POLITICA IN MATERIA DI PROTEZIONE E VALORIZZAZIONE DEI DATI PERSONALI

Bologna, 9 novembre 2023

[PAGINA VOLUTAMENTE LASCIATA IN BIANCO]

Indice

1 Introduzione

1.1 Obiettivi del documento

La Politica in materia di protezione e valorizzazione dei Dati Personali (la "**Politica di *Data Protection***" o la "**Politica**") ha l'obiettivo di definire le linee guida generali del Gruppo Unipol (il "**Gruppo**") in materia di protezione delle persone fisiche con riguardo al trattamento dei Dati Personali (come *infra* definiti).

La Politica pertanto definisce, con riguardo alle esigenze di protezione dei Dati Personali nell'ambito dei Trattamenti effettuati dalle società del Gruppo che trattano Dati Personali e che rientrano nel perimetro di applicazione di cui al successivo par. 2.2 (le "**Società in perimetro**"):

- il Modello organizzativo (organizzazione e ruoli, persone, cultura e competenze);
- il Modello operativo (processi e regole e documentazione);
- il Modello architetturale (Dati Personali, tecnologie e strumenti).

La Politica si compone, altresì, di un allegato che definisce gli impegni assunti dal Gruppo - in relazione allo specifico modello di *business* - nei confronti dei propri clienti e di tutti gli *stakeholder* affinché la protezione accordata ai Dati Personali che sono nella disponibilità delle Società in perimetro sia sostenuta da un'attività crescente di valorizzazione. Per "valorizzazione" dei Dati Personali è da intendersi l'attività di promozione, sviluppo ed arricchimento del patrimonio informativo del Gruppo al fine di creazione di valore condiviso; da tenersi distinta rispetto alla "protezione" dei Dati Personali, avente carattere conservativo e volta alla tutela dei medesimi rispetto ai rischi per i diritti e le libertà degli Interessati.

Si precisa che, laddove non diversamente specificato, gli Organi/Aree/Direzioni/Funzioni citati nella Politica si intendono riferiti a quelli di UnipolSai Assicurazioni S.p.A. ("**UnipolSai**"), ovvero gli Organi/Aree/Direzioni/Funzioni equivalenti, ove presenti, delle altre Società in perimetro anche qualora esternalizzati.

1.2 Approvazione e revisione del documento

La Politica, per la cui redazione/revisione sono state coinvolte tutte le strutture aziendali interessate, al fine di poter assicurare una chiara definizione e condivisione degli obiettivi, dei ruoli e delle responsabilità, è approvata dal Consiglio di Amministrazione di Unipol Gruppo S.p.A. ("**Unipol**" o la "**Capogruppo**"), anche nella sua qualità di Capogruppo, nell'esercizio della propria attività di direzione e coordinamento nei confronti delle società controllate ed in coerenza con il processo aziendale di Gruppo in materia di predisposizione e validazione delle politiche aziendali.

Successivamente, i Consigli di Amministrazione delle altre Società in perimetro, nell'ambito delle proprie responsabilità in tema di *governance*, sistema dei controlli interni e gestione dei rischi, valutano e approvano la Politica, per quanto applicabile, in conformità con il proprio modello di *business*.

La Politica sarà rivista e – se del caso – modificata, ogni qualvolta esigenze di aggiornamento normativo, interventi dell'Autorità di Controllo, strategie di *business* o modifiche di contesto (modifiche rilevanti di processi aziendali, riorganizzazioni strutturali significative, modifiche rilevanti alle piattaforme informatiche utilizzate) lo richiedano.

La Politica è comunicata e resa disponibile dalle Società in perimetro a tutto il personale interessato mediante adeguati canali di comunicazione.

2 Contesto di riferimento

2.1 Riferimenti normativi

Il 24 maggio 2016 è entrato in vigore il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei Dati Personali, nonché alla libera circolazione di tali dati (il "**GDPR**"), direttamente applicabile in tutti gli Stati membri a partire dal 25 maggio 2018.[1]

Il GDPR si applica ai Trattamenti di Dati Personali effettuati da (i) imprese stabilite nel territorio dell'Unione Europea (anche se il Trattamento avviene al di fuori), nonché (ii) da imprese stabilite fuori dal territorio dell'Unione Europea che offrano beni o servizi ad Interessati che si trovino nell'Unione Europea e/o che monitorino il loro comportamento all'interno dell'Unione Europea.

La protezione dei Dati Personali è, ad oggi, disciplinata in Italia (i) dal GDPR, (ii) dal Codice *Privacy* (come *infra* definito[2]), nonché (iii) dai Provvedimenti e dalle Linee Guida del Garante per la protezione dei dati personali (come *infra* definito) per sua diretta iniziativa o in riferimento a reclami, segnalazioni, richieste di pareri, presentate da cittadini, aziende, associazioni, enti[3].

Inoltre, il Gruppo di Lavoro istituito ai sensi dell'art. 29 della Direttiva 95/46/CE (il "**WP29**", *infra* definito), sostituito dal **Comitato europeo per la protezione dei dati**, emana linee guida e documenti di indirizzo in materia di protezione dei Dati Personali al fine di fornire raccomandazioni e chiarimenti applicativi in merito ad alcuni istituti previsti dal GDPR.

La presente Politica inoltre è coerente ed integra il sistema di autoregolamentazione in vigore nel Gruppo[4].

2.2 Perimetro di applicazione

La presente Politica si applica alla Capogruppo e alle società del Gruppo da essa controllate con sede legale in Italia che trattano dati personali.

Le società del Gruppo non aventi sede legale in Italia si dotano di una propria politica in materia di protezione dei Dati Personali coerente con la presente Politica.

---

1 Il GDPR ha abrogato la precedente normativa in materia, ossia la Direttiva 95/46/CE del 24 ottobre 1995, "relativa alla tutela delle persone fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati"; conseguentemente anche le normative nazionali emanate in applicazione di tale Direttiva sono state oggetto di modifica, almeno nelle parti in contrasto con il GDPR.

2 Il Codice Privacy è stato oggetto di revisione con il Decreto Legislativo 10 agosto 2018, n. 101, in attuazione dell'art. 13 della Legge di Delegazione del 25 ottobre 2017, n. 163. Il Decreto Legislativo 10 agosto 2018, n. 101 ha abrogato le parti del Codice in contrasto con il GDPR.

3 Le prescrizioni contenute in Provvedimenti del Garante emessi prima del 25 maggio 2018 che non sono in contrasto con le disposizioni del GDPR sono rimasti in vigore, talvolta per mezzo di nuovi provvedimenti volti a chiarire espressamente le prescrizioni compatibili con il nuovo assetto normativo.

4 In particolare, la Politica è integrata dalla Politica di Gruppo in materia di *Data Governance*, dalla Politica di sicurezza delle informazioni e dalla Politica in materia di sostenibilità.

2.3 Definizioni e terminologia

Alta Direzione	L'Amministratore Delegato e/o il Direttore Generale (ove nominati) e, con riferimento a Unipol e alle Società assicurative del Gruppo aventi sede in Italia, l'alta dirigenza che svolge compiti di sovrintendenza gestionale (ovvero i Dirigenti con responsabilità strategiche identificati ai fini della applicazione della normativa di vigilanza in materia di operatività infragruppo).
Altre Società	Le società controllate del Gruppo aventi sede legale in Italia, diverse da Arca Vita S.p.A. ("**Arca Vita**") e le sue controllate italiane, che non hanno stipulato un accordo di *service* con la Funzione *Privacy* di UnipolSai.
Area Risk	La funzione fondamentale Risk Management di Unipol e di UnipolSai, nonché le analoghe funzioni delle altre Società in perimetro, anche qualora esternalizzate.
Audit	La funzione fondamentale Audit di Unipol e di UnipolSai, nonché le analoghe funzioni delle altre Società in perimetro, anche qualora esternalizzate.
Autorità di Controllo o Garante	Il Garante per la protezione dei dati personali, ovvero l'Autorità di Controllo nazionale italiana in materia di protezione dei Dati Personali.
Categorie particolari di Dati Personali	Dati personali (come *infra* definiti) che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale. Sono da ritenersi appartenenti a tale categoria anche i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute nonché i dati che rivelino l'orientamento sessuale della persona.
Codice *Privacy*	Decreto Legislativo 30 giugno 2003, n. 196 "*Codice in materia di protezione dei dati personali*" come modificato dal decreto legislativo 10 agosto 2018, n. 101, recante "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016*".
Comitato europeo per la protezione dei dati (*European Data Protection Board* o EDPB)	Il Comitato Europeo per la protezione dei dati sostituisce il WP29 (o Gruppo di lavoro articolo 29 per la protezione dei dati). È istituito ai sensi dell'art. 68 del GDPR ed è composto dalla figura di vertice di un'autorità di controllo per ciascuno Stato membro e dal Garante europeo della protezione dei dati, o dai rispettivi rappresentanti.
Compliance and Anti-Money Laundering	Per l'ambito delle attività di compliance, la funzione fondamentale Compliance di Unipol e UnipolSai, nonché le analoghe strutture delle altre Società in perimetro, anche qualora esternalizzate. Per l'ambito delle attività di antiriciclaggio, la funzione di cui (i) al Capo II del Regolamento IVASS n. 44 del 12 febbraio 2019 o (ii) al Capitolo II del Provvedimento di Banca d'Italia del 26 marzo 2019 di Unipol e UnipolSai, nonché le analoghe strutture delle altre Società in perimetro, anche qualora esternalizzate.

Consenso dell'Interessato	Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'Interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, affinché i Dati Personali che lo riguardano siano oggetto di Trattamento (*cfr.* art. 4 del GDPR).
***Data Breach* o Violazione dei Dati Personali**	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 (*cfr*. art. 4 del GDPR).
Dati comuni	Dati Personali diversi dai dati appartenenti alle Categorie particolari di Dati Personali (come definiti) e dai Dati Personali relativi a condanne penali e reati. Sono dati con un livello di criticità tendenzialmente più basso rispetto ai rischi per i diritti e le libertà degli Interessati. A titolo esemplificativo: i dati anagrafici, i recapiti, i riferimenti bancari, i dati contrattuali, lavorativi, retributivi, altri Dati Personali che possono essere ricondotti alla persona quali, ad esempio, il numero di targa del veicolo, etc.
Dato Personale (o Dati Personali)	Qualsiasi informazione riguardante una persona fisica identificata o identificabile; 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 (*cfr*. art. 4 del GDPR).
Delegato *Privacy*	L'Amministratore Delegato, il Direttore Generale (ove non presente l'Amministratore Delegato), ovvero in assenza di Amministratore Delegato/Direttore Generale, il soggetto individuato dal Consiglio di Amministrazione e provvisto dei necessari poteri; tale figura è incaricata dal Consiglio di Amministrazione di sovraintendere all'esecuzione delle linee di indirizzo definite dal Consiglio di Amministrazione stesso, curando la progettazione, realizzazione e gestione del sistema di controllo interno e di gestione del rischio *privacy*, e verificandone costantemente l'adeguatezza e l'efficacia.
DPIA o *Data Protection Impact Assessment*	Valutazione d'impatto sulla protezione dei Dati Personali.
DPO o DPO di Gruppo o *Data Protection Officer*	Responsabile della protezione dei dati personali. Unipol Gruppo ha istituito un DPO di Gruppo, che svolge le attività di competenza per Unipol e per le altre Società in perimetro, secondo un approccio *risk-based*. Le società controllate aventi sede legale in un altro paese dell'Unione

	Europea nominano un proprio DPO, ove necessario o ritenuto opportuno, che si coordina con il DPO di Gruppo sui temi di rilevanza generale.
GDPR (*General Data Protection Regulation*)	Regolamento dell'Unione Europea 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (Regolamento Generale sulla protezione dei dati).
Gruppo Unipol (o Gruppo)	Unipol Gruppo S.p.A. e le società controllate.
Incaricati o Soggetti autorizzati al Trattamento	Persone fisiche autorizzate a compiere operazioni di Trattamento dal Titolare o dal Responsabile del Trattamento. Ogni dipendente di ciascuna Società in perimetro è Incaricato del Trattamento dei Dati Personali.
Interessato	La persona fisica identificata o identificabile cui si riferiscono i Dati Personali.
Modello per la protezione dei Dati Personali	Insieme di scelte a livello organizzativo, gestionale/operativo e tecnologico compiute dal Gruppo volte ad assicurare un'adeguata protezione dei Dati Personali trattati dalla Capogruppo e dalle società controllate.
Monitoraggio regolare e sistematico	Con riferimento all'aggettivo "regolare" si intende un'attività di monitoraggio che avviene in modo continuo ovvero ad intervalli definiti per un arco di tempo determinato; ricorrente o ripetuta ad intervalli costanti; o che avviene in modo costante o ad intervalli periodici. Con riferimento all'aggettivo "sistematico" si intende un'attività di monitoraggio che avviene per sistema; predeterminata, organizzata o metodica; che ha luogo nell'ambito di un progetto complessivo di raccolta di dati; svolta nell'ambito di una strategia. A titolo esemplificativo, sono attività che possono configurare un monitoraggio regolare e sistematico degli Interessati: la prestazione di servizi di telecomunicazioni; attività di *marketing* sull'analisi dei dati raccolti; Profilazione e *scoring*; tracciamento dell'ubicazione; programmi di fidelizzazione; etc…
Normativa *Privacy*	Il GDPR, il Codice *Privacy*, i Provvedimenti del Garante e in generale tutta la normativa esterna in materia di protezione delle persone fisiche con riguardo al trattamento di Dati Personali.
Privacy Lab	Portale dedicato sulla *intranet* di Gruppo finalizzato alla diffusione della materia *privacy* a tutti i soggetti interni ed esterni (dipendenti, agenti e loro collaboratori). Contiene, a titolo esemplificativo, la documentazione inerente alla Normativa *Privacy*, i modelli di informativa e consenso in vigore, la documentazione inerente a tematiche *privacy* per alcuni specifici settori del Gruppo, per la rete agenziale, etc.
Process Owner	Il Chief/Direttore o, ove non presente, il Responsabile *pro tempore* dell'Area/Direzione/Funzione aziendale a cui fa capo il Trattamento, o suo

	delegato.
Profilazione	Qualsiasi forma di Trattamento automatizzato di Dati Personali consistente nell'utilizzo di tali Dati Personali per valutare determinati aspetti 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 (art. 4 del GDPR).
Referente *Privacy*	Figura interna alle Aree/Direzioni/Funzioni di UnipolSai Assicurazioni e alle Società in *service* (come definite) che fornisce, nell'ambito di propria competenza, supporto al *Process Owner* per tutte le questioni inerenti all'applicazione della Normativa *Privacy*, nonché per un efficace governo del rischio *privacy*. Con riferimento ad UnipolSai s'intende il Referente *Privacy* designato nelle principali Aree/Direzioni/Funzioni aziendali. Con riferimento alle Società in *service*, s'intende il Referente *Privacy* designato per ciascuna Società. Il Referente *Privacy* non può coincidere con il Delegato *Privacy* che, nell'ambito delle proprie attribuzioni, lo designa e ne sorveglia l'operato.
Responsabile o Responsabile del Trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta Dati Personali per conto del Titolare. Il Responsabile è un soggetto terzo (ad es. fornitore di servizi) che effettua uno o più Trattamenti di Dati Personali di cui è Titolare la Società in perimetro. Sono considerati Responsabili gli intermediari assicurativi di cui all'art. 109, comma 2, lettere "a", "d" e "f"" del Codice delle Assicurazioni Private, che operano per conto del Gruppo.
Rischio *privacy*	Nell'ambito del rischio di non conformità, è il rischio di incorrere in sanzioni giudiziarie o amministrative, perdite patrimoniali, o danni reputazionali in conseguenza della violazione della Normativa *Privacy*.
Servizio ICT, o Servizio Informatico	Insieme di sistemi ICT utilizzati da un processo aziendale per la ricezione, archiviazione, elaborazione, trasmissione e fruizione di dati (ad es. *software* applicativo, posta elettronica).
Società *in service*	Le società controllate del Gruppo che hanno stipulato un accordo di *service* con la Funzione *Privacy* di UnipolSai.
Titolare o Titolare del Trattamento	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. Ciascuna Società in perimetro è Titolare di Trattamenti di Dati Personali e deve individuare un Delegato *Privacy* (come definito) per sovrintendere

	alla corretta applicazione della Normativa *Privacy*.
Trattamento	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a Dati Personali o insiemi di Dati Personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (art. 4 del GDPR).
Trattamento su larga scala	Trattamento di una notevole quantità di Dati Personali a livello regionale, nazionale o sovranazionale e che potrebbe incidere su un vasto numero di Interessati e che potenzialmente presenta un rischio elevato[5].

[5] L'EDPB, al fine di stabilire se un Trattamento sia effettuato su larga scala, raccomanda di tenere conto dei seguenti fattori: il numero di soggetti Interessati dal Trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; il volume dei dati e/o le diverse tipologie di dati oggetto del Trattamento; la durata, ovvero la persistenza, dell'attività di Trattamento; la portata geografica dell'attività di Trattamento.

3 Linee guida in materia di protezione dei Dati Personali

3.1 Premessa

Il GDPR ha comportato un vero e proprio cambio di filosofia: si è abbandonato un sistema di tipo formalistico, basato sulla previsione di regole formali, adempimenti analiticamente definiti e misure minime di sicurezza tassativamente elencate per passare a un sistema di *governance* dei Dati Personali, basato su un'alta responsabilizzazione sostanziale ("*accountability*") del Titolare, che deve garantire ed essere in grado di dimostrare la conformità al GDPR. Tale onere probatorio si sostanzia nell'adozione di misure tecniche ed organizzative la cui adeguatezza deve essere valutata sulla base delle specifiche caratteristiche dei Trattamenti di Dati Personali (natura, ambito di applicazione, contesto e finalità del Trattamento), nonché dei rischi per i diritti e le libertà degli Interessati (artt. 5 e 24 del GDPR).

Il GDPR ha introdotto importanti novità in materia di protezione dei Dati Personali; tuttavia sono stati confermati molti istituti già previsti dalla normativa previgente. Di seguito, è riportato uno schema di sintesi degli aspetti (i) invariati o variati marginalmente e (ii) nuovi, rispetto alla disciplina previgente.

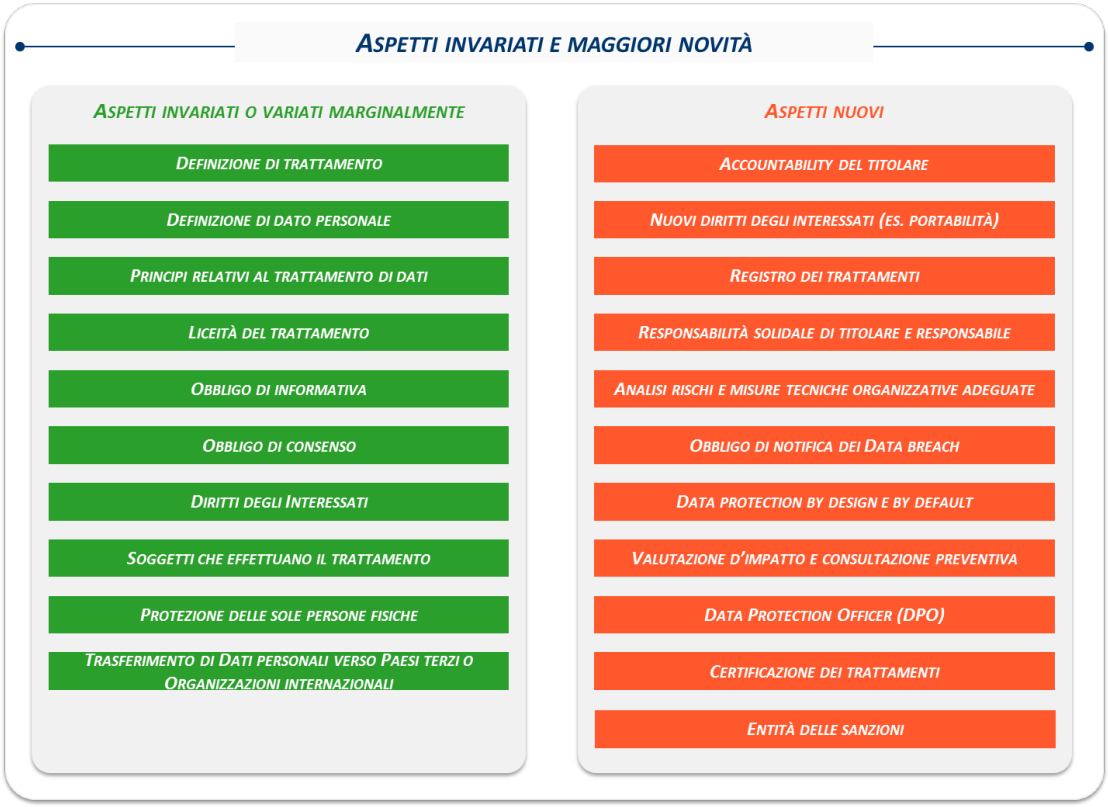

Figura 1: Previsioni invariate o variate marginalmente e Nuove previsioni

3.2 Previsioni invariate o variate marginalmente

Di seguito sono riportati i principali obblighi normativi rimasti invariati, con particolare attenzione a quelli variati solo marginalmente; con riferimento alla descrizione degli aspetti di nuova introduzione si rimanda ai successivi paragrafi 3.3 e 3.4.

Principi applicabili al Trattamento di Dati Personali

Le definizioni e i principi generali previsti dalla normativa previgente rimangono sostanzialmente invariati.

I Dati Personali sono:

- trattati in modo lecito, corretto e trasparente nei confronti dell'Interessato ("liceità, correttezza e trasparenza");
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in un modo che non sia incompatibile con tali finalità ("limitazione della finalità");
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati");
- esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti, incompleti o non aggiornati rispetto alle finalità per le quali sono trattati ("esattezza");
- 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 ("limitazione della conservazione");
- 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 ("integrità e riservatezza").

Informativa

La disciplina generale relativa alle Informative da fornire agli Interessati, prevista dalla normativa previgente, è stata sostanzialmente confermata. È stato previsto un ampliamento dei contenuti delle Informative (rif. par. 3.4.2.2), disponendo, in particolare, che il Titolare adotti misure appropriate per fornire all'Interessato le informazioni e le comunicazioni inerenti anche all'esercizio dei suoi diritti in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro ed il più possibile adatto ai destinatari di riferimento e da essi comprensibile. Le informazioni possono essere fornite per iscritto o con altri mezzi, anche elettronici.

Consenso e altre basi giuridiche legittimanti

Il consenso espresso dell'Interessato al Trattamento dei propri dati per una o più specifiche finalità, per poter costituire condizione di liceità al Trattamento, deve essere, in tutti i casi, libero, specifico, informato ed inequivocabile; non è ammesso il consenso tacito o presunto.

Il Trattamento è inoltre lecito qualora sia necessario a: (i) dare esecuzione ad un contratto di cui l'Interessato è parte o a misure precontrattuali adottate su richiesta dello stesso, (ii) adempiere agli obblighi di legge cui è soggetto il Titolare, (iii) salvaguardare gli interessi vitali dell'Interessato o di un'altra persona fisica, (iv) eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del Trattamento, (v) perseguire un interesse legittimo del Titolare o di terzi (a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'Interessato che richiedono la protezione dei dati).

Diritti degli Interessati

Ad eccezione dei nuovi diritti introdotti (ad es. diritto alla portabilità, etc.), il GDPR conferma i diritti degli Interessati già previsti dalla normativa previgente, quali: diritto di accesso, diritto di rettifica e diritto di opposizione (rif. par. 3.4.2.4).

Incaricati del Trattamento

La figura dell'Incaricato non è più espressamente prevista nel GDPR, tuttavia il Garante ha precisato[6] che questa è compatibile con la figura del Soggetto autorizzato al Trattamento.

3.3 Nuove previsioni

Oltre al sostanziale rovesciamento di prospettiva di cui alla Premessa, il GDPR ha introdotto anche alcune novità:

- ***Data Protection Officer (DPO)*** *(*Artt. 37-39) - La figura del DPO rappresenta una delle principali novità del GDPR e costituisce uno degli elementi-chiave della *governance* del Modello per la protezione Dati Personali (come definito). La sua designazione è finalizzata a facilitare l'attuazione del GDPR da parte del Titolare o del Responsabile ed è obbligatoria in alcuni casi (rif. par. 2.3 e 3.4.1.5);
- **Registro dei Trattamenti** (Art. 30) - Il GDPR ha introdotto l'obbligo di istituire e mantenere aggiornato un Registro dei Trattamenti, sia per il Titolare, con riferimento alle attività di Trattamento svolte sotto la propria responsabilità, che per il Responsabile per le attività di Trattamento svolte per conto di ogni Titolare, salvo ricorrano determinate condizioni in deroga (rif. par. 3.4.2.8);
- ***Data Protection by Design*** (Art. 25, co. 1) - Il GDPR ha previsto che, preliminarmente al momento dell'avvio di un nuovo Trattamento o della modifica di un Trattamento già in essere, il Titolare attui misure che soddisfino i principi di protezione dei Dati Personali (rif. par. 3.4.2.5);
- ***Data Protection by Default*** (Art. 25, co. 2) - Il GDPR ha previsto che il Titolare debba mettere in atto misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i Dati Personali necessari per ogni specifica finalità del Trattamento (rif. par. 3.4.2.5);
- ***Data Protection Impact Assessment*** **(DPIA)** (Art. 35) - Il GDPR ha previsto che, qualora un Trattamento presenti un rischio elevato per i diritti e le libertà degli Interessati, il Titolare effettui, prima di procedere al Trattamento, una valutazione preliminare d'impatto sulla protezione dei Dati Personali (rif. par. 3.4.2.6);
- **Notifica di un *Data Breach*** (Artt. 33 e 34) - Il GDPR ha introdotto l'obbligo di notificare alle autorità di controllo, senza ingiustificato ritardo (e, ove possibile, entro 72 ore), eventuali violazioni dei Dati Personali, nonché di comunicarle agli Interessati senza ingiustificato ritardo laddove vi sia un rischio elevato per i diritti e le libertà degli Interessati (rif. par. 3.4.2.10);
- **Nuovi diritti degli Interessati** (Artt. 17, 18, 20 e 22) - Il GDPR ha rafforzato il diritto alla cancellazione ("diritto all'oblio") ed ha introdotto il diritto di limitazione del Trattamento, il diritto alla portabilità dei dati, nonché il diritto di non essere sottoposto a una decisione basata unicamente sul Trattamento automatizzato, compresa la Profilazione (rif. par. 3.4.2.4);
- **Responsabile del Trattamento** (Art. 28) - Il GDPR ha individuato, rispetto alla normativa previgente, specifici obblighi e responsabilità in capo direttamente anche ai Responsabili. Ad esempio, essi possono ricevere richieste da parte del Garante, devono mettere in atto misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio, sono direttamente passibili di sanzioni

[6] Nella "*Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali*" pubblicata dal Garante sul proprio sito istituzionale, lo stesso afferma che pur non prevedendo espressamente la figura dell' "incaricato" del Trattamento (ai sensi dell'art. 30 del Codice Privacy, abrogato dalle modifiche introdotte dal Decreto Legislativo 10 agosto 2018, n. 101), il GDPR non ne esclude la presenza in quanto fa riferimento a "*persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile*".

amministrative, rispondono per il danno causato dal Trattamento non solo se non hanno rispettato le istruzioni del Titolare, ma anche se non hanno adempiuto agli obblighi specificamente diretti loro dal GDPR. Il Responsabile, inoltre, può ricorrere ad un altro Responsabile ("sub-responsabile") previo consenso scritto del Titolare, imponendo al sub-responsabile, tramite contratto o altro atto legale, le stesse obbligazioni gravanti sul Responsabile (rif. par. 3.4.2.7);

- **Sicurezza del Trattamento** (Art. 32) – Rispetto alla normativa previgente, il GDPR ha confermato la rilevanza degli obblighi in tema di sicurezza dei dati, non prevedendo più misure "minime" di sicurezza, ma prescrive, in capo al Titolare e al Responsabile, l'obbligo di adottare misure tecniche ed organizzative adeguate al rischio. Per valutare l'adeguatezza delle misure, il Titolare e il Responsabile devono pertanto effettuare un'analisi dei rischi[7] derivanti dal tipo di Trattamento che intendono porre in essere, anche alla luce della classificazione dei Dati Personali e delle possibili conseguenze per i diritti e le libertà degli Interessati (rif. par. 3.4.2.9);
- **Certificazione dei Trattamenti** (Artt. 42 e 43) - Il GDPR ha introdotto la facoltà di richiedere il riconoscimento della conformità allo stesso tramite meccanismi di certificazione o sigilli e marchi di protezione dei dati;
- **Entità delle sanzioni** (Art. 83) - Il GDPR ha aumentato in modo rilevante l'importo massimo delle sanzioni, prevedendo la possibilità per il Garante di irrogare sanzioni amministrative fino all'importo di Euro 10.000.000 o, per le imprese, se superiore, al 2% del fatturato globale annuo, ovvero fino all'importo di Euro 20.000.000 o, per le imprese, se superiore, al 4% del fatturato globale annuo, a seconda delle disposizioni violate.

[7] Rischio per i diritti e le libertà dell'Interessato, derivante dalla distruzione, perdita, modifica, divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a Dati Personali trasmessi, conservati o comunque trattati.

3.4 Modello per la protezione dei Dati Personali

Nel predetto contesto normativo che richiede al Titolare di progettare, implementare e dimostrare di aver adottato misure tecniche ed organizzative adeguate, il Gruppo ha definito il Modello per la protezione dei Dati Personali.

In particolare, il Modello per la protezione dei Dati Personali adottato dal Gruppo si compone di (i) un modello organizzativo, (ii) un modello operativo e (iii) un modello architetturale.

Componenti	Aree coperte
Modello organizzativo	– **organizzazione e ruoli**, ovvero l'insieme di strutture, organi e ruoli coinvolti nell'indirizzo e governo, esecuzione e controllo del modello di protezione dei Dati Personali; – **persone, cultura e competenze**, ovvero l'insieme di risorse, interne ed esterne, che ricoprono un ruolo nell'ambito del modello di protezione dei Dati Personali.
Modello operativo	– **processi e regole**, ovvero l'insieme di disposizioni interne aziendali e a livello di Gruppo che garantiscono la conformità alla Normativa *Privacy*; – **documentazione**, ovvero l'insieme di documenti da seguire o adottare nell'ambito di processi e regole legati, in modo diretto o indiretto, alla protezione dei Dati Personali.
Modello architetturale	– **Dati Personali**, ovvero l'insieme di Dati Personali trattati nell'ambito dei processi aziendali, sia di *staff* sia di *business*, su cui si basano le scelte relative al modello di protezione dei Dati Personali; – **tecnologia e strumenti**, ovvero l'insieme di servizi applicativi che trattano Dati Personali e misure di sicurezza, logica e fisica, adottate dal Gruppo, suddivise tra misure di prevenzione e misure di protezione.

Si rimanda ai paragrafi successivi per la descrizione di dettaglio di ciascuna componente del Modello per la protezione dei Dati Personali.

3.4.1 Modello organizzativo per la protezione dei Dati Personali

Al fine di conseguire un efficace presidio in materia di protezione dei Dati Personali, è necessario che, presso la Capogruppo e le Società in perimetro, il processo di *governance* sia chiaramente e coerentemente stabilito.

Il Gruppo ha definito ruoli e responsabilità, sia a livello di Capogruppo sia a livello di società controllate, che garantiscono l'indirizzo e governo, l'esecuzione e il controllo del Modello per la protezione dei Dati Personali.

Area	Obiettivo	Strutture, comitati e ruoli
Indirizzo e governo	Garantire la definizione del Modello di protezione dei Dati Personali, favorendone la comunicazione e la corretta implementazione in conformità alla Normativa *Privacy*.	– Consiglio di Amministrazione
Esecuzione	Garantire l'implementazione del Modello di protezione dei Dati Personali definito, nel rispetto non solo delle disposizioni della Normativa *Privacy*, ma anche di disposizioni interne di cui si è dotato il Gruppo.	– Delegato *Privacy* – Alta Direzione – *Process Owner* – Referenti *Privacy* – Funzione *Privacy* – Funzione Qualità Acquisti, Sicurezza e Supporto DPO di Arca Vita per quest'ultima e le sue controllate italiane – Responsabili del Trattamento – Soggetti autorizzati al Trattamento – *Team* cui sono affidati ruoli specifici nelle procedure aziendali (es. *Task Force Data Breach*) – Area *Information* – Direzione Immobiliare
Controllo	Identificare, valutare, gestire e monitorare i rischi di non conformità rispetto alla Normativa *Privacy* e alle norme di autoregolamentazione.	– DPO[8] – Funzione Compliance and Anti-Money Laundering – Area Risk – Funzione Audit

Di seguito sono definiti i compiti e le responsabilità del Modello per la protezione dei Dati Personali.

[8] Il DPO svolge anche funzioni informative e consultive (rif. par. 3.4.1.5).

3.4.1.1 Consiglio di Amministrazione

Il Consiglio di Amministrazione di ciascuna delle Società in perimetro ha la responsabilità ultima del sistema dei controlli interni e di gestione del Rischio *privacy* e ne assicura la costante completezza, funzionalità ed efficacia, anche con riferimento alle attività esternalizzate.

Il Consiglio di Amministrazione della Capogruppo nomina un unico DPO di Gruppo per Unipol e per le altre Società in perimetro, fornendogli le risorse necessarie per assolvere ai compiti ad esso attribuiti (rif. par. 3.4.1.5), secondo un approccio *risk-based*.

A tali fini, nell'ambito dei compiti di indirizzo strategico e organizzativo, il Consiglio di Amministrazione della Capogruppo:

- approva, previo esame del Comitato Rischi di Gruppo, la presente Politica e le sue successive modifiche;
- approva l'assetto organizzativo nonché l'attribuzione di compiti e di responsabilità per la gestione del Rischio *privacy*;
- verifica che l'Alta Direzione implementi correttamente il sistema dei controlli interni e di gestione del Rischio *privacy* secondo le direttive impartite e che ne valuti la funzionalità e l'adeguatezza;
- nomina il Delegato *Privacy*;
- riceve dal DPO una volta l'anno una relazione contenente: (i) la valutazione sulla adeguatezza ed efficacia dei presidi adottati dall'impresa per la gestione del rischio *privacy*, sull'attività svolta, sulle verifiche effettuate, sui risultati emersi e sulle criticità riscontrate, dando conto dello stato di implementazione dei relativi interventi migliorativi, qualora effettuati e (ii) un programma di attività in cui sono indicati, secondo un approccio *risk-based,* gli interventi di verifica ritenuti prioritari relativamente al Rischio *privacy*[9];
- assicura che il DPO sia tempestivamente ed adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei Dati Personali;
- assicura le risorse necessarie al DPO per assolvere i propri compiti e accedere ai Dati Personali e ai Trattamenti, nonché per mantenere aggiornata la propria conoscenza specialistica;
- assicura che ulteriori compiti e funzioni svolti dal DPO non diano adito ad un conflitto di interessi.

I Consigli di Amministrazione delle altre Società in perimetro svolgono, nelle proprie realtà aziendali e per gli aspetti a loro applicabili, i medesimi compiti del Consiglio di Amministrazione della Capogruppo.

3.4.1.2 Alta Direzione

L'Alta Direzione attua, mantiene e monitora il sistema dei controlli interni e di gestione del Rischio *privacy* sulla base delle indicazioni del Delegato *Privacy*.

[9] La Relazione del DPO predisposta per il Consiglio di Amministrazione della Capogruppo descrive le attività svolte dal DPO, secondo un approccio *risk-based,* con riferimento sia ad Unipol medesima sia alle altre Società in perimetro. Inoltre, è data evidenza dell'attività di raccordo con le società del Gruppo aventi sede legale in Irlanda.

3.4.1.3 Comitato Controllo e Rischi

Il Comitato Controllo e Rischi della Capogruppo[10] e il Comitato Controllo e Rischi di UnipolSai hanno, nei confronti dei rispettivi Consigli di Amministrazione, funzioni di supporto nell'identificazione e gestione dei principali rischi aziendali e nella verifica che gli stessi risultino correttamente identificati, adeguatamente misurati, gestiti e monitorati, nonché compatibili con una gestione dell'impresa coerente con gli obiettivi strategici individuati.

In particolare, entrambi i Comitati Controllo e Rischi esaminano le proposte in merito alla presente Politica e alle successive modifiche: inoltre ricevono dal DPO di Gruppo la relazione annuale di cui al punto 3.4.1.1, e la esaminano preventivamente rispetto al Consiglio di Amministrazione.

3.4.1.4 Comitato Rischi di Gruppo

Il Comitato Rischi di Gruppo, nell'ambito della sua funzione consultiva a supporto del Direttore Generale della Capogruppo, esamina le proposte in merito alla Politica e alle successive modifiche.

3.4.1.5 *Data Protection Officer* (DPO)

Il DPO è designato in funzione della sua conoscenza specialistica della normativa e delle prassi in materia di protezione dei Dati Personali, delle sue qualità professionali, della sua capacità di assolvere i propri compiti sopracitati, nonché della sua posizione di autonomia e indipendenza; al DPO è consentito svolgere altri compiti e funzioni a condizione che sia assicurata l'assenza di conflitto di interessi.

I compiti principali del DPO sono quelli di informare e fornire consulenza a Titolare, Responsabili ed Incaricati, nonché di sorvegliare l'osservanza della Normativa *Privacy* e delle disposizioni interne in materia di protezione dei Dati Personali di cui si è dotato il Gruppo, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai Trattamenti e alle connesse attività di controllo.

Nell'ambito dei suoi compiti di controllo, il DPO:

- monitora e fornisce consulenza in merito alle normative applicabili in ambito *privacy,* attivando ove opportuno i *Process Owner* e i rispettivi Referenti *Privacy*, anche in conformità al processo di monitoraggio e adeguamento normativo in vigore nel Gruppo;
- individua, avvalendosi anche della collaborazione della Funzione Compliance and Anti-Money Laundering, i Trattamenti maggiormente esposti al Rischio *privacy*;
- presenta annualmente al Consiglio di Amministrazione una relazione contenente: (i) la valutazione sulla adeguatezza ed efficacia dei presidi adottati dall'impresa per la gestione del Rischio *privacy*, sull'attività svolta, sulle verifiche effettuate, sui risultati emersi e sulle criticità riscontrate, dando conto dello stato di implementazione dei relativi interventi migliorativi, qualora effettuati e (ii) un programma di attività in cui sono indicati, secondo un approccio *risk-based,* gli interventi di verifica ritenuti prioritari relativamente al Rischio *privacy*. La programmazione degli interventi tiene conto sia delle carenze eventualmente riscontrate nei controlli precedenti sia di eventuali nuovi rischi;
- valuta il sistema dei controlli interni e di gestione dei rischi in ambito *privacy* anche avvalendosi della collaborazione della Funzione Compliance and Anti-Money Laundering, della Funzione Audit e dell'Area

[10] Ai sensi del Regolamento IVASS n. 38 del 3 luglio 2018, il Comitato Controllo e Rischi della Capogruppo opera anche per conto delle Compagnie del Gruppo aventi governo societario "rafforzato" (ad esclusione di UnipolSai) e "ordinario".

Risk;

- monitora l'implementazione degli interventi di adeguamento definiti, secondo le procedure aziendali in vigore (rif. par. 3.4.2.5 e par. 3.4.2.6), in relazione a nuovi Trattamenti o alla modifica di Trattamenti già in essere;
- sorveglia la tenuta del Registro dei Trattamenti (rif. par.3.4.2.8).

Inoltre, il DPO:

- coopera con il Garante e funge da punto di contatto per questioni connesse al Trattamento di Dati Personali, ed effettua, se del caso, consultazioni relativamente a qualsiasi altra questione;
- funge da punto di contatto per gli Interessati per tutte le questioni relative al Trattamento dei loro Dati Personali e all'esercizio dei loro diritti;
- fornisce pareri e svolge le altre attività di competenza, in base alle procedure aziendali in vigore, nell'ambito dei processi di definizione dei termini di conservazione dei Dati Personali (rif. par. 3.4.2.3), di valutazione e notifica di un *Data Breach* (rif. par. 3.4.2.10) e di svolgimento di una DPIA (rif. par. 3.4.2.6).

3.4.1.6 Funzione Privacy (e Funzione Qualità Acquisti, Sicurezza e Supporto DPO di Arca Vita per quest'ultima e le sue controllate italiane)

Funzioni che supportano, per quanto di competenza, il DPO nello svolgimento dei compiti ad esso attribuiti e svolgono altresì un'attività di supporto nella definizione e nella implementazione degli interventi necessari.

3.4.1.7 Delegato *Privacy*

Il Delegato *Privacy*:

- dà esecuzione alle linee di indirizzo definite dal Consiglio di Amministrazione, curando la progettazione, realizzazione e gestione del sistema di controllo interno e di gestione del rischio *privacy*, e verificandone costantemente l'adeguatezza e l'efficacia;
- designa il Referente *Privacy*, che non può coincidere con il Delegato *Privacy* stesso;
- cura l'adattamento di tale sistema alla dinamica delle condizioni operative e del panorama legislativo e regolamentare;
- verifica che il Consiglio di Amministrazione sia periodicamente informato sull'efficacia e sull'adeguatezza del sistema dei controlli interni e di gestione del rischio *privacy* e comunque tempestivamente ogni qualvolta siano riscontrate criticità significative;
- notifica tempestivamente al Garante e, eventualmente, comunica agli Interessati, previo parere del DPO, la violazione di Dati Personali (rif. par. 3.4.2.10).

3.4.1.8 *Process Owner*

Il *Process Owner* coordina le operazioni di Trattamento di Dati Personali effettuate nell'ambito del ruolo cui è preposto e presidia il rischio *privacy* in relazione alla propria area di responsabilità, anche avvalendosi del supporto del Referente *Privacy*.

Il *Process Owner*:

- individua le modalità da seguire nell'ambito dell'area di propria responsabilità affinché il Trattamento dei Dati Personali avvenga nel pieno rispetto delle disposizioni della Normativa *Privacy* e delle disposizioni interne di Gruppo, con particolare riferimento ai principi di liceità, correttezza e trasparenza, minimizzazione dei dati, esattezza, limitazione della conservazione ed integrità e riservatezza;
- individua le modalità da seguire affinché la raccolta dei Dati Personali avvenga con la previa comunicazione all'Interessato delle informazioni previste dal GDPR e con l'acquisizione, ove necessario, del consenso dell'Interessato (rif. par. 3.4.2.2);
- organizza e predispone misure idonee a garantire, nell'ambito delle Aree/Direzioni/Funzioni aziendali attribuitegli, l'effettivo esercizio dei diritti da parte degli Interessati (rif. par. 3.4.2.4), provvedendo, in conformità alle procedure aziendali, a collaborare con il DPO per fornire tempestivo riscontro alle relative richieste;
- garantisce l'adozione delle misure tecniche ed organizzative adeguate per garantire un livello di sicurezza proporzionato al rischio tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del Trattamento, come anche del rischio per i diritti e le libertà degli Interessati;
- coordina, avvalendosi del supporto e delle Aree/Direzioni/Funzioni aziendali competenti, il processo di avvio di un nuovo Trattamento o di modifica di un Trattamento già in essere (rif. par. 3.4.2.5 e par. 3.4.2.6);
- adotta le misure idonee a garantire che la comunicazione e la diffusione dei Dati Personali avvengano nel rispetto della Normativa *Privacy*;
- adotta le misure necessarie ed utili ai fini di consentire, nel caso di Trattamento di Categorie Particolari di Dati Personali e di dati relativi a condanne a condanne penali e reati, il rispetto della Normativa *Privacy*;
- adotta le misure necessarie e utili ai fini di consentire, qualora si renda necessario, il ricorso a Responsabili del trattamento e il trasferimento dei Dati Personali all'estero, nel rispetto delle condizioni previste dal GDPR.

Inoltre, il *Process Owner*:

- individua l'ambito dei Trattamenti consentiti agli Incaricati, nonché le banche dati e gli archivi cui hanno accesso, verificandone annualmente i presupposti e limiti;
- segue e controlla l'osservanza, da parte degli Incaricati che operano nell'ambito dell'area di propria responsabilità, delle misure di sicurezza previste, così come definite nelle varie disposizioni di Gruppo;
- gestisce, nei limiti dei poteri affidati, i rapporti con i fornitori terzi che comportano operazioni di Trattamento di Dati Personali rientranti nella propria area di competenza, vigilando sul loro operato, anche secondo quanto stabilito nella Politica in materia di esternalizzazione e scelta dei fornitori ("*Outsourcing Policy*");
- richiede un parere al DPO qualora intenda derogare ai Termini di conservazione definiti nell'apposita disposizione interna di Gruppo (DIG), ovvero avviare nuovi Trattamenti di Dati Personali o Trattamenti che non ritiene ricompresi nella citata DIG;
- informa tempestivamente il DPO in caso di ricevimento di richieste di informazioni o documenti,

accertamenti ed ispezioni da parte del Garante o di altre autorità giudiziarie o di polizia giudiziaria, collaborando alla predisposizione di atti, comunicazioni o istanze in materia.

3.4.1.9 Referente *Privacy*

Il Referente *Privacy* svolge un ruolo fondamentale di supporto al *Process Owner* e al DPO nelle attività operative di applicazione del Modello per la protezione dei Dati Personali, nonché di valutazione e gestione del rischio *privacy* nell'ambito di propria competenza. È designato in relazione alle sue qualità professionali, alla sua capacità di assolvere i propri compiti con autonomia e mantenendo allo stesso tempo uno stretto raccordo con il DPO. Approfondisce la conoscenza specialistica della normativa e delle prassi in materia di protezione dei Dati Personali attraverso interventi formativi dedicati.

Il Referente *Privacy*:

- è coinvolto ogni qualvolta, nella propria Area/Direzione/Funzione o società di competenza, debbano essere assunte decisioni aventi un potenziale impatto *privacy*;
- garantisce nel continuo un coordinamento con il DPO, al fine di un corretto mantenimento dei presidi di controllo all'interno dell'Area/Direzione/Funzione o società di appartenenza;
- può richiedere consulenza al DPO qualora venga a conoscenza di problematiche *privacy* presso l'Area/Direzione/Funzione o società di competenza;
- contribuisce ad aumentare la sensibilizzazione in materia di protezione dei Dati Personali all'interno dell'Area/Direzione/Funzione o società di propria competenza.

Inoltre, il Referente *Privacy*:

- cura, con la consulenza del DPO, l'attività di gestione e di riscontro alle richieste di esercizio dei diritti da parte degli Interessati (rif. par. 3.4.2.4), in ordine alla raccolta di dati, documenti e supporti, nonché alle altre operazioni che si rendano necessarie al fine di fornire riscontro agli stessi entro i termini previsti dal GDPR;
- su indicazione del *Process Owner*, aggiorna e conserva il Registro dei Trattamenti con riferimento ai Trattamenti svolti nell'Area/Direzione/Funzione o società di propria competenza (rif. par.3.4.2.8), inserendo anche il riferimento ai servizi informatici utilizzati;
- su indicazione del *Process Owner*, inserisce nel Registro dei Trattamenti i nuovi termini di conservazione una volta ricevuto il parere in merito da parte del DPO;
- fornisce supporto al *Process Owner* nelle valutazioni in caso di avvio di un nuovo Trattamento o di modifica di un Trattamento già in essere (rif. par. 3.4.2.5 e par. 3.4.2.6);
- partecipa al *team* istituito per la valutazione del rischio per i diritti e le libertà degli Interessati nell'ambito della procedura di *Data Breach* (rif. par. 3.4.2.10).

3.4.1.10 Soggetti autorizzati ai Trattamenti (o "Incaricati")

Gli Incaricati trattano i Dati Personali nell'ambito dell'Area/Direzione/Funzione o società di appartenenza operando sotto la direzione e il controllo del *Process Owner* e attenendosi alle istruzioni ricevute dal medesimo, nel rispetto della Normativa *Privacy*, nonché del Modello per la protezione dei Dati Personali. Si consultano, ove necessario, con il Referente *Privacy* designato.

Gli Incaricati sono tenuti a:

- svolgere, in modo lecito e secondo correttezza, le operazioni di Trattamento unicamente su Dati Personali necessari alle attività affidate e unicamente per le connesse finalità, nell'ambito delle mansioni assegnate nel rapporto lavorativo in essere, utilizzando a tal fine gli strumenti indicati o messi a disposizione dalla società;
- mantenere la riservatezza sui Dati Personali di cui vengano a conoscenza o in possesso per le suddette attività, astenendosi dal comunicarli a soggetti esterni diversi da quelli indicati dalla società;
- trattare i Dati Personali in modo che, nel rispetto delle prassi aziendali, siano esatti, completi, se necessario aggiornati, pertinenti, necessari e non eccedenti rispetto alle finalità per le quali vengono trattati, secondo le istruzioni ricevute;
- aver cura che i Dati Personali vengano conservati in modo da consentire l'identificazione degli Interessati solo per il tempo necessario alle finalità per le quali sono stati raccolti;
- provvedere alla cancellazione dei dati nei casi previsti dalle disposizioni interne in vigore;
- custodire e controllare i Dati Personali mediante l'adozione delle misure di sicurezza previste per evitarne la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso, in modo accidentale o illegale, ai Dati Personali trasmessi, conservati o comunque trattati;
- restituire integralmente alla società i dati oggetto della propria attività o acquisiti nel corso di essa, in seguito all'eventuale cessazione del rapporto di lavoro, astenendosi dal conservare, duplicare, comunicare o diffondere tali dati.

3.4.1.11 Responsabili del Trattamento

Le Società in perimetro ricorrono unicamente a Responsabili che offrano idonee garanzie di messa in atto di misure tecniche e organizzative adeguate rispetto ai Trattamenti effettuati per loro conto, che siano in grado di soddisfare i requisiti del GDPR e che garantiscano la tutela dei diritti dell'Interessato.

I Trattamenti effettuati dal Responsabile sono disciplinati da specifici contratti che vincolano il Responsabile al Titolare e che definiscono, tra l'altro, 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 Responsabile e del Titolare (rif. par. 3.4.2.7).

3.4.1.12 Funzione Compliance and Anti-Money Laundering

La Funzione Compliance and Anti-Money Laundering:

- presenta annualmente al Consiglio di Amministrazione un programma di attività in cui, ove ritenuto opportuno dal DPO e previo accordo con il medesimo, sono indicati gli interventi da eseguire relativamente al rischio privacy*;*
- sulla base del piano di cui al punto precedente, valuta il sistema dei controlli interni in ambito *privacy* secondo il processo e le metodologie descritte nella Politica della Funzione Complianceand Anti-Money Laundering;
- informa il DPO in merito ai risultati emersi dalle attività e dalle verifiche svolte sul sistema dei controlli in ambito *privacy*;

- condivide con il DPO la Relazione che quest'ultimo presenta al Consiglio di Amministrazione con periodicità annuale, con particolare riferimento alle eventuali verifiche effettuate e concordate con il medesimo.

Inoltre, la Funzione Compliance and Anti-Money Laundering partecipa ai *team* istituiti per la valutazione del rischio per i diritti e le libertà degli Interessati nell'ambito della procedura di *Data Breach* (rif. par. 3.4.2.10).

3.4.1.13 Area Information

L'Area Information:

- effettua, con riferimento ai Servizi ICT in fase di nuova realizzazione o di reingegnerizzazione, l'analisi del rischio di sicurezza dei Dati Personali al fine di individuare le misure di sicurezza da implementare, valutandone l'efficacia;
- compie una attività di revisione almeno annuale dell'efficacia delle misure di sicurezza in atto;
- svolge le attività di competenza, in base alle procedure aziendali in vigore, nell'ambito dei processi di definizione dei termini di conservazione dei Dati Personali (rif. par. 3.4.2.3) e di valutazione e notifica di un *Data Breach* (rif. par. 3.4.2.10);
- fornisce supporto al *Process Owner* e partecipa al team istituito per la valutazione del rischio per i diritti e le libertà degli Interessati nell'ambito della procedura di DPIA (rif. par. 3.4.2.6);
- supporta il DPO, in particolare tramite il responsabile della funzione di sicurezza IT, sulle tematiche informatiche, ad esempio in materia di misure di sicurezza.

3.4.1.14 Direzione Immobiliare

La Direzione Immobiliare:

- effettua la valutazione e l'analisi del rischio di sicurezza fisica dei Dati Personali, al fine di individuare le misure di sicurezza da implementare (ad es. in materia di videosorveglianza), valutandone l'efficacia;
- svolge le attività di competenza, in base alle procedure aziendali in vigore, nell'ambito del processo di valutazione e notifica di un *Data Breach* (rif. par. 3.4.2.10);
- fornisce supporto al *Process Owner* e partecipa al *team* istituito per la valutazione del rischio per i diritti e le libertà degli Interessati nell'ambito della procedura di DPIA (rif. par. 3.4.2.6);
- supporta il DPO sulle tematiche di sicurezza fisica dei Dati Personali.

3.4.1.15 Area Risk

L'Area Risk:

- presenta annualmente al Consiglio di Amministrazione un programma di attività che intende eseguire nell'ambito del sistema di gestione dei rischi operativi, incluso il rischio *privacy*; nel programma di attività si tiene conto dei Trattamenti maggiormente esposti al rischio *privacy* individuati dal DPO;
- sulla base del programma di cui al punto precedente, identifica e valuta il rischio operativo secondo le previsioni di cui alla Politica di gestione del rischio operativo in vigore nel Gruppo;

- con riferimento al rischio *privacy*, informa il DPO in merito ai risultati emersi dalle attività svolte sul sistema di gestione dei rischi.

Inoltre, l'Area Risk partecipa ai *team* istituiti per la valutazione del rischio per i diritti e le libertà degli Interessati nell'ambito delle procedure di DPIA (rif. par. 3.4.2.6) e *Data Breach* (rif. par. 3.4.2.10).

3.4.1.16 Funzione Audit

La Funzione Audit ha il compito di valutare e monitorare l'efficacia, l'efficienza e l'adeguatezza del sistema di controllo interno e delle ulteriori componenti di governo societario, in relazione alla natura dell'attività esercitata ed al livello dei rischi assunti, la sua coerenza con le linee di indirizzo definite dal Consiglio nonché le eventuali necessità di adeguamento, anche attraverso attività di supporto e consulenza alle altre Aree/Direzioni/Funzioni aziendali.

3.4.2 Modello operativo per la protezione dei Dati Personali

Il Gruppo ha definito disposizioni interne aziendali e a livello di Gruppo che garantiscono la conformità ai requisiti della Normativa *Privacy*, formalizzandole all'interno di tre categorie di documenti.

Categoria	Breve descrizione	Tipologia documento
Linee guida di alto livello	Le politiche/linee guida di Gruppo forniscono indirizzi alle Società e alle strutture aziendali per la gestione del rischio *privacy* e definiscono processi di alto livello per tutte o parte delle Società in perimetro.	– *Policy* – *Direttive* – *DIG*
Disciplina processi	Definizione di processi e procedure delle singole Società in perimetro in attuazione delle politiche/linee guida.	– *DIS*
Regole operative	Definizione delle regole di dettaglio per l'operatività di una o più strutture aziendali della Società in perimetro, o della rete distributiva, in coerenza con la disciplina dei processi.	– *ROP* – *Circolari/Disposizioni per la rete* – *Moduli*

3.4.2.1 *Accountability*

A seguito di una forte semplificazione burocratica voluta dal Regolatore europeo (come l'eliminazione dei processi autorizzativi dell'Autorità), il Titolare è stato individuato quale soggetto competente a garantire il rispetto dei principi posti dalla nuova disciplina e a mantenerne prova nel continuo (formalizzazione), dimostrando le motivazioni che hanno portato all'adozione di determinate decisioni e documentando le scelte effettuate.

Il Gruppo ha pertanto definito un *set* di misure tecniche e organizzative, tese a garantire, e a permettere di dimostrare che il Trattamento è effettuato conformemente alla Normativa *Privacy*; tra queste: (i) la definizione del modello organizzativo, con attribuzione di ruoli e responsabilità, formalizzazione di nomine, definizione di processi, procedure e controlli tracciabili; (ii) la predisposizione ed erogazione di interventi formativi ed informativi in materia di protezione dei Dati Personali per i dipendenti e i soggetti che ricoprono ruoli specifici; (iii) la creazione di strumenti operativi di supporto.

3.4.2.2 Informative e consensi

Il Titolare fornisce all'Interessato specifiche informazioni, per garantire un Trattamento corretto e trasparente, che variano in funzione della modalità di raccolta dei Dati Personali (presso l'Interessato o ottenuti attraverso canali alternativi, ad es. fonti pubbliche).

Qualora il Trattamento sia basato sul consenso, il Titolare deve essere in grado di dimostrare che l'Interessato abbia prestato un valido consenso (rif. par. 3.2) al Trattamento dei propri Dati Personali. Il Titolare non può trattare Categorie Particolari di Dati Personali e/o dati relativi a condanne penali e reati per il perseguimento

di un proprio interesse legittimo, ma esclusivamente in presenza delle condizioni previste dal GDPR (oltre al consenso esplicito da parte dell'Interessato, ad es. quando il Trattamento è necessario per tutelare un interesse vitale dell'Interessato o di un'altra persona fisica, etc.).

Il Gruppo, al fine di adeguarsi alle previsioni sopra riportate, definisce:

- modelli di informativa e consenso in linea con i requisiti del GDPR;
- un *repository* ("*Privacy Lab*"), nell'ambito dell'intranet aziendale, in cui sono raccolti i diversi modelli in vigore e la documentazione *privacy* ufficiale del Gruppo;
- un processo operativo che disciplina l'aggiornamento/gestione dei modelli di informativa e consenso, nonché regole operative per garantire la corretta raccolta, registrazione, conservazione dei consensi e delle revoche, identificando ruoli e responsabilità affidate ad Organi/Aree/Direzioni/Funzioni aziendali della Capogruppo e delle Società in perimetro.

3.4.2.3 Termini di conservazione dei Dati Personali

Nell'ambito delle informazioni da fornire all'Interessato, il Titolare definisce il periodo di conservazione dei Dati Personali trattati, ovvero i criteri utilizzati per determinare tale periodo, decorso il quale i Dati Personali sono anonimizzati/cancellati.

Il Gruppo pertanto definisce:

- i termini di conservazione previsti dalla Normativa *Privacy* e dalle altre normative applicabili in relazione ai settori di *business* delle Società in perimetro;
- un processo operativo che disciplina le attività di determinazione, validazione e controllo di nuovi termini di conservazione (in deroga o non espressamente riconducibili a quelli identificati di cui al punto precedente), identificando ruoli e responsabilità affidate ad Organi/Aree/Direzioni/Funzioni aziendali della Capogruppo e delle Società in perimetro; il processo prevede, altresì, la valutazione da parte delle strutture competenti degli impatti informatici derivanti dall'implementazione dei nuovi termini di conservazione.

3.4.2.4 Diritti dell'Interessato

All'Interessato è garantito l'esercizio dei seguenti diritti:

- **Diritto di accesso**: diritto di ottenere dal Titolare la conferma che sia o meno in corso un Trattamento di Dati Personali che lo riguarda e in tal caso, di ottenere l'accesso ai Dati Personali e ad uno specifico set di informazioni (es. finalità del Trattamento, categorie di Dati Personali);
- **Diritto di rettifica**: diritto di ottenere dal Titolare la rettifica dei Dati Personali inesatti che lo riguardano; tenuto conto delle finalità del Trattamento, l'Interessato ha il diritto di ottenere l'integrazione dei Dati Personali incompleti, anche fornendo una dichiarazione integrativa;
- **Diritto di revoca**: diritto di revocare il proprio consenso in qualsiasi momento e con la stessa facilità con cui è accordato, senza pregiudicare la liceità del Trattamento basata sul consenso prima della revoca;
- **Diritto alla cancellazione ("diritto all'oblio")**: diritto di ottenere dal Titolare la cancellazione dei Dati Personali che lo riguardano senza ingiustificato ritardo, cui corrisponde l'obbligo del Titolare di

cancellarli senza ingiustificato ritardo qualora ricorrano determinate condizioni[11];

- **Diritto di limitazione del Trattamento**: diritto di ottenere dal Titolare, quando ricorrano determinati presupposti[12], che l'utilizzo dei suoi dati e, quindi, il Trattamento, sia limitato a quanto necessario ai fini della conservazione;
- **Diritto alla portabilità dei dati**: qualora i dati siano trattati con mezzi automatizzati, l'Interessato può richiedere[13] al Titolare di (i) ricevere "*in un formato strutturato, di uso comune, leggibile da dispositivo automatico ed interoperabile*" un sottoinsieme di Dati Personali che lo riguardano e di conservarli in vista di un ulteriore utilizzo per scopi personali su supporto personale o su *cloud* privato; o (ii) trasferirli ad altro Titolare "*senza impedimenti*" e ove ciò sia tecnicamente fattibile;
- **Diritto di opposizione**: consiste nel diritto dell'Interessato di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al Trattamento dei Dati Personali che lo riguardano effettuato per ragioni di interesse pubblico o per un legittimo interesse del Titolare, compresa la Profilazione, nonché per finalità di *marketing* diretto;
- **Diritto di non essere sottoposto ad una decisione basata unicamente sul Trattamento automatizzato**, compresa la Profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla propria persona, a meno che ricorrano determinate condizioni in deroga.

Il Titolare, tramite il Referente *Privacy* e avvalendosi della consulenza del DPO, fornisce riscontro agli Interessati a fronte delle richieste di esercitare i suddetti diritti senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa[14].

Il Gruppo, al fine di adeguarsi alle previsioni sopra riportate, definisce:

- un processo operativo che disciplina la gestione dei diritti degli Interessati, identificando ruoli e responsabilità affidate ad Organi/Aree/Direzioni/Funzioni aziendali della Capogruppo e delle Società in perimetro;
- canali appositi per veicolare e raccogliere le richieste dagli Interessati, quali ad esempio i siti *web* istituzionali della Capogruppo e delle società controllate (*form ad hoc*);
- un *repository* in cui tracciare le richieste degli Interessati gestite dal Gruppo, ivi compresa la documentazione a supporto.

[11] Ad esempio, i Dati Personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; l'Interessato revoca il consenso su cui si basa il Trattamento e non sussiste altro motivo legittimo per trattare i dati; l'Interessato si oppone al Trattamento di Dati Personali e non sussiste alcun motivo legittimo prevalente per procedere al Trattamento; etc… (cfr. art. 17).

[12] L'Interessato può esercitare tale diritto nei confronti del Titolare quando sussista almeno uno dei seguenti presupposti: (i) che il Trattamento sia illecito (ma l'Interessato non voglia la cancellazione dei propri dati); (ii) che l'Interessato abbia previamente esercitato il diritto di rettifica dei propri dati (per il periodo necessario a verificarne l'esattezza); (iii) che l'Interessato si sia opposto al Trattamento (per il tempo necessario a verificare se i motivi legittimi del Titolare del Trattamento non prevalgano su quelli dell'Interessato); (iv) che l'Interessato abbia l'esigenza di tutelare in giudizio i propri diritti (e dunque voglia prevenire la cancellazione dei dati da parte del Titolare).

[13] L'Interessato può esercitare tale diritto qualora abbia fornito egli stesso i Dati Personali e il Trattamento sia effettuato con mezzi automatizzati e sulla base del consenso o di un contratto di cui è parte.

[14] Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Il Titolare informa l'Interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta.

3.4.2.5 *Data Protection by Design* e *Data Protection by Default*

Il Titolare, sin dalla progettazione del Trattamento (*"by design"*), mette in atto misure tecniche ed organizzative adeguate[15] volte ad attuare in modo efficace i principi di protezione dei Dati Personali (rif. par. 3.2), e a integrare nel Trattamento le necessarie garanzie al fine di soddisfare i requisiti normativi e tutelare i diritti degli Interessati, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del Trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà degli Interessati costituiti dal Trattamento.

Inoltre, il Titolare garantisce che siano trattati, per impostazione predefinita ("*by default*"), solo i Dati Personali necessari per ogni specifica finalità del Trattamento. Tale obbligo vale per la quantità dei Dati Personali raccolti, la portata del Trattamento, il periodo di conservazione e l'accessibilità.

Il Gruppo, al fine di adeguarsi alle previsioni sopra riportate, definisce:

- un processo operativo che disciplina le attività per garantire la *Privacy by Design* e la *Privacy by Default,* identificando ruoli e responsabilità affidate ad Organi/Aree/Direzioni/Funzioni aziendali della Capogruppo e delle Società in perimetro;
- una metodologia di lavoro e strumenti operativi volti a valutare, in fase di avvio di qualsiasi Progetto o Modifica evolutiva (o *change*)[16], l'impatto *privacy*.

3.4.2.6 *Data Protection Impact Assessment* (DPIA)

Nell'ambito della *Data Protection by Design* sopra descritta il Titolare, anche consultandosi con il DPO, prima di procedere ad un Trattamento, quando il Trattamento possa presentare "*un rischio elevato per i diritti e le libertà delle persone fisiche*[17]" considerati la natura, l'oggetto, il contesto e le finalità del Trattamento, effettua una valutazione dell'impatto dello stesso sulla protezione dei dati - in particolare qualora sia previsto l'utilizzo di nuove tecnologie.

La DPIA non è obbligatoria per ogni singolo Trattamento ed è consentito effettuarne una complessiva per esaminare un insieme di Trattamenti simili che presentano rischi elevati analoghi (ad esempio per Trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità, rischi).

Il Titolare, inoltre, è tenuto a consultare il Garante, prima di procedere al Trattamento, qualora la DPIA indichi che il Trattamento presenterebbe un rischio elevato nonostante le misure individuate per attenuare il rischio.

Il Gruppo, al fine di adeguarsi alle previsioni sopra riportate, definisce:

- un processo operativo, che disciplina la preparazione e l'esecuzione di una DPIA, il relativo r*eporting*, nonché l'eventuale consultazione preventiva con il Garante, identificando ruoli e responsabilità affidate ad Organi/Aree/Direzioni/Funzioni aziendali della Capogruppo e delle Società in perimetro;
- una metodologia a supporto della valutazione sulla necessità di effettuare o meno una DPIA e per

[15] Ad es. la pseudonimizzazione, che consiste in un Trattamento dei Dati Personali in modo tale che non possano più essere attribuiti a un Interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali Dati Personali non siano attribuiti a una persona fisica identificata o identificabile.

[16] Per le definizioni di Progetto e di Modifica evolutiva (o *change*) si rimanda alla DIG/UGH/232 del 25 giugno 2018 adottata in adeguamento alla Normativa *Privacy*.

[17] Si considerano ad elevato rischio i Trattamenti che: (i) determinano 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 che incidono in modo analogo significativamente su dette persone fisiche; (ii) coinvolgono, su larga scala, Categorie particolari di Dati Personali o relativi a condanne penali e a reati; (iii) abbiano ad oggetto la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

l'eventuale esecuzione della DPIA.

3.4.2.7 Fornitori e contratti

Il GDPR disciplina sotto il profilo della protezione Dati Personali l'eventualità che taluni Trattamenti siano effettuati dai Responsabili, precisando i ruoli e le responsabilità in capo rispettivamente al Titolare e al Responsabile.

Il Gruppo, al fine di adeguarsi alle previsioni sopra riportate:

- predispone modelli di contratto o altri atti giuridici, comprensivi di clausole specifiche (es. trasferimento dati *extra* UE, sub-responsabili, ecc.) e allegati, che consentono un'adeguata tutela delle Società in perimetro nei confronti dei rispettivi Responsabili;
- definisce un processo operativo che disciplina la selezione e gestione dei fornitori, nonché le attività di sottoscrizione ed archiviazione dei relativi contratti, identificando ruoli e responsabilità affidate ad Organi/Aree/Direzioni/Funzioni aziendali della Capogruppo e delle Società in perimetro;
- implementa una piattaforma per la gestione dematerializzata dei contratti o altri atti giuridici e la relativa archiviazione, che funge anche da *database* per l'anagrafica dei fornitori delle Società in perimetro, con specifica indicazione di quelli che trattano Dati Personali per conto di tali Società in qualità di Responsabili.

3.4.2.8 Registro dei Trattamenti

Il Registro dei Trattamenti consente di tenere traccia di tutti i Trattamenti di Dati Personali effettuati da ognuna delle Società in perimetro, anche in qualità di Responsabile.

Il contenuto previsto dal GDPR varia a seconda che si tratti del Registro dei Trattamenti del Titolare o del Responsabile.

Il Registro del Titolare contiene: (i) il nome e i dati di contatto del Titolare, del contitolare ove applicabile, del rappresentante nell'Unione Europea del Titolare e del DPO; (ii) le finalità del Trattamento; (iii) una descrizione delle categorie di Interessati e dei Dati Personali; (iv) le categorie di destinatari a cui i Dati Personali sono stati o saranno comunicati, compresi i destinatari di Paesi Terzi od organizzazioni internazionali; (v) ove applicabile, i trasferimenti di Dati Personali verso un Paese Terzo o un'organizzazione internazionale, compresa l'identificazione del Paese Terzo o dell'organizzazione internazionale; (vi) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati; (vii) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Il Registro del Responsabile contiene, oltre al *sub* (v) e al *sub* (vii): (i) il nome e i dati di contatto del Responsabile o dei Responsabili, di ogni Titolare per conto del quale agisce il Responsabile, del rappresentante nell'Unione Europea del Titolare o del Responsabile e, ove applicabile, del DPO; (ii) le categorie dei Trattamenti effettuati per conto di ogni Titolare.

Il GDPR esonera dall'obbligo di tenere il Registro le imprese con meno di 250 dipendenti, a meno che i Trattamenti effettuati possano presentare un rischio per i diritti e le libertà dell'Interessato o consistano in Trattamenti non occasionali che includono Categorie particolari di Dati Personali o Dati Personali relativi a condanne penali e a reati.

Il Gruppo, al fine di adeguarsi alle previsioni sopra riportate:

- istituisce, tramite un apposito applicativo informatico[18], il Registro dei Trattamenti di Dati Personali per ciascuna Società in perimetro avente i requisiti anzidetti, sia in qualità di Titolare che di Responsabile (ove applicabile);
- definisce un processo operativo che disciplina le attività di aggiornamento, validazione e tenuta del Registro dei Trattamenti, identificando ruoli e responsabilità affidate ad Organi/Aree/Direzioni/Funzioni aziendali della Capogruppo e delle Società in perimetro.

3.4.2.9 Rischi e misure di sicurezza

Il Titolare e il Responsabile, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del Trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà degli Interessati, sono tenuti a mettere in atto misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio. Tali misure comprendono, a titolo esemplificativo:

- la capacità di assicurare nel continuo la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di Trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei Dati Personali in caso di incidente fisico o tecnico;
- un processo per verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del Trattamento;
- la cifratura dei Dati Personali e la pseudonimizzazione.

Il Gruppo, al fine di adeguarsi alle previsioni sopra riportate, definisce un processo operativo, e la relativa metodologia, per l'effettuazione dell'analisi del rischio[19] e per l'identificazione delle misure adeguate in relazione al rischio stesso, individuando ruoli e responsabilità.

Le misure tecniche ed organizzative adottate in relazione ad ogni Trattamento effettuato sono sinteticamente descritte nell'apposito campo del Registro dei Trattamenti e riportate in dettaglio nei documenti adottati per la disciplina del processo operativo.

3.4.2.10 Notifica di un *Data Breach*

Il Titolare è tenuto a notificare il *Data Breach* al Garante, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza. L'obbligo non ricorre qualora il Titolare sia in grado di dimostrare che sia improbabile che la violazione dei Dati Personali presenti un rischio per i diritti e le libertà degli Interessati.

Il Titolare inoltre deve comunicare all'Interessato la violazione dei Dati Personali senza indebito ritardo in caso di rischio elevato per i diritti e le libertà degli Interessati.

Il Gruppo, al fine di adeguarsi alle previsioni sopra riportate, definisce:

- un processo operativo di notifica al Garante/comunicazione agli Interessati di un *Data Breach* identificando ruoli e responsabilità affidate ad Organi/Aree/Direzioni/Funzioni aziendali della

[18] Lo strumento a supporto della gestione del Registro dei Trattamenti e del relativo processo di aggiornamento consente di tenere traccia di tutte le modifiche effettuate.

[19] Rischio per i diritti e le libertà dell'Interessato, derivante dalla distruzione, perdita, modifica, divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a Dati Personali trasmessi, conservati o comunque trattati.

Capogruppo e delle Società in perimetro;

- una metodologia di valutazione del rischio per i diritti e le libertà dell'Interessato associato al *Data Breach* oggetto di analisi e dei conseguenti obblighi di Notifica al Garante/Comunicazione agli Interessati;
- un Registro dei *Data Breach*, che comprenda la documentazione a supporto.

3.4.2.11 Trasferimento dei Dati Personali verso Paesi Terzi o organizzazioni internazionali

Il trasferimento di Dati Personali verso Paesi Terzi[20] è vietato, in linea di principio, dal GDPR, a meno che il Paese in questione garantisca un livello di protezione dei Dati Personali adeguato. La Commissione Europea ha il potere di stabilire tale adeguatezza attraverso una specifica decisione. Per quanto attiene ai Paesi non inclusi in quelli considerati adeguati, in deroga al suddetto divieto, il trasferimento verso Paesi Terzi può essere consentito anche sulla base di strumenti contrattuali che offrano garanzie adeguate.

Il Gruppo, al fine di adeguarsi alle previsioni sopra riportate, definisce un processo operativo per la gestione dei trasferimenti dei Dati Personali verso Paesi Terzi o organizzazioni internazionali, che prevede la verifica:

- dell'esistenza della decisione di adeguatezza dei Paesi Terzi da parte della Commissione Europea;
- dell'adozione, per i Paesi Terzi ritenuti non adeguati dalla Commissione Europea, di garanzie adeguate per i trasferimenti di Dati Personali, tra le quali:
- dell'adesione al "*Data Privacy Framework*", il programma statunitense che certifica l'impegno, da parte delle organizzazioni che vi aderiscono, a rispettare i principi europei di protezione dei dati e consente pertanto il trasferimento di dati tra Unione Europea e USA;
- le "*Binding Corporate Rules*" (norme vincolanti di impresa), quale strumento contrattuale approvato dalla competente Autorità di controllo volto a consentire il trasferimento tra società facenti parte dello stesso gruppo d'impresa;
- le "Clausole Contrattuali *Standard* UE", ai sensi dell'art. 46, secondo paragrafo, lettera c) del GDPR e della Decisione di Esecuzione (UE) 2021/914 della Commissione del 4 giugno 2021, tramite le quali l'importatore dei Dati Personali con sede in un Paese Terzo garantisce contrattualmente all'esportatore europeo che effettuerà il Trattamento conformemente ai principi europei di protezione dei dati anche nel Paese Terzo di destinazione[21].

[20] S'intendono i paesi al di fuori dell'Unione Europea o dello Spazio Economico Europeo.
[21] Tali clausole restano in vigore fino a loro eventuale revisione o modifica.

3.4.3 Modello architetturale per la protezione dei Dati Personali

Il Gruppo adotta un modello architetturale per la protezione dei Dati Personali che garantisce un livello di sicurezza adeguato al rischio di varia probabilità e gravità per i diritti e le libertà degli Interessati.

3.4.3.1 Classificazione e conservazione dei Dati Personali

Il GDPR richiede al Titolare di classificare opportunamente le categorie dei Dati Personali trattati, con particolare riferimento alle Categorie Particolari di Dati Personali ed ai dati relativi a condanne penali e reati. Al Titolare, infatti, è consentito trattare tali dati solo a fronte del rispetto di determinate condizioni di garanzia e in presenza di basi giuridiche tassativamente previste.

Il Titolare, inoltre, è tenuto a informare l'Interessato in merito:

- al periodo di conservazione dei Dati Personali oppure, se non è possibile, ai criteri utilizzati per determinare tale periodo;
- ai Dati Personali soggetti alla richiesta di esercizio da parte dell'Interessato del diritto alla portabilità.

Il Gruppo, al fine di adeguarsi alle previsioni sopra riportate, definisce:

- una classificazione – anche in linea con gli *standard* definiti nella Politica di Gruppo in materia di *Data Governance* e nella Politica di sicurezza delle informazioni, con riferimento alla protezione dei dati da minacce interne ed esterne – dei Dati Personali allineata alle categorie di Dati Personali sopra indicate, individuando e tenendo traccia anche dei Dati Personali soggetti a portabilità;
- i periodi di conservazione dei Dati Personali trattati dal Gruppo, conformi agli obblighi di legge (ove presenti), oppure, se non è possibile, i criteri utilizzati per determinare tale periodo (rif. par. 3.4.2.3).

3.4.3.2 Servizi Informatici

Il Gruppo dispone dell'elenco dei Servizi Informativi che trattano Dati Personali di cui le Società in perimetro sono Titolari o Responsabili. Nello specifico, il Gruppo per ciascun servizio applicativo che tratta Dati Personali, dispone di un catalogo integrato delle seguenti informazioni: processi e attività ("contenitori" del Trattamento), finalità del Trattamento, categorie di dati trattati, categorie di Interessati dal Trattamento, referenti interni per la protezione dei Dati Personali, categorie di soggetti autorizzati al Trattamento, responsabili esterni del Trattamento, eventuali comunicazioni e trasferimenti dati *extra* UE.

Il Gruppo, inoltre, dispone delle informazioni in merito alle infrastrutture (es. Building; Server) presso le quali risiedono tali dati, sia proprietarie sia di soggetti terzi. In particolare, il Titolare presta attenzione a eventuali casi in cui i Dati Personali sono archiviati o trattati al di fuori dei confini europei, adottando le opportune garanzie in funzione del Paese di riferimento per assicurare un livello adeguato di protezione dei Dati Personali trasferiti.

Si rimanda alla mappa dei Sistemi Informativi e ai Registri dei Trattamenti del Gruppo per maggiori informazioni in merito ai Trattamenti di Dati Personali collegati ai sistemi informatici.

3.4.3.3 Misure di sicurezza

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del Trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà degli

Interessati, il Titolare e il Responsabile devono mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

Il Gruppo, alla luce delle indicazioni emerse dalla valutazione dei rischi di varia probabilità e gravità per i diritti e le libertà degli Interessati connessi ai Trattamenti censiti nel Registro di ciascuna Società in perimetro, definisce un insieme di misure tecniche - logiche e fisiche - che garantiscono un livello di sicurezza adeguato (rif. par. 3.4.2.9).

POLITICA IN MATERIA DI PROTEZIONE E VALORIZZAZIONE DEI DATI PERSONALI

IMPEGNI ASSUNTI DAL GRUPPO UNIPOL PER LA PROTEZIONE E LA VALORIZZAZIONE DEI DATI PERSONALI

("*UNIPOL DATA VISION*")

[PAGINA VOLUTAMENTE LASCIATA IN BIANCO]

Indice

1 Introduzione

Il presente documento, che costituisce parte integrante della Politica in materia di protezione e valorizzazione dei Dati Personali, definisce gli impegni assunti dal Gruppo per la protezione e valorizzazione dei Dati Personali nei confronti dei clienti e di tutti gli *stakeholder*.

L'attenzione accordata da parte del Gruppo alla protezione e valorizzazione dei Dati Personali nello svolgimento del proprio *business* garantisce il rispetto dei valori del Gruppo contenuti nella Carta dei Valori e nel Codice Etico, dimostrando la responsabilità nel processo decisionale e il dialogo con gli *stakeholder*.

2 Perimetro di applicazione

Il presente allegato si applica alla Capogruppo e alle Società in perimetro.

Con riferimento alle società del Gruppo con sede legale in un Paese non appartenente all'Unione Europea, ferma restando la previsione per cui le stesse si dotano di una propria politica in materia di protezione dei Dati Personali coerente con la Politica, nell'ambito del coordinamento tra il DPO di Unipol Gruppo e i DPO individuati a livello locale, saranno condivisi gli impegni assunti dal Gruppo per la protezione e valorizzazione dei Dati Personali. Ciò affinché le società del Gruppo con sede legale in un altro Paese non appartenente all'Unione Europea possano valutare le modalità di recepimento dei predetti impegni all'interno delle rispettive politiche.

3 *Unipol Data Vision*

Sempre più spesso si parla dei dati relativi alle persone fisiche, ed in particolare di quelli connessi ai loro comportamenti, scelte, movimenti e preferenze, come punto di partenza per la creazione e lo sviluppo di prodotti, servizi e soluzioni innovative, che rispondano alle effettive preferenze dell'utente finale. Alla disponibilità dei Dati Personali e al loro utilizzo da parte di chi ne è in possesso sono quindi connesse grandi opportunità di sviluppo sociale ed economico.

Per una piena realizzazione di queste opportunità è necessario che si strutturi un rapporto trasparente ed equilibrato tra i soggetti cui i dati si riferiscono e chi, invece, utilizza questi dati. In particolare, è necessario che gli Interessati siano sempre consapevoli delle finalità per cui i loro dati sono raccolti e delle modalità con cui vengono trattati ed utilizzati, che possano avere la certezza che tali dati siano adeguatamente protetti e che siano sempre in grado di esercitare i diritti riconosciuti dalla normativa in materia di protezione dei Dati Personali. Occorre, poi, che il valore che viene creato attraverso l'analisi e l'elaborazione dei Dati Personali sia condiviso, cioè che ne possano beneficiare anche i soggetti cui i dati si riferiscono, direttamente o come parte della collettività.

Nell'ambito del Gruppo, ad esempio, l'uso dei Dati Personali da parte di una compagnia assicurativa è necessario per poter svolgere il proprio ruolo sociale, attraverso un'assunzione quanto più consapevole dei rischi, che consenta di definire tariffe adeguate, in grado di rendere sostenibile la gestione di eventuali sinistri. La sempre maggior quantità di dati che le compagnie possono raccogliere ed analizzare potrà condurre ad una sempre maggiore capacità delle imprese di assicurazioni di proteggere i propri clienti dai rischi in modo accessibile.

Nel Gruppo, in considerazione dei *business* eterogenei condotti dalle Società in perimetro (a titolo esemplificativo attività assicurativa, di noleggio a lungo termine, alberghiera), sono trattati numerosi Dati Personali, che attengono ai diversi momenti della vita delle persone fisiche, ai loro comportamenti, alle

risorse che hanno a disposizione, allo stato di salute, alle abitudini, alle preferenze. Questo aspetto avrà impatti sempre maggiori con la diffusione crescente dei nuovi dispositivi connessi (ad esempio la scatola nera per l'auto, la telematica per la casa). Le informazioni raccolte dai nuovi dispositivi connessi sono, infatti, particolarmente preziose e devono essere trattate con cura, non solo per garantire la tutela delle persone fisiche cui i dati si riferiscono, ma anche per condividere il valore che si può generare dalla loro gestione evoluta, ad esempio, con riferimento al *business* assicurativo, migliorando la prevenzione dei rischi connessi alla salute/malattia, alla sicurezza alla guida, al furto in abitazione, all'abbandono di minori in autoveicoli.

4 I cinque impegni assunti dal Gruppo per la protezione e valorizzazione dei Dati Personali

Con l'obiettivo di implementare sempre più il sistema di protezione e valorizzazione dei Dati Personali di cui il Gruppo si è dotato, comportandosi in modo trasparente con i clienti e con tutti gli *stakeholder*, con l'obiettivo di rafforzare la fiducia che questi ripongono nel Gruppo medesimo, sono stati individuati cinque impegni che il Gruppo ha assunto e intende portare avanti in questo ambito.

In particolare:

- Rispetto: il Gruppo si impegna a svolgere le attività di raccolta, analisi, impiego dei dati nel pieno rispetto dei valori che guidano il suo agire, come espressi nella sua Carta dei Valori e nel suo Codice Etico;
- Protezione: il Gruppo protegge i Dati Personali detenuti: ciò rappresenta il primo pilastro per garantire i diritti dei clienti e di tutti gli *stakeholder* con cui il Gruppo entra in contatto. In linea con quanto previsto nella Politica in materia di sostenibilità, a fronte del crescente ruolo delle tecnologie informatiche nelle attività e nei processi dell'impresa, che interessano le relazioni con gli *stakeholder*, con particolare riferimento a dipendenti e clienti, e del conseguente interscambio di dati e informazioni, il Gruppo si è impegnato a porre una costante attenzione al fine di garantire un approccio responsabile alla gestione dei dati. Tale approccio si sviluppa nel tempo in modo coerente all'evoluzione normativa, culturale e tecnologica ed è orientato ad adottare sistemi avanzati di protezione e a promuovere la consapevolezza nei propri interlocutori di come e per quali finalità i loro dati vengono utilizzati. Il Gruppo continuerà a investire risorse per mantenere aggiornato e rafforzare il sistema che tutela la sicurezza dei dati;
- Informazione: le società del Gruppo informano in modo trasparente i propri clienti circa l'uso cui saranno destinati i dati raccolti, al fine di metterli in condizione di comprendere gli impatti delle proprie scelte di condivisione dei dati.
- Comprensione: lo sviluppo di soluzioni basate sui Dati Personali e sulla loro elaborazione - quali ad esempio i sistemi di Intelligenza Artificiale (AI) - ha l'obiettivo di individuare approcci innovativi per migliorare prodotti e processi. Il Gruppo si impegna, anche quando sviluppa soluzioni tecnologiche, a mettere sempre al centro la persona e i suoi bisogni; la loro comprensione è fondamentale per chi sviluppa tali soluzioni, al fine di realizzare sistemi inclusivi e non discriminatori;
- Creazione di valore: il Gruppo ritiene che l'utilizzo dei Dati Personali rappresenti un ambito significativo di creazione di valore condiviso. In particolare, prendendo ad esempio il settore assicurativo, quale *business* predominante svolto dal Gruppo, si ritiene che l'utilizzo dei dati possa accrescere il valore per:
- i clienti, che grazie all'utilizzo dei dati possono beneficiare di una migliore comprensione da parte della società del Gruppo dei propri bisogni reali di protezione e di soluzioni che diano risposte mirate e

concrete rispetto a questi ultimi; attraverso i dati è inoltre possibile sviluppare strumenti, servizi e percorsi volti alla prevenzione e riduzione del rischio;

- il Gruppo, in ragione del fatto che la raccolta e l'utilizzo dei dati permettono una migliore conoscenza dei rischi, che comporta un'assunzione più consapevole e quindi una maggiore sostenibilità complessiva; attraverso i dati, inoltre, le compagnie assicurative sono in grado di sviluppare prodotti e servizi più efficaci nel proteggere i clienti e di offrire loro maggiori opportunità;
- la comunità, in ragione del fatto che la disponibilità dei dati da parte del Gruppo e la competenza tecnologica sviluppata supportano lo sviluppo di soluzioni che mettono a fattor comune il contributo di più attori, in particolare tramite *partnership* pubblico-privato[1], per dare risposte a bisogni della collettività.

5 Il Gruppo di lavoro per la valorizzazione dei Dati Personali

Ferme restando le previsioni in materia di protezione dei Dati Personali recepite dal Gruppo all'interno della Politica in materia di protezione e valorizzazione dei Dati Personali, nonché quanto disciplinato dalla Politica di Gruppo in materia di *Data Governance* e dalla Politica di Sicurezza delle Informazioni, il Gruppo ha provveduto a definire i propri impegni in materia di gestione responsabile dei dati nella Politica in materia di Sostenibilità, che definisce i compiti in capo al Consiglio di Amministrazione e ai Comitati Consiliari in merito alla identificazione, valutazione e gestione dei principali rischi connessi a temi di impatto ambientale, sociale e di *governance* considerati "materiali" per il Gruppo e per gli *stakeholder* di riferimento (cosiddetti fattori "ESG – *Environmental, Social and Governance*" e relativi rischi).

In tale contesto ed in linea con l'obiettivo della valorizzazione dei Dati Personali è istituito un Gruppo di lavoro (c.d. "Gruppo di lavoro *Data Ethics"*) che ha il compito, a livello di Gruppo, di: (i) comprendere e valutare l'impatto sugli *stakeholder* della valorizzazione dei Dati Personali sottesa a progetti avviati o da avviare, o ad attività di *business*, commisurandone opportunità ed impatti in un'ottica di aderenza ai valori contenuti nella Carta dei Valori e nel Codice Etico (ii) definire, caso per caso, scelte coerenti con la visione aziendale e con i richiamati valori del Gruppo.

Il Gruppo di lavoro si riunisce almeno annualmente ed è composto da Aree/Direzioni/Funzioni di Unipol Gruppo/UnipolSai che hanno un ruolo chiave per la comprensione e gestione di tali impatti: Area Innovation, Area Beyond Insurance, Area Information, Direzione Marketing & Commercial Communication e Funzione Sustainability. Al Gruppo di lavoro partecipano, inoltre, con funzione consultiva, l'Area Legal, la Funzione Compliance and Anti-Money Laundering, l'Ethics Officer e il Data Protection Officer. Quest'ultimo è chiamato ad esprimere il proprio parere in relazione ai quesiti specifici sollevati dal Gruppo di lavoro e relativi alle tematiche di protezione dei Dati Personali, ferme restando le attività che lo stesso svolge con riferimento a nuovi trattamenti o modifiche a trattamenti in essere, in linea con le previsioni della Politica in materia di protezione e valorizzazione dei Dati Personali.

[1] Si richiamano, a titolo di esempio, le *partnership* pubblico-private avviate per il miglioramento della mobilità sostenibile in città, per l'assistenza domiciliare, per l'adozione di adeguati strumenti per la valutazione, la prevenzione e la gestione dei rischi legati agli eventi catastrofali.