tali fini (*limitazione della conservazione),* mettendo in atto misure tecniche ed organizzative per la protezione dei dati a partire dalla fase di progettazione (*privacy by design*) per tutte le iniziative, processi aziendali, servizi offerti, sistemi informatici, soluzioni innovative e ogni altro progetto che preveda il trattamento di dati personali.

Al verificarsi di un cambiamento organizzativo e/o dell'introduzione di nuovi processi e/o progetti (es. introduzione di un nuovo processo aziendale o modifica a un processo già in essere, applicazione di una nuova tecnologia; ecc.) con impatto sui trattamenti effettuati, le Società del Gruppo Acea devono prevedere una serie di attività che permettano di considerare in maniera adeguata, e fin dalle fasi iniziali, ogni modifica o iniziativa che potrebbe avere un impatto sulla gestione dei dati personali nel Gruppo e sui diritti e libertà degli interessati. Pertanto, in tali casi, saranno preventivamente valutati gli eventuali impatti ed analizzati i relativi rischi sui diritti e libertà degli interessati secondo le metodologie definite, con particolare focus sulla rischiosità, intesa come *lesione di diritti* e *libertà degli interessati*, dell'eventuale trattamento di dati personali.

In virtù dei risultati emersi, le Società del Gruppo devono implementare adeguate misure tecnico – organizzative a presidio del trattamento stesso, coinvolgendo, ove necessario le diverse strutture coinvolte nel trattamento (security, gestione dei sistemi informativi ecc..).

Il Gruppo Acea garantisce che le attività di valutazione in ambito *privacy by design* e *privacy by default* siano opportunamente documentate e tracciate. Inoltre, le attività di verifica e monitoraggio sono espletate mediante, a titolo esemplificativo:

- audit sui fornitori;
- privacy screening (cfr. All. C);
- analisi dei rischi (cfr. All. F);
- verifiche sulle impostazioni di privacy by design (cfr. All. D) e scheda sul trattamento dei dati personali (cfr. All. I).

Principi di base per la progettazione di nuove iniziative

Di seguito sono riportati i requisiti di base che le strutture competenti / coinvolte devono tenere in considerazione durante le fasi di progettazione di nuove iniziative aziendali.

Tali requisiti si suddividono nelle due seguenti categorie, a seconda dell'ambito su cui si focalizzano:

- Requisiti orientati al dato:
  - *Minimizzazione dei dati*: la quantità di dati personali, legittimamente raccolti ed elaborati, deve essere limitata ai soli dati strettamente necessari per il perseguimento delle finalità prestabilite;
  - *Nascondere e proteggere*: è necessario prediligere l'utilizzo di misure a di protezione dei dati, quali, ad esempio, la crittografia;
  - *Separare*: si dovrebbe prevedere la separazione tra l'elaborazione e l'archiviazione dei dati personali relativi alla stessa persona fisica in diverse fonti dati, in modo da ridurre la possibilità di creare profili completi della persona;
  - *Aggregare*: i dati personali dovrebbero essere raccolti e trattati, ove possibile, in forma aggregata, al fine di salvaguardare la tutela dei diritti dell'interessato.
- Requisiti relativi al processo:
  - *Informare:* il nuovo servizio o sistema deve essere progettato e configurato in modo tale che l'interessato sia sufficientemente informato sul funzionamento e sulle modalità di elaborazione dei propri dati personali. Qualora sia previsto un processo decisionale automatizzato di dati personali, l'interessato deve essere informato su come tale processo viene svolto e della facoltà di opporsi ad esso. L'interessato deve pertanto essere informato sulle modalità di esercizio dei diritti allo stesso riconosciuti dalla Normativa applicabile;
  - *Controllare:* l'interessato ha il diritto di mantenere il controllo sui propri dati personali. Ciò include il diritto di accesso, nonché l'aggiornamento e/o cancellazione dei propri dati. Nei casi in cui sia previsto un processo decisionale automatico o vengano prese decisioni senza l'intervento umano, l'interessato potrebbe, inoltre, richiedere l'elaborazione manuale dei dati;
  - *Documentazione:* il nuovo servizio o sistema deve essere progettato in modo che la documentazione relativa alla salvaguarda dei diritti dell'interessato e alla conformità alla normativa sia facilmente disponibile in caso di audit o di ispezioni dell'Autorità;
  - *Dimostrazione:* il Titolare del trattamento deve essere in grado di dimostrare che nel nuovo servizio o sistema o altra iniziativa siano stati implementati i requisiti della Normativa applicabile.

2.2.5 Gestione delle attività di trattamento

In ottemperanza a quanto dettato dalla Normativa applicabile, le Società del Gruppo Acea si sono dotate di apposito "Registro delle attività di trattamento", redatto ed aggiornato dai competenti soggetti individuati all'interno delle Società.

Il Registro rappresenta lo strumento che le Società del Gruppo Acea hanno adottato per la compliance al GDPR e per il censimento delle attività di trattamento dei dati personali svolte sotto la responsabilità di ciascun Titolare (cfr. All. E).

Tale strumento fornisce un quadro aggiornato dei trattamenti sui dati personali svolti all'interno dell'azienda e, come tale, deve essere aggiornato periodicamente a fronte di cambiamenti organizzativi o di processo, in linea con quanto dettagliato all'interno della procedura di riferimento.

Il Registro è conservato in formato elettronico e, su richiesta, il Titolare del trattamento lo mette a disposizione delle Autorità di controllo.

Acea SpA, in qualità di fornitore di servizi verso le Società del Gruppo - con le quali stipula appositi contratti di servizio e, quindi, nel ruolo di Responsabile Esterno del Trattamento - mantiene un distinto registro delle attività relative ai trattamenti svolti per conto dei Titolari che periodicamente aggiorna e condivide su richiesta.

Elaborazione dei Registri delle attività di trattamento

Il registro viene redatto attraverso il coinvolgimento di referenti aziendali degli ambiti di *business* e delle società in ambito. Per ciascuna società sono stati identificati i processi GDPR rilevanti verticali e trasversali, le strutture aziendali e i referenti da coinvolgere. A partire dai processi, sono stati identificati i trattamenti che successivamente sono stati censiti all'interno del registro dei trattamenti.

Aggiornamento e manutenzione dei Registri

Per mantenere la compliance al GDPR e preservare la validità delle informazioni contenute nel Registro, il Gruppo Acea prevede che tale strumento sia riesaminato ed eventualmente aggiornato con cadenza periodica, almeno annuale, da parte del *Process Owner* di rifermento, con il supporto dei Presidi Privacy.

In particolare, il Registro deve essere riesaminato e aggiornato a fronte di variazioni delle informazioni in esso contenute o di altre circostanze esterne che possano avere impatti sui trattamenti e sulle informazioni riportate. Ad esempio, l'aggiornamento del Registro dei trattamenti di Acea SpA risulta necessario nei seguenti casi:

- modifiche normative o nuovi vincoli introdotti da normative esterne o regolamenti;
- cambi organizzativi (ad es. cambio di ruolo del referente aziendale identificato per il trattamento);

- modifiche che coinvolgono i processi GPDR rilevanti (ad es. modifica della finalità di trattamento, introduzione di una nuova iniziativa di business che prevede il trattamento di dati personali, variazione delle categorie di dati trattati e delle operazioni di trattamento svolte).

2.2.6 *Gestione del trasferimento dei dati*

Il Gruppo Acea garantisce il trasferimento dei dati personali di cui le Società sono titolari in maniera sicura, nel rispetto del GDPR e della relativa normativa di attuazione.

Trasferimento a soggetti terzi interni al perimetro UE

In particolare, il trasferimento di dati di cui le Società del Gruppo Acea sono titolari avviene nel rispetto dei seguenti principi e regole:

- rilascio di un'informativa all'interessato, che indichi almeno le categorie di destinatari del dato e le finalità per le quali tali dati sono comunicati;
- sottoscrizione di un apposito DPA (Data Processing Agreement), integrativa al contratto, con il fornitore / Soggetto terzo che individui, tra le altre cose, la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento, nonché le modalità del trattamento e le relative misure di sicurezza da adottare;
- adozione di misure tecnico organizzative adeguate al fine di proteggere la riservatezza, integrità e disponibilità di tali dati durante il processo di trasferimento;
- il trasferimento a soggetti terzi esterni al perimetro UE o organizzazioni internazionali[7] è ammesso quando lo stesso sia rivolto verso Paesi ricompresi nell'elenco dei quelli che, ai sensi di una "decisione di adeguatezza" della Commissione Europea, presentino un livello di protezione adeguato tale da fornire idonee garanzie per i diritti degli interessati[8];
- sia disciplinato, a livello contrattuale, tra le parti tramite l'inserimento di apposite clausole standard adottate dalla Commissione Europea (SCC), ovvero tramite apposite "Norme Vincolanti di Impresa" (BCR – Binding Corporate Rules);
- sia giustificato da una previa acquisizione del consenso specifico al trasferimento da parte dell'interessato o dalle altre deroghe in specifiche situazioni previste dall'art. 49 GDPR.

[7]Organizzazione internazionale (Art. 4, 26 GDPR): un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

[8] Per maggiori informazioni, si rimanda al link: https://www.garanteprivacy.it/home/provvedimenti-normativa/normativa/normativa-comunitaria-e-intenazionale/trasferimento-dei-dati-verso-paesi-terzi.

Tecnologie di cloud computing

Il Gruppo Acea intende garantire un livello adeguato di protezione dei dati personali nell'utilizzo di tecnologie *cloud*, avvalendosi di *Cloud Provider* che garantiscono elevati standard di sicurezza e di protezione dei dati personali degli utenti coinvolti.

Caratteristica essenziale del *Cloud* è che l'accesso ai suoi servizi e le prestazioni fornite possono essere utilizzate attraverso l'utilizzo di Internet. In tale ambito, il Gruppo Acea rispetta le *Linee guida dello European Data Protection Supervisor* relative all'uso dei servizi di *cloud computing* da parte delle Istituzioni europee, le quali pongono l'attenzione su alcuni punti, affermando i seguenti tre principi chiave da tenere presente nella valutazione e nella scelta di soluzioni *cloud*:

- localizzazione dei server e delle infrastrutture (obbligo di valutazione dell'adeguatezza dei diversi ordinamenti e delle misure che è necessario adottare a seconda dei Paesi, prediligendo opzioni *EU based* all'atto della scelta del fornitore);
- circostanza che il Titolare del trattamento (e quindi le Istituzioni UE) devono avere una piena conoscenza del sistema di governance che regola i diversi tipi di *Cloud*;
- necessità del Titolare del trattamento di avvalersi di fornitori (Responsabili del trattamento) che rispettano gli obblighi previsti dal GDPR, anche mediante la verifica del possesso di certificazioni in ambito.

2.2.7 Gestione delle misure di sicurezza e valutazione dei rischi

Misure di sicurezza integrate

Acea SpA, in qualità di Holding di Gruppo, suggerisce misure di sicurezza per ambito, contribuisce alla loro implementazione e vigila sul relativo rispetto. Il Gruppo Acea, in linea con i princìpi generali di sicurezza delle informazioni, con le strategie di business, gli obblighi di legge vigenti ed il profilo di rischio aziendale, preserva la sicurezza dei dati personali (di cui è Titolare e Responsabile), delle informazioni, dei dati e degli asset aziendali.

Il Gruppo Acea provvede a:

- mettere in atto, ove possibile, misure di crittografia e cifratura dei dati personali;
- preservare la riservatezza, integrità, disponibilità delle informazioni trattate e dei servizi di trattamento, definendo criteri adeguati e modalità di gestione nonché di utilizzo delle informazioni in conformità alle norme di legge e a regolamenti interni ed esterni (e garantendo che il trattamento delle informazioni avvenga nel rispetto dei diritti e degli interessi di personale, clienti e partner commerciali);

- promuovere l'adozione di misure di sicurezza adeguate alla salvaguardia dei diritti e delle libertà delle persone fisiche i cui dati vengono trattati, mitigando il livello di rischio e attuando misure di prevenzione e mitigazione dei rischi / minacce sulla base delle risultanze dell'analisi dei rischi e valutazione d'impatto;
- promuovere l'adozione di misure che garantiscano il ripristino tempestivo della disponibilità e dell'accesso dei dati personali in caso di incidente fisico o tecnico;
- definire formalmente le modalità operative per valutare e verificare l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento, tenendo conto dei rischi dovuti alla distruzione, perdita, modifica, divulgazione non autorizzata o all'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati;
- garantire altresì la tracciatura di tutti gli eventi di sicurezza, eseguiti o tentati, al fine di monitorare l'adeguatezza delle misure adottate e definirne il miglioramento;
- attribuire al proprio personale (secondo il principio dell'accountability) in modo non ambiguo e per l'intero ciclo di vita delle informazioni, i ruoli e le responsabilità nell'ambito della gestione dei processi in esame.

Le misure di sicurezza adottate dal Gruppo Acea, revisionate periodicamente (e su base almeno annuale), possono essere ricondotte alle seguenti categorie (cfr. All. A per una prima mappatura ad ampio spettro delle misure presenti alla data di pubblicazione della LG):

- *Misure di sicurezza logica,* ovvero misure di sicurezza per la protezione degli asset tecnologici (es. dispositivi mobili, sistemi e reti) per la tutela dei dati personali, nonché delle informazioni in essi contenuti*;*
- *Misure di sicurezza fisica,* ovvero misure per prevenire l'accesso non autorizzato alle sedi ed ai singoli locali aziendali, nonché garantire adeguati livelli di sicurezza alle aree e agli asset mediante i quali vengono gestiti o custoditi i dati personali e le informazioni, a tutela del proprio patrimonio*;*
- *Misure procedurali,* ovvero la definizione di un *framework* documentale per la gestione degli aspetti legati alla sicurezza logica e fisica degli asset ovvero dei dati personali e delle informazioni in essi contenute*;*
- *Misure organizzative,* ovvero la declinazione di ruoli e responsabilità, provvedendo a garantire nel continuo che l'operato del personale sia conforme alle politiche di sicurezza dei dati personali e delle informazioni definite.

Valutazione del rischio: metodologia e metriche

Le Società del Gruppo Acea, in qualità di Titolari e/o di Responsabili del trattamento, considerano la protezione dei dati personali un aspetto rilevante e integrato all'interno delle iniziative aziendali. In coerenza a quanto previsto dalla Normativa applicabile e dalle indicazioni del Garante della Privacy, l'approccio utilizzato è orientato all'analisi e *valutazione del rischio*.

A tale scopo, le Società del Gruppo Acea devono prevedere una serie di attività che permettano di considerare, valutare e mitigare in maniera adeguata, e fin dalle fasi iniziali, i rischi sottesi ad ogni trattamento che potrebbero avere un impatto sulla gestione della privacy del Gruppo.

In tale ottica, vengono adottate due metodologie di valutazione del rischio, come di seguito descritte:

- *Analisi e valutazione del rischio*:
  metodologia di analisi e valutazione finalizzata a misurare l'adeguatezza delle misure tecniche ed organizzative tramite la rilevazione del rischio, sia a livello inerente che residuo, per ciascun trattamento censito all'interno del registro dei trattamenti. Essa ha le seguenti peculiarità:
  - mira a valutare impatti e probabilità di accadimento;
  - si applica a tutti i trattamenti dei dati personali;
  - deve essere ripetuta con periodicità almeno annuale.
- *Data Protection Impact Assessment (DPIA):*
  metodologia di analisi degli impatti volta ad individuare e valutare i trattamenti che presentano, potenzialmente, un **rischio elevato per i diritti e le libertà delle persone fisiche**. Essa è caratterizzata dai seguenti aspetti:
  - valuta gli impatti sui diritti e le libertà degli interessati;
  - è svolta sui trattamenti che presentano potenzialmente *elevato impatto data protection* sui diritti e le libertà degli interessati.

Di seguito sono riportate le principali differenze intercorrenti tra le due metodologie di valutazione del rischio, nonché gli ambiti di responsabilità e di competenza dei soggetti coinvolti.

Figura 2: Differenze tra analisi e valutazione del rischio e DPIA

Nel complesso, le due tipologie di analisi dei rischi possono essere considerate complementari, fermo restando che, mentre l'analisi dei rischi deve essere svolta sulla totalità dei trattamenti presenti all'interno del Registro dei Trattamenti, la DPIA è effettuata dalla Società al verificarsi delle casistiche elencate all'art.35.3 del GDPR, ovvero:

- di almeno uno dei trattamenti di cui al Provvedimento del 11 ottobre 2018 dell'Autorità Garante;
- di almeno due dei criteri elencati dal WP29 nel WP248;
- ulteriori condizioni che, a discrezione e valutazione del Titolare del trattamento, possono far sorgere la necessità della DPIA, in un'ottica di accountability.

Con particolare riferimento alla DPIA, come previsto dall'art.35 del GDPR, essa può essere svolta su una singola operazione di trattamento dei dati o per più trattamenti dati simili tra loro in termini di natura, ambito di applicazione, contesto, finalità e rischi associati, secondo il principio della riconducibilità.

Inoltre, può essere svolta una singola DPIA anche nel caso in cui venga implementata una nuova applicazione o un servizio che preveda molteplici trattamenti.

Con particolare riferimento alla DPIA, oltre ai casi specificatamente richiamati dalla normativa applicabile, essa può risultare necessaria, a titolo esemplificativo, nei seguenti casi:

- qualora il trattamento comporti una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- qualora si effettui un trattamento, su larga scala, di "categorie particolari di Dati", o di "Dati relativi a condanne penali e a reati";

- qualora si effettui un'attività di sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Di seguito sono identificati e descritti i criteri per i quali un trattamento è da sottoporsi obbligatoriamente a DPIA, nonché le condizioni per cui la DPIA risulta non necessaria per uno specifico trattamento.

Criteri che rendono obbligatoria la DPIA

Il Titolare deve eseguire la DPIA nei seguenti casi:

1. Allorquando è presente almeno uno dei seguenti trattamenti di dati personali (in accordo al Provvedimento del Garante del 11 ottobre 2018):

Provvedimento 11 Ottobre 2018 – Garante italiano per la Protezione dei Dati	
ID	**Ambito (da Provvedimento)**
1	Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato".
2	Trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi).
3	Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.
4	Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure

	la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).
5	Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).
6	Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).
7	Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01
8	Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche
9	Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment)
10	Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.
11	Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.
12	Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

2. Allorquando sono presenti almeno due dei criteri del WP248:

Linee Guida WP 248 del WP29		
ID	**Ambito (da Linee Guida WP248 del WP29)**	**Esempi**
1	Valutazioni o punteggi (scoring) inclusa profilazione	Credit scoring, profiling online
2	Decisioni automatizzate con effetti legali o analoghi	Profilazione
3	Monitoraggio sistematico	Videosorveglianza sistematica di un'area accessibile al pubblico
4	Dati Sensibili o di natura estremamente personale	Cartelle sanitarie, comunicazioni elettroniche, geo localizzazioni, dati personali relativi a condanne penali o reati
5	Dati trattati su larga scala	Big Data
6	Combinazione o connessione tra banche dati	Dati provenienti da diversi titolari con diverse finalità
7	Dati relativi a interessi vulnerabili	Squilibrio di poteri fra interessato e Titolare del trattamento (es. minori)
8	Utilizzi per nuove finalità o ricorso a soluzioni organizzative o tecniche	Biometria, facial recognition, IoT
9	Trattamenti che condizionano o limitano esercizio di diritti o facoltà	Videosorveglianza, credit scoring

Inoltre, qualora l'analisi dei rischi eseguita sul trattamento restituisca un valore di rischio residuo elevato, si consiglia di valutare anche i potenziali impatti sui diritti e le libertà delle persone fisiche.

Criteri che rendono non obbligatoria la DPIA

Lo svolgimento di una DPIA non è obbligatorio qualora il trattamento non sia tale da presentare un rischio elevato per i diritti e le libertà degli interessati o qualora si verifichi uno dei casi di seguito riportati:

- quando la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a un trattamento per il quale è stata già svolta una DPIA. In tali casi, si possono utilizzare i risultati della DPIA per un trattamento riconducibile;
- quando le tipologie di trattamento sono state già verificate dall'Autorità di controllo prima del maggio 2018 in condizioni specifiche e tali condizioni non sono variate;
- qualora un trattamento, effettuato a norma dell'articolo 6, trovi una base giuridica nel diritto dell'Unione o nel diritto dello Stato membro, tale diritto disciplini il trattamento specifico o sia

già stata effettuata una DPIA nel contesto dell'adozione di tale base giuridica a meno che uno Stato membro non abbia dichiarato che è necessario effettuare tale valutazione prima di procedere alle attività di trattamento;

- qualora il trattamento sia incluso nell'elenco facoltativo (stabilito dall'Autorità di controllo) delle tipologie di trattamento per le quali non è richiesta alcuna DPIA (articolo 35).

Per l'esecuzione dell'attività di DPIA, il Gruppo Acea ha deciso di adottare come strumento di valutazione ad oggi, il Tool della Commission Nationale de l'Informatique et des Libertés (CNIL) con riserva di variazione a seguito di evoluzioni del framework di riferimento.

Con riferimento agli aspetti specifici, alle modalità operative ed ai ruoli e responsabilità afferenti l'*analisi* e *valutazione del rischio* ed al *Data Protection Impact Assessment (DPIA)*, si rimanda alla specifica procedura. Con riferimento, invece, agli specifici strumenti e metriche, si rimanda agli allegati al presente documento (cfr. All. F, G e H).

3 Definizioni, abbreviazioni ed acronimi

Autorità di controllo[9]: l'autorità amministrativa indipendente, istituita da ciascuno Stato membro, avente l'incarico di sorvegliare l'applicazione del Regolamento (UE) n. 2016/679 al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento dei loro dati personali.

BCR (Binding Corporate Rules)[10] ***– Norme Vincolanti di Impresa***: strumento volto a consentire il trasferimento di dati personali dal territorio dello Stato verso Paesi terzi (al di fuori dello Spazio Economico Europeo) tra società facenti parti dello stesso gruppo d'impresa.

Categorie particolari di dati personali[11] dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Comunicazione[12]: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del Titolare nel territorio dello Stato, dal responsabile e dalle persone autorizzate al trattamento, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Consenso:[13] qualsiasi manifestazione di volontà libera, specifica, informata ed inequivocabile con la quale l'interessato accetta, mediante dichiarazione o azione positiva inequivocabile che i dati personali che lo riguardano siano oggetto di trattamento. Il consenso costituisce una delle basi giuridiche a fondamento della liceità di un trattamento.

Data Breach - Violazione dei dati personali:[14] la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Dato personale[15]: 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,

[9] Artt. 4 n° 21 e 51.
[10] Artt. 4, n° 20 e 47.
[11] Artt 4, nn. 9, 13, 14 e 15.
[12] Art. 4 n 9.
[13] Art. 4, n 11.
[14] Art. 4 n° 12.
[15] Art. 4, n° 1.

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 (art. 4, 1 comma, n. 1, GDPR).

Data retention[16]***:*** tempo di conservazione di un dato personale, legato alla specifica finalità del trattamento.

Diffusione[17]: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

DPA (Data Protection Agreement):[18] contratto o altro atto giuridico a norma del diritto dell'Unione Europea o degli Stati membri, che vincoli il responsabile del trattamento al Titolare del trattamento e che stipuli, in particolare, la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento.

DPIA (Data Protection Impact Assessment)[19]***:*** valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali effettuata quando uno o più trattamenti presentano un rischio elevato per i diritti e le libertà delle persone fisiche, soprattutto con riguardo ad innovazioni tecnologiche e nuovi progetti.

Finalità[20]***:*** scopo per cui i dati personali sono raccolti; le finalità devono essere determinate, esplicite e legittime e il trattamento dei dati (anche ulteriore) non può avvenire per finalità incompatibili con quelle originarie di raccolta.

Informativa[21]: documento contenente le principali informazioni riguardanti modalità e finalità del trattamento di dati personali e fornito all'interessato prima della raccolta dei suoi dati personali.

Interessato[22]: la persona fisica cui si riferiscono i dati personali oggetto di trattamento.

GDPR: General Data Protection Regulation "Regolamento (UE) 2016/679.

Gruppo Acea o Gruppo*:* Acea SpA e Società del Gruppo Acea.

Misure di sicurezza:[23] il complesso delle misure tecniche, informatiche, organizzative, logiche e procedurali volte a garantire un livello di sicurezza adeguato tenuto conto dei rischi derivanti dalla distruzione, perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale a dati personali trasmessi, conservati o comunque trattati.

[16] Art. 5 lett. e).
[17] Art. 4 n. 9.
[18] Art. 28.
[19] Art. 35.
[20] Art. 5 lett. b).
[21] Artt. 12, 13, 14.
[22] Art. 4 n. 1.
[23] Art. 32.

Profilazione[24]: qualsiasi forma di trattamento automatizzato di dati personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

Registro delle attività di Trattamento[25]**:** documento che censisce i trattamenti effettuati da un Titolare e che adempie all'obbligo, per la società o l'ente che gestisce dati personali, di documentare adeguatamente la tipologia dei dati trattati. Deve essere aggiornato, completo e messo a disposizione dell'Autorità di Controllo su richiesta.

SCC – Clausole Contrattuali standard[26]**:** strumento contrattuale da includere nell'ambito di un contratto più ampio - utilizzabile in caso di mancanza di una decisione di adeguatezza della Commissione Europea - la cui finalità è assicurare adeguate garanzie al trasferimento di dati personali da parte di un titolare o responsabile del trattamento europeo (il cosiddetto "esportatore") verso un responsabile o titolare situato al di fuori del SEE (il cosiddetto "importatore"), conformemente a quanto stabilito dal GDPR.

Società del Gruppo Acea*:* Società Controllate direttamente o indirettamente da Acea.

Trattamento[27]***:*** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento e/o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione e/o qualsiasi altra forma di messa a disposizione, il raffronto e/o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Vertice aziendale delle Società del Gruppo (o Vertice aziendale): Presidente, Amministratore Delegato, Amministratore Unico, ovvero soggetto che, sulla base delle deleghe ricevute dal Consiglio di Amministrazione della Società del Gruppo, ha la responsabilità in materia di gestione dei rischi a livello locale.

[24] Art. 4 n. 4.
[25] Art. 30.
[26] Art. 46.
[27] Art. 4 n. 2.

4 Principi di riferimento

Tutte le risorse aziendali coinvolte nel funzionamento del Modello operano nel rispetto del sistema normativo, organizzativo e dei poteri e delle deleghe interne e sono tenute ad operare in conformità con le normative di legge ed i regolamenti vigenti e nel rispetto dei principi riportati di seguito.

- **Accountability** - La responsabilizzazione del Titolare nel garantire la conformità agli adempimenti normativi e la capacità dello stesso di dimostrare le scelte effettuate all'interno del contesto di riferimento in cui il dato personale viene trattato.
- **Liceità, correttezza e trasparenza –** I dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato. Il trattamento deve sempre essere giustificato da una valida base giuridica. Il trattamento deve essere preceduto dalla resa di una informativa all'interessato che ne specifichi gli aspetti salienti affinché l'interessato sia pienamente consapevole del trattamento effettuato sui suoi dati personali.
- **Privacy by design** - Impone al Titolare la necessità di progettare i sistemi informativi/iniziative privacy relevant in modo da garantire la conformità e la tutela del dato sin dalla progettazione e durante tutto il suo ciclo di vita, ponendo la privacy come obiettivo finale.
- **Privacy by default –** Il Titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità (in fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali).
- **Limitazione della finalità** - I dati personali devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali per finalità ulteriori non deve essere incompatibile con le finalità iniziali di raccolta.
- **Limitazione della conservazione** - I dati personali devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati. Possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatta salva l'attuazione di misure tecniche e organizzative adeguate a tutela dei diritti e delle libertà dell'interessato.
- **Integrità, riservatezza disponibilità** - I dati personali devono essere trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali. In tal senso, per preservare l'integrità, la riservatezza e la disponibilità dei dati, sono definiti criteri adeguati

e modalità di gestione nonché di utilizzo delle informazioni in conformità alle norme di legge e a regolamenti interni ed esterni (e garantendo che il trattamento delle informazioni avvenga nel rispetto dei diritti e degli interessi di personale, clienti e partner commerciali).

- **Minimizzazione dei dati** - I dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. Devono essere oggetto di trattamento solo i dati personali strettamente necessari.
- **Esattezza** - I dati personali devono essere esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.
- **Gestione delle informazioni e tutela della privacy del personale -** Ciascun dipendente deve conoscere e attuare quanto previsto dalle politiche aziendali in tema di sicurezza delle informazioni per garantirne l'integrità, la riservatezza e la disponibilità. Acea tutela altresì la privacy di ciascun dipendente, in conformità alla normativa applicabile, e adotta standard che prevedono il divieto, fatte salve le eccezioni previste dalla legge, di comunicare e diffondere i dati personali senza previo consenso dell'interessato, stabilendo le regole per il controllo delle norme a protezione della privacy.
- **Segregazione delle attività** - Nel Modello è attuata una segregazione di compiti e responsabilità tale da evitare situazioni di concentrazione di attività incompatibili su uno stesso soggetto e la creazione di condizioni di rischio in merito all'attendibilità delle informazioni e alla correttezza dello svolgimento delle attività. L'applicazione del principio è attuata in relazione alla natura delle attività, al grado e alla tipologia di rischio associato all'attività medesima, evitando inefficienze organizzative, in particolare nel caso di realtà organizzative di modeste dimensioni.
- **Sistema dei poteri** – Ciascuno degli attori convolti nel Modello deve essere individuato all'interno del sistema di ruoli e responsabilità aziendale, in linea con le esigenze dettate dallo svolgimento delle proprie mansioni e con gli obblighi previsti per legge.
- **Tracciabilità** - Le persone coinvolte nel Modello garantiscono, ciascuna per la parte di propria competenza, la tracciabilità delle attività e dei documenti inerenti al funzionamento del Modello, assicurandone l'individuazione e la ricostruzione delle fonti, degli elementi informativi e dei controlli effettuati. Inoltre, assicurano la conservazione della relativa documentazione, nel rispetto dei termini di legge, utilizzando, laddove disponibili, i sistemi informativi dedicati.
- **Trasferimento di dati all'estero**: Il trasferimento di dati personali al di fuori del territorio europeo che può avvenire solo in presenza di garanzie adeguate.

Il Gruppo Acea è da sempre impegnato nel garantire la conduzione dei propri *business* nel completo rispetto della Normativa applicabile, con modalità evolutive rispetto alle esigenze via via emergenti. In tal contesto, la presente linea guida funge da Linea Guida a descrizione del Modello di gestione degli impatti privacy /data Protection che, nelle operazioni *day by day,* mira a garantire che il trattamento dei dati personali avvenga in modo lecito e corretto, e comunque sulla base di regole formali e specifiche volte a individuare, prevenire e mitigare i rischi relativi alla violazione dei dati personali. Nell'implementazione di quanto sopra, Acea SpA tiene conto, a titolo esemplificativo e non esaustivo, dei trattamenti di dati personali afferenti i rapporti con i propri dipendenti (ivi inclusi eventuali rapporti di collaborazione), con le terze parti coinvolte nel proprio business (es. fornitori, consulenti, partners, ecc.) e con i clienti.

5 Riferimenti interni ed Esterni

5.1 Riferimenti interni

- Codice Etico
- Linee di indirizzo del Sistema di Controllo Interno e di Gestione dei Rischi del Gruppo Acea
- Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs. 231/2001
- Antitrust - Manuale di conformità alla normativa in materia antitrust e di tutela del consumatore
- Antitrust - Regolamento organizzativo Compliance antitrust e pratiche commerciali scorrette
- Procedure in vigore presso Acea Spa e le Società del Gruppo che regolano materie correlate all'oggetto della Presente normativa e che si applicano per quanto non in contrasto con quest'ultima e in coerenza con l'assetto organizzativo aziendale in vigore

5.2 Riferimenti esterni

Qualità

- UNI EN ISO 9001:2015 - Sistemi di gestione per la qualità - Requisiti
- UNI EN ISO 9000:2015 - Sistemi di gestione per la qualità - Fondamenti e vocabolario
- UNI EN ISO 9004:2018 - Gestione per la qualità - Qualità di un'organizzazione - Linee guida per conseguire il successo durevole

Sicurezza

- UNI ISO 45001:2018 - Sistemi di Gestione per la Salute e Sicurezza sul Lavoro - Requisiti e guida per l'uso
- Documento normativo Biosafety trust certification – Rina 2020 - Sistemi di gestione della prevenzione e controllo delle infezioni

I riferimenti alle norme ISO sono validi solo per le Società con sistema certificato.

Data Protection

- Codice in materia di protezione dei dati personali (D. Lgs. 196/03 e ss.mm.ii ai sensi del D.Lgs. 101/2018) e Regolamento UE 2016/679 (GDPR)

Altre tematiche specifiche

- Standard ISO 31000: 2018 Gestione del rischio - Principi e linee guida
- Standard ISO/IEC 27001:2017 "Information Technology - Security techniques - Information Security

Management Systems"

- Standard ISO/IEC 29134:2017 "Information technology — Security techniques — Guidelines for privacy impact assessment" Standard ISO 29100:2018 "Information technology - Security techniques - Privacy framework"

Riferimenti legislativi nazionali ed europei specifici

- Framework Nazionale per la Cybersecurity e la Data Protection – febbraio 2019
- ENISA – Allegato A al Manuale sulla Sicurezza nel trattamento dei dati personali (dicembre 2017)

6 Archiviazione, conservazione e tracciabilità

Le strutture aziendali coinvolte nel funzionamento del Modello per quanto di propria competenza, assicurano il corretto trattamento, la tracciabilità dei dati e delle informazioni, provvedono alla conservazione e all'archiviazione della documentazione prodotta e di origine esterna, in qualsiasi formato e supporto prodotto, in modo da consentire la tracciabilità delle informazioni e del processo decisionale e preservare il documento da un eventuale utilizzo improprio, perdita di riservatezza e perdita d'integrità.

7 Elenco Allegati

Titolo Allegato	Codice Allegato
Misure di sicurezza integrate (Catalogo)	Allegato A
Principi di Data Retention	Allegato B
Privacy Screening (Checklist)	Allegato C
Profili di conformità data protection Privacy by Design	Allegato D
Modello registro dei trattamenti	Allegato E
Tool analisi e valutazione dei rischi	Allegato F
Metriche analisi e valutazione dei rischi	Allegato G
Tool applicabilità DPIA	Allegato H
Scheda sul trattamento dei dati personali	Allegato I
DPO Control Framework	Allegato L