CASFIR
Cassa di Assistenza per prestatori di lavoro Subordinato

# MANUALE OPERATIVO PRIVACY

## Aggiornamento

Firenze, 31 marzo 2026

Via Lorenzo il Magnifico, 1 - 50129 Firenze – codice fiscale 94054630481
Uffici: Tel. 055 / 5095662 PEC: casfir@legalmail.it
Iscritta all'anagrafe dei Fondi Sanitari

Indice

## 1. Premessa

Il presente documento è emanato allo scopo di definire e regolare gli adempimenti previsti per CASFIR – Cassa di Assistenza Interaziendale per Prestatori di Lavoro Subordinato (l'"**Ente**") dal 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 "**Regolamento**" o "**GDPR**").

In particolare, il Regolamento ha introdotto alcune importanti novità in materia di *privacy*, prevedendo, *inter alia*, più ampi diritti per gli Interessati (come definiti) da una parte e una maggiore responsabilizzazione del Titolare (come definito) dall'altra.

Il presente Manuale ha l'obiettivo di definire nel dettaglio, con riguardo alle esigenze di protezione dei dati personali nell'ambito dei processi svolti dall'Ente, i processi di:

- aggiornamento, validazione e tenuta del Registro dei trattamenti;
- gestione dei rapporti con i fornitori nel processo di acquisto di beni e servizi;
- gestione di una violazione dei dati personali (Data Breach);
- protezione dei dati fin dalla progettazione (Privacy by default e by design) e di valutazione di impatto sulla protezione dei dati (DPIA);
- definizione e aggiornamento dei termini di conservazione dei dati personali;
- gestione delle richieste di esercizio dei diritti da parte degli interessati.

Il presente documento potrà essere oggetto di modifiche e/o integrazioni a seguito di ulteriori provvedimenti normativi ed interpretativi in materia da parte dei competenti enti ed autorità o al seguito di cambiamenti organizzativi.

## 2. Definizioni e terminologia

| | |
|---|---|
| ***Accountability*** | Principio generale previsto dall'art. 5, co. 2 del Regolamento, che comporta l'individuazione del Titolare 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. |
| **Garante o Autorità di controllo** | Il Garante per la protezione dei dati personali, ovvero l'Autorità di Controllo nazionale in materia di protezione dei dati personali. |

| | |
|---|---|
| **Categorie particolari di dati personali** | Dati personali (come definiti) che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o i dati che rivelano l'orientamento sessuale della persona. |
| ***Change o* Modifica Evolutiva** | Attività/iniziativa che comporta modifiche a processi esistenti dell'Ente, ovvero a Servizi IT (come definiti). Sono ricomprese anche le modifiche evolutive tecnologiche, quali cambi di strumenti o di piattaforma tecnologica in quanto tali modifiche possono implicare variazioni nella gestione della sicurezza dei dati personali. |
| **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. |
| **Comitato europeo per la protezione dei dati (EDPB)** | Organismo dell'Unione, dotato di personalità giuridica e rappresentato dal suo presidente che garantisce l'applicazione coerente del GDPR. 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. |
| **DPO o *Data Protection Officer*** | Responsabile della protezione dei dati personali, cha ha il compito di (i) informare e fornire consulenza al Titolare o al Responsabile del trattamento, (ii) sorvegliare l'osservanza del GDPR, (iii) fornire, se richiesto, un parere sulla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento, (iv) cooperare con l'autorità di controllo e (v) fungere da punto di contatto per l'autorità di controllo e per gli Interessati. |
| **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.<br>Sono dati con un livello di criticità tendenzialmente più basso rispetto ai rischi per i diritti e le libertà degli Interessati.<br>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** | 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. |
| **Delegato *Privacy*** | Il soggetto incaricato dal Consiglio di Amministrazione di sovraintendere all'esecuzione delle linee di indirizzo definite dal Consiglio di Amministrazione medesimo, 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. |
| **Diritti** | S'intende l'insieme dei diritti dell'Interessato (come *jnfra* definito) previsti dagli artt. 15-22 del Regolamento (come di seguito definiti). |
| **Diritto alla cancellazione o Diritto all'oblio** | Diritto dell'Interessato 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. |
| **Diritto alla portabilità dei dati** | Diritto dell'Interessato, qualora i dati siano trattati con mezzi automatizzati, di richiedere 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 accesso** | Diritto dell'Interessato 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, etc.). |
| **Diritto di limitazione del trattamento** | Diritto dell'Interessato di ottenere dal Titolare, quando ricorrano determinati presupposti, che l'utilizzo dei suoi dati e, quindi, il trattamento, sia limitato a quanto necessario ai fini della conservazione. |

| | |
|---|---|
| **Diritto di non essere sottoposto ad una decisione basata unicamente sul trattamento automatizzato** | Diritto dell'Interessato 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. |
| **Diritto di opposizione** | 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 rettifica** | Diritto dell'Interessato 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 del consenso** | Diritto dell'Interessato 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. |
| **Evento** | Evento avverso accertato che può potenzialmente sottendere una violazione di dati personali. |
| **Interessato** | La persona fisica identificata o identificabile cui si riferiscono i dati personali. |
| **Minimizzazione dei dati personali** | Principio secondo cui i dati personali raccolti e trattati sono adeguati, pertinenti e limitati a quanto strettamente necessario rispetto alle finalità per le quali sono trattati. |
| **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. |
| **Organo Decisionale** | Il Presidente dell'Ente Titolare del trattamento. |
| **Parti interessate** | Gli Interessati o loro rappresentanti. |

| | |
|---|---|
| **Progetto** | Attività a carattere straordinario (ad es. progresso tecnologico rilevante o sviluppo di un nuovo modello di *business*), ovvero attività resa necessaria a seguito di cambiamenti della normativa di riferimento o dell'introduzione di nuove norme, che (i) può comportare rilevanti cambiamenti nei processi dell'Ente in essere e/o nei Servizi IT (come definiti) e (ii) si estende in un periodo temporale medio-lungo. |
| **Protezione dei dati fin dalla progettazione *("Privacy by Design")*** | Principio secondo cui il Titolare mette in atto, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, misure tecniche ed organizzative adeguate volte ad attuare in modo efficace i principi di protezione dei dati e ad integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del Regolamento e tutelare i diritti degli Interessati, tenuto 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 delle persone fisiche costituiti dal trattamento. |
| **Protezione dei dati per impostazione predefinita ("*Privacy by Default*")** | Principio secondo cui il Titolare mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, 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. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica. |
| **Referente *Privacy*** | Soggetto che fornisce, nell'ambito di propria competenza, supporto al Delegato Privacy per tutte le questioni inerenti all'applicazione della Normativa *Privacy*, nonché per un efficace governo del rischio *privacy*. |

| | |
|---|---|
| **Registro o Registro dei trattamenti** | Registro delle attività di trattamento istituito, ai sensi dell'art. 30 del Regolamento, (i) dal Titolare con riferimento alle attività svolte sotto la propria responsabilità, nonché (ii) dal Responsabile, ove applicabile, relativamente alle attività di trattamento svolte per conto del Titolare.<br>Tale obbligo non sussiste per le imprese con meno di 250 dipendenti, a meno che (i) i trattamenti effettuati possano presentare un rischio per i diritti e le libertà dell'Interessato; o (ii) consistano in trattamenti non occasionali; o (iii) includono Categorie particolari di dati personali o dati relativi a condanne penali e a reati. |
| **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 del trattamento (come definito).<br>Il Responsabile è un soggetto terzo (ad esempio la compagnia/società che fornisce servizi all'Ente), il quale effettua uno o più trattamenti di dati personali di cui è Titolare l'Ente. |
| **Servizio IT** | Insieme di risorse informatiche utilizzate da un processo dell'Ente per la ricezione, archiviazione, elaborazione, trasmissione e fruizione di ciascun insieme di informazioni e transazioni. |
| **Titolare o Titolare del trattamento** | Persona fisica o giuridica, autorità pubblica, servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.<br>Il Titolare è il Consiglio di Amministrazione dell'Ente. |
| **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. |

| | |
|---|---|
| **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[1]. |
| **Valutazione di Impatto sulla protezione dei dati *("Data Protection Impact Assessment"* o "DPIA"*)*** | Processo finalizzato ad effettuare, prima di procedere al trattamento, una valutazione dell'impatto sulla protezione dei dati personali, quando il trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, considerati la natura, l'oggetto, il contesto e le finalità dello stesso. |
| **Violazione dei dati personali (o "*Data Breach*")** | 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) |
| **WP29 o Gruppo di lavoro articolo 29 per la protezione dei dati** | Organo consultivo indipendente dell'Unione Europea per la protezione dei dati personali e della vita privata, istituito in virtù dell'articolo 29 della Direttiva 95/46/CE, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro, dal GEPD (Garante europeo della protezione dei dati), nonché da un rappresentante della Commissione. I suoi compiti sono fissati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE. Il 25 maggio 2018 il WP29 è stato sostituito dal Comitato europeo per la protezione dei dati (EDPB). |

[1] Il WP29, 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. Registro delle attività di Trattamento

Obiettivo del presente capitolo è quello di definire il processo di aggiornamento, validazione e tenuta del Registro dei trattamenti (come definito) dell'Ente.

### 3.1. Quadro normativo di riferimento

La presente procedura è stata redatta ai sensi:

i. dell'art. 30 del GDPR "Registri delle attività di trattamento";

ii. del parere del WP29 (come definito) in merito alle deroghe all'obbligo di tenuta del Registro di cui al punto precedente.

Il Registro consente di censire tutti i trattamenti di dati personali effettuati dall'Ente, anche in qualità di Responsabile (ove l'Ente rivesta tale ruolo).

La tenuta del Registro, infatti, oltre ad essere un obbligo normativo, riveste una grande importanza, sia quale presupposto per il perseguimento del principio di *Accountability*, sia in quanto il Registro deve poter essere messo a disposizione del Garante, su richiesta, per le verifiche del caso.

Da ciò ne consegue che le informazioni del Registro devono essere sempre aggiornate, accurate, complete e coerenti.

#### 3.1.1. Contenuti del Registro dei trattamenti

Il contenuto minimo del Registro dei trattamenti previsto dal Regolamento varia a seconda che si tratti del Registro del Titolare o del Responsabile.

1. I dati minimi obbligatori per il Registro del Titolare sono:
    i. il nome e i dati di contatto del Titolare e del DPO;
    ii. le finalità del trattamento;
    iii. una descrizione delle categorie di Interessati e delle categorie di dati personali;
    iv. le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari in paesi terzi od organizzazioni internazionali;
    v. ove applicabile, i trasferimenti di dati personali verso un paese terzo (al di fuori dell'Unione Europea o dello Spazio Economico Europeo) o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale;
    vi. ove possibile, i termini previsti per la cancellazione delle diverse categorie di dati;
    vii. ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative tali da garantire un livello di sicurezza adeguato al rischio per i diritti e le libertà degli Interessati.
2. I dati minimi obbligatori per il Registro del Responsabile, qualora sia necessario adottarlo, sono:
    i. ove applicabile, i trasferimenti di dati personali verso un paese terzo (al di fuori dell'Unione

Europea o dello Spazio Economico Europeo) o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale;

ii. ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative tali da garantire un livello di sicurezza adeguato al rischio per i diritti e le libertà degli Interessati;

iii. il nome e i dati di contatto del Responsabile o dei Responsabili, di ogni titolare per conto del quale agisce il Responsabile e, ove applicabile, del DPO;

iv. le categorie di trattamenti effettuate per conto di ogni Titolare.

3. Registro "esteso"

Oltre alle informazioni sopra indicate, il *format* predisposto dall'Ente (Allegato 3A) consente altresì la gestione di ulteriori informazioni che, sebbene non obbligatorie, sono considerate utili nell'ottica di una visione il più possibile completa dei trattamenti (cd. Registro "esteso"), quali ad esempio la base giuridica del trattamento dei dati personali, i mezzi e le modalità utilizzati per la raccolta e il trattamento dei dati personali.

## 3.2. Disposizioni operative

### 3.2.1. Il processo di aggiornamento, validazione e tenuta del Registro dei trattamenti (il "Processo Registro")

Il Processo Registro, per quanto concerne i nuovi trattamenti e le modifiche dei trattamenti esistenti, si attiva una volta concluse le attività disciplinate dal presente Manuale in materia di *privacy by design* e *Data Protection Impact Assessment* (rif. Capitolo 6) e si articola nelle fasi di:

1. Inserimento di un nuovo trattamento o modifica di un trattamento già esistente[2].
2. Valutazione della coerenza delle informazioni del trattamento censite.
3. Validazione e tenuta del Registro.

#### 3.2.1.1. Inserimento di un nuovo trattamento o modifica di un trattamento già esistente

Nel caso di inserimento di un nuovo trattamento, il Referente Privacy, informando il Delegato Privacy, può procedere alla compilazione del Registro, inserendo tutte le informazioni relative al trattamento in oggetto e necessarie al censimento dello stesso.

Una volta completato e consolidato il censimento del trattamento, il Referente Privacy, informando il Delegato Privacy, comunica via *mail* al DPO l'avvenuto inserimento del trattamento all'interno del Registro.

Nel caso di modifica di un trattamento esistente, il Referente Privacy, informando il Delegato Privacy, può procedere alla modifica delle informazioni direttamente all'interno del Registro.

[2] S'intendono variazioni delle caratteristiche del trattamento in oggetto (ad es. dati personali trattati, categorie di Interessati, etc.); è da ricomprendersi in tale casistica anche l'eventuale cessazione del trattamento stesso.

Il Delegato Privacy, o il Referente Privacy su indicazione del Delegato Privacy, riporta altresì tali modifiche nel campo "Note", previsto nell'ambito delle informazioni che caratterizzano ciascun trattamento.

Sia nel caso di inserimento, sia nel caso di modifica dovrà essere indicata la data di aggiornamento nella prima pagina del documento.

Al termine degli interventi, il Delegato Privacy, o il Referente Privacy su indicazione del Delegato Privacy, trasmette via mail al DPO il documento comunicando le modifiche effettuate.

#### 3.2.1.2. Valutazione della coerenza delle informazioni del trattamento censite

Una volta ricevute le sopracitate comunicazioni, il DPO valuta la coerenza dei dati inseriti/modificati entro il termine di 7 giorni lavorativi e, qualora:

- non si esprima entro il termine stabilito, le informazioni del trattamento censite sono da considerarsi confermate (silenzio assenso);
- consideri le informazioni inserite coerenti, procede a comunicare al Delegato Privacy, o al Referente Privacy, che le informazioni del trattamento censite sono confermate;
- non consideri le informazioni inserite coerenti, ne dà comunicazione motivata al Delegato Privacy, o al Referente *Privacy*, che dovrà apportare le necessarie modifiche segnalandole, come sopra specificato, nel campo "Note"; a seguito di tale attività, il Delegato Privacy, o il Referente *Privacy,* comunica via *mail* al DPO le modifiche effettuate, riattivando quindi il processo di approvazione;
- ritenga necessario svolgere ulteriori approfondimenti, ne informa, entro il termine stabilito, il Delegato Privacy o il Referente Privacy; il trattamento rimane sospeso per tutto il periodo di valutazione, al termine del quale, previa comunicazione del DPO medesimo, può essere richiesto al Delegato Privacy, o al Referente Privacy, di apportare le eventuali modifiche necessarie, riattivando quindi il processo di approvazione; viceversa il DPO comunica che le informazioni del trattamento censite sono confermate.

#### 3.2.1.3. Validazione e tenuta del Registro

Al termine del processo di valutazione da parte del DPO, il Registro viene ritenuto validato. Il documento digitale – in formato *Excel* – validato, trasmesso dal Referente Privacy, per conto del Delegato Privacy, al DPO, verrà trattenuto sia dal DPO sia dal Referente Privacy in apposite cartelle di rete.

**Allegati**

Allegato 3A - *Format* Registro dei trattamenti

## 4. Gestione dei rapporti con i fornitori nel processo di acquisto di beni e servizi

Qualora sorga per l'Ente la necessità di approvvigionarsi di un bene o di un servizio, l'Ente dovrà coinvolgere la società del Gruppo Unipol fornitrice di attività in *Service*, affinché identifichi la soluzione più idonea, verificando, tra le possibili soluzioni, se:

- l'esigenza può essere soddisfatta senza ricorrere al mercato, avvalendosi del supporto della società fornitrice del *Service*;
- sia necessario il ricorso ad un fornitore esterno, attivando il processo di acquisto.

### 4.1. Quadro normativo di riferimento

Il presente capitolo è stato redatto secondo quanto previsto dall'art. 28 del GDPR "*Responsabile del trattamento*".

### 4.2. Disposizioni operative

#### 4.2.1. Fornitura o supporto della società fornitrice del *Service*

La società fornitrice del *Service*, in considerazione delle competenze possedute e sulla base di quanto stabilito all'interno del contratto di *Service*, può supportare l'Ente mediante l'*erogazione diretta* di consulenza e pareri o di altre prestazioni. I servizi sono forniti nel rispetto delle modalità definite tramite il contratto di *Service*.

#### 4.2.2. Fornitura esterna

Le esigenze espresse dall'Ente che prevedono il ricorso al mercato, attivano un processo di acquisto, che determina una sequenza di attività, supportate da specifica documentazione accompagnatoria, che definiscono il cosiddetto ciclo passivo.

I Fornitori Esterni sono identificati tenendo conto di diversi parametri, tra cui il livello di servizio atteso, la qualità dell'offerta, i costi e i tempi di approvvigionamento, nonché il possesso di determinate tipologie di certificazioni, ove necessarie alla fornitura del bene e/o del servizio.

##### 4.2.2.1. Adeguamento contrattuale

Per valutare se in un rapporto con un Fornitore Esterno vi sia o meno trattamento di dati personali e a prescindere da quale sia il ruolo *privacy* del medesimo Fornitore Esterno (Autonomo Titolare o Responsabile del trattamento) è necessario che il Fornitore Esterno e il Referente Privacy compilino, ognuno per quanto di propria competenza, l'apposita "Scheda Privacy" (Allegato 4A), utile a comprendere la presenza di elementi rilevanti ai fini privacy nell'ambito del rapporto.

Per i rapporti con Fornitori Esterni per cui è emerso che lo stesso tratti dati personali di cui è Titolare l'Ente, è necessario che il Delegato Privacy, con il supporto del Referente, preveda specifiche tutele contrattuali, tali da garantire il medesimo livello di protezione e sicurezza garantito dall'Ente.

Il Fornitore Esterno identificato dovrà altresì presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate affinché il trattamento soddisfi i requisiti del presente Manuale e garantisca la tutela dei diritti dell'interessato (come definito).

Qualora i suddetti rapporti con Fornitori Esterni comportino trattamenti di dati personali e il Fornitore esterno rivesta il ruolo di Responsabile del trattamento, dovranno essere formalizzati per iscritto, tramite la sottoscrizione, da parte del soggetto provvisto di potere di firma, di un atto giuridico vincolante tra le parti (Data Processing Agreement o DPA). Tale atto, da allegare al contratto di fornitura del bene o del servizio, dovrà regolare (Allegato 4B):

- la materia disciplinata;
- la durata del trattamento;
- la natura e la finalità del trattamento;
- il tipo di dati personali;
- le categorie di interessati;
- i diritti del Titolare e gli obblighi del Responsabile del trattamento (anche nel caso faccia ricorso a subfornitori);
- l'eventuale trasferimento di dati all'estero;
- l'eventuale fornitura delle prestazioni tramite *cloud computing*:

l'elenco degli Amministratori di Sistema (Allegato 4C), qualora nominati dal Responsabile

**Allegati:**

- Allegato 4A - Modello Scheda Privacy
- Allegato 4B - Modello Data Processing Agreement (DPA)
- Allegato 4C - Individuazione Amministratori di Sistema

## 5. Gestione di una violazione dei dati personali (Data Breach)

Il presente capitolo ha l'obiettivo di disciplinare il processo di segnalazione e valutazione di una violazione dei dati personali (come definita), nonché dell'eventuale notifica al Garante e della Comunicazione all'interessato/i (di seguito, il "**Processo *Data Breach***").

### 5.1. Quadro normativo di riferimento

La presente procedura è stata redatta ai sensi:

- dell'art. 33 del GDPR "*Notifica di una violazione dei dati personali all'autorità di controllo*";
- dell'art. 34 del GDPR "*Comunicazione di una violazione dei dati personali all'interessato del Regolamento*";
- delle Linee Guida emanate dal WP29 (come definito) che forniscono suggerimenti e indicazioni pratiche in materia di notifica di un *Data Breach*;
- del Provvedimento del Garante sulla notifica delle violazioni dei dati personali (Data Breach) del 30 luglio 2019.

### 5.2. Disposizioni operative

Nel caso si verifichi un Evento (come definito), il soggetto che l'ha rilevato ne dà immediata comunicazione al Referente. Quest'ultimo informa tempestivamente il Delegato Privacy che, a sua volta, qualora ipotizzi che l'Evento possa aver comportato un *Data Breach*, contatta immediatamente il Presidente dell'Ente e il DPO fornendo:

- una sintetica descrizione dell'Evento,
- se disponibile, la data o il periodo in cui l'Evento si è verificato.

Il DPO analizza l'Evento insieme al Referente e al Delegato Privacy, se del caso richiedendo ai medesimi ulteriori elementi conoscitivi, e avvia le attività di valutazione, al termine delle quali fornisce un parere consultivo.

Il parere potrà:

a) escludere che l'Evento possa aver comportato un *Data Breach*: in tal caso non vengono svolte ulteriori azioni;

b) ritenere che l'Evento abbia comportato un *Data Breach* di rischio trascurabile o basso per i diritti e la libertà degli interessati – in ragione, ad esempio, (i) del fatto che il medesimo riguardi esclusivamente categorie di dati personali comuni, (ii) delle misure di sicurezza adottate a protezione dei dati (es. sistemi di crittografia dei dati personali che presentano un elevato grado di sicurezza), oppure (iii) del tempo (non superiore alle 12 ore) necessario a rispristinare completamente la situazione antecedente all'Evento – dando indicazione sulla necessità o meno di procedere con la Notifica al Garante;

c) ritenere che l'Evento abbia comportato un *Data Breach* di rischio più elevato o comunque, in ragione delle circostanze, sia opportuno procedere con ulteriori azioni.

Nei casi b) e c) è dal momento dell'invio del parere del DPO che si considera attestata l'esistenza del *Data Breach* e, pertanto, inizia a decorrere il termine di 72 ore, prescritto dall'art. 33 del GDPR, per effettuare l'eventuale Notifica al Garante/Comunicazione agli Interessati. Il Presidente dell'Ente, cui spetta il ruolo di Organo Decisionale, sentito il parere del DPO, informa il CdA dell'Ente dell'accaduto e delle decisioni prese.

### 5.2.1. Notifica al Garante

Il DPO predispone la Notifica al Garante per la violazione accertata che dovrà contenere, ai sensi dell'art. 33 del GDPR, almeno le seguenti informazioni:

- la descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati nonché le categorie e il numero approssimativo di registrazioni dei dati personali;
- il nome e i dati di contatto del DPO o di altro punto di contatto presso cui ottenere più informazioni;
- la descrizione delle probabili conseguenze della violazione dei dati personali;
- la descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Nel caso in cui la raccolta delle informazioni e la valutazione della violazione, per la loro complessità e onerosità, abbiano comportato il superamento del termine per la Notifica, quest'ultima dovrà essere opportunamente corredata con le motivazioni che hanno indotto il ritardo.

Il DPO sottopone la propria proposta al Presidente dell'Ente, inviando il testo della Notifica per l'approvazione.

### 5.2.2. Comunicazione agli Interessati

Il DPO valuta, in base alla numerosità e tipologia degli Interessati, il contenuto della comunicazione e le modalità di invio:

- invio di una comunicazione personale agli Interessati attraverso il mezzo considerato più idoneo (es. posta ordinaria, *email*, SMS, ecc.);
- comunicazione pubblica, o simile, sui *media* ritenuti più idonei (es. siti istituzionali dell'Ente, quotidiani, ecc.), da effettuarsi solo in casi considerati molto gravi ed eccezionali qualora la violazione di dati personali abbia coinvolto un numero elevato, se non tutti, di Interessati al trattamento;

Il DPO sottopone la propria proposta al Presidente dell'Ente, inviando il testo della Comunicazione per l'approvazione.

### 5.2.3. Validazione e Invio del testo della Notifica al Garante ed eventualmente della Comunicazione agli Interessati

Il Titolare, nella persona del Delegato Privacy, sottoscrive il testo e procede all'invio della Notifica al Garante e della eventuale Comunicazione agli Interessati.

### 5.2.4. Archiviazione nel Registro *Data Breach*

Le informazioni relative ad ogni *Data Breach* avvenuto, indipendentemente dal fatto che sia stato notificato al Garante o eventualmente comunicato agli Interessati sono archiviate nel Registro *Data Breach* (Allegato 5A), da tenere a cura del *Delegato Privacy,* con il supporto operativo del Referente Privacy, nel quale dare evidenza delle motivazioni delle decisioni adottate.

In particolare, il Registro *Data Breach* riporta: (i) le cause del *Data Breach*, (ii) i sistemi (infrastrutturali ed applicativi) e i dati personali coinvolti, (iii) i possibili effetti sugli Interessati, nonché (iv) le misure di sicurezza adottate e da implementare.

**Allegati:**

Allegato 5A - Registro *Data Breach*

## 6. Protezione dei dati fin dalla progettazione e valutazione di impatto sulla protezione dei dati (DPIA)

Il presente capitolo disciplina il processo di *Privacy by design*, nonché, per i casi in cui si renda necessario, di Valutazione di Impatto sulla protezione dei dati ("DPIA"), come definiti (congiuntamente, il "**Processo**"). Sono fornite, altresì, indicazioni per il rispetto del principio di *Privacy by default*, come definito.

### 6.1. Quadro normativo di riferimento

La presente procedura è stata redatta ai sensi:

- dell'art. 25 del GDPR "*Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita*";
- dell'art. 35 del GDPR "*Valutazione di impatto sulla protezione dei dati*";
- dell'art. 36 del GDPR "*Consultazione preventiva*";
- delle "*Linee Guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento possa presentare un rischio elevato*", emanate dal WP29 (come definito), che forniscono nozioni, suggerimenti e indicazioni in materia di DPIA.

### 6.2. Disposizioni operative

In caso l'Ente intenda avviare un nuovo Progetto o una Modifica Evolutiva, il Delegato Privacy, con il supporto del Referente Privacy, effettua una valutazione preliminare volta a verificare la conformità del Trattamento ai principi di cui all'art. 5 del GDPR e la necessità di avviare una DPIA, secondo la metodologia riportata nell'Allegato 6B.

All'esito di tale valutazione, il Delegato Privacy, con il supporto del Referente Privacy, compila la *Check-list* per il disegno e la valutazione (Allegato 6A), volta a descrivere il Trattamento e a valutarne la necessità e la proporzionalità, in applicazione dei principi di *Privacy by Design* e *Privacy by Default*, con riferimento alla quantità dei Dati Personali raccolti, alla portata e alle modalità del Trattamento, al periodo di conservazione e all'accessibilità dei Dati Personali, al fine di verificarne l'adeguatezza e la pertinenza rispetto alle finalità perseguite.

Il Delegato Privacy, anche per il tramite del Referente Privacy, sottopone al DPO la Check-list al fine di acquisirne il parere in merito alla conformità del Progetto o della Modifica Evolutiva al GDPR. Sulla base del parere espresso dal DPO, il Delegato Privacy, anche per il tramite del Referente Privacy, procede con le azioni di disegno e valutazione del Trattamento e, qualora ne ricorrano i presupposti, avvia lo svolgimento della DPIA, avvalendosi della consulenza del DPO medesimo.

**Allegati:**

Allegato 6A - *Check-list* per il disegno e la valutazione

Allegato 6B - Determinazione della necessità di effettuare una DPIA

## 7. Definizione e aggiornamento dei Termini di conservazione dei dati personali

Con il presente capitolo sono impartite disposizioni sui Termini di conservazione dei dati personali in relazione a trattamenti di cui sia Titolare l'Ente.

In particolare, gli obiettivi perseguiti sono i seguenti:

a) indicare i Termini di conservazione previsti da normative esterne in vigore (leggi, regolamenti, provvedimenti dell'Autorità Garante per la protezione dei dati personali, norme generali, di settore, ecc.), cui l'Ente è tenuto ad attenersi. Tali Termini sono elencati nell'Allegato 7A;

b) definire il processo e i criteri per la determinazione dei Termini di conservazione nei casi non disciplinati nell'Allegato 7A.

### 7.1. Quadro normativo di riferimento

Il principio di Minimizzazione dei dati personali (come definito) è stato confermato e rafforzato dal Regolamento, che parla di "limitazione della conservazione"[3] e che prevede:

- una maggiore responsabilizzazione di ogni Ente, quale Titolare (come definito), in relazione alle misure organizzative e tecniche (i) da adottare secondo un approccio basato sul rischio (*risk-based approach*) e (ii) da documentare per dimostrare la conformità alla Normativa *Privacy*, come definita (principio di c.d. *Accountability*);
- rilevanti sanzioni pecuniarie per la violazione di tali adempimenti.

Il principio di limitazione della conservazione trova altresì applicazione:

i. nelle **informative *privacy*** fornite agli Interessati (*cfr*. artt. 13 e 14 del Regolamento), le quali sono integrate con le predette indicazioni sul periodo di conservazione dei dati personali oppure, se non è possibile, sui criteri utilizzati per determinare tale periodo, nonché sull'esistenza del Diritto alla cancellazione;

ii. nei nuovi **obblighi *Privacy by Design* e *Privacy by Default***), come definiti;

iii. nel **registro delle attività di trattamento** che l'Ente, quale Titolare (come definito), predispone e conserva secondo le disposizioni del presente Manuale (rif. Capitolo 3);

iv. nelle procedure di **DPIA** (rif. Capitolo 6), che l'Ente, quale Titolare, è chiamato a svolgere, per i trattamenti ad elevato rischio[4] e prima di procedere a tali trattamenti; con tale valutazione sono analizzati altresì i criteri utilizzati per determinare i periodi di conservazione e le procedure di cancellazione dei

[3] V. il principio della "limitazione della conservazione" di cui all'art. 5.1.e) del GDPR, secondo il quale i dati dovrebbero essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati, ferma la possibilità che i dati personali siano conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici (intendendosi per tali qualsiasi operazione di raccolta e trattamento di dati personali necessari alle indagini statistiche o alla produzione di risultati statistici. Sul punto, si precisa che la finalità statistica implica che il risultato del trattamento per finalità statistiche non siano dati personali, ma dati aggregati, e che tale risultato o i dati personali non siano utilizzati a sostegno di misure o decisioni riguardanti persone fisiche specifiche).

[4] Per trattamenti rischiosi si intendono ad esempio, i trattamenti su larga scala di dati c.d. appartenenti a Categorie particolari (come definite) e giudiziari (relativi a condanne penali e reati), nonché i trattamenti di dati relativi alla c.d. geo-localizzazione e trattamenti che prevedono attività di profilazione degli interessati.

dati personali che, in base alla Normativa *Privacy*, non potranno più essere oggetto di trattamento (*cfr.* art. 35 del Regolamento).

### 7.2. Determinazione dei Termini di conservazione

#### 7.2.1. Principi per la determinazione dei Termini di conservazione

Al fine di garantire una corretta determinazione dei Termini di conservazione devono essere osservati i seguenti principi/criteri:

- i Termini di conservazione devono essere **coerenti** con le finalità dei trattamenti determinate, esplicite e legittime;
- i Termini di conservazione devono tendere al **minimo indispensabile** per il conseguimento delle finalità dei trattamenti;
- i Termini di conservazione sono **legittimati**, oltre che dal consenso dell'Interessato, dalla necessità di dare esecuzione ad un contratto, adempiere a un obbligo legale, eseguire un compito di interesse pubblico, perseguire un legittimo interesse del Titolare, ovvero per accertare, esercitare o difendere un diritto in sede giudiziaria.

#### 7.2.2. Deroghe ai Termini di conservazione di cui all' Allegato 7A

I Termini di conservazione indicati nell'Allegato 7A possono essere derogati, come di seguito precisato:

- **aumentati** (se minimi), qualora la finalità del trattamento ne giustifichi tempi di conservazione più elevati, sulla base di un'analisi adeguatamente motivata e documentata.

  Potrebbero infatti emergere ulteriori, legittime e motivate esigenze a livello operativo, amministrativo, contabile e fiscale, organizzativo, tecnico e di sicurezza, per le quali sia effettivamente giustificato e necessario, in rapporto alle peculiarità del settore di riferimento, conservare, per periodi temporali più ampi, determinate categorie di dati personali.

  Inoltre, con riguardo a specifiche esigenze di conservazione dei dati personali e/o dei documenti in cui sono contenuti per finalità di c.d. difesa di diritti **in sede giudiziaria**, i termini minimi di conservazione, coincidenti con i termini di prescrizione dei predetti diritti, sono aumentati in relazione alla durata della vertenza avviata, a prescindere dalla formulazione della richiesta di validazione dei Termini di conservazione.

- **ridotti** (se massimi), qualora l'analisi dei singoli trattamenti riveli la non indispensabilità della ulteriore conservazione dei dati trattati rispetto alle finalità perseguite, specie se si tratta di Categorie particolari di dati personali o dati relativi a condanne penali e reati, e sempre che tali dati non formino parte integrante di documenti per cui vige un obbligo di legge per la conservazione (es. documenti contabili, fiscali, ecc.).

### 7.3. Disposizioni operative

Qualora l'Ente intenda:

a. derogare ai Termini di conservazione (minimi o massimi) di cui all'Allegato 7A, in relazione a determinate finalità del trattamento;

oppure

b. avviare nuovi trattamenti di dati personali o trattamenti non espressamente riconducibili a quelli elencati nell'Allegato 7;

il Delegato Privacy si rivolge al DPO che attiva la procedura regolamentata di seguito.

### 7.3.1. Identificazione e validazione dei Termini di conservazione

Il Delegato Privacy effettua, con il supporto del Referente Privacy, una **verifica preliminare** dell'attività e/o del progetto cui i Termini di conservazione si riferiscono e, in particolare, delle esigenze di conservazione dei dati, al fine di individuare la specifica **finalità** per la quale si ritiene necessario mantenere i dati registrati, memorizzati o archiviati.

Tali esigenze di mantenimento dei dati – in base al settore di riferimento – possono essere di carattere operativo, normativo, amministrativo, contabile, fiscale, organizzativo, tecnico, storico, ecc.

Il Delegato Privacy, con il supporto del Referente Privacy, individua, inoltre, il/i repository dei dati cui i Termini di conservazione si riferiscono. Tale ambiente può essere identificato in sistemi applicativi, banche dati, cartelle di rete e repository documentali normalmente utilizzati nello svolgimento delle attività.

Sulla base di quanto sopra, il Delegato Privacy, con il supporto del Referente Privacy, **identifica i Termini di conservazione** ritenuti adeguati e li sottopone al DPO, formulando apposita richiesta.

Il DPO, ricevuta la richiesta di parere, procede a fornire riscontro motivato entro il termine di 15 giorni lavorativi (prorogabili a 30 nei casi di particolare complessità e che richiedono maggiori approfondimenti), fornendo altresì l'indicazione della misura (cancellazione/anonimizzazione) che si rende necessaria, identificando il perimetro dei soggetti cui il nuovo Termine deve ritenersi applicabile.

### 7.3.2. Formalizzazione e controllo periodico dei Termini di conservazione

I Termini di conservazione così individuati:

- sono riportati dal Referente *Privacy*, su indicazione del soggetto richiedente, nel Registro dei Trattamenti dell'Ente, aggiornando gli eventuali termini precedentemente indicati, attraverso le procedure in vigore (rif. Capitolo 3);
- sono verificati periodicamente dal DPO, soprattutto laddove si tratti di Categorie particolari di dati, attraverso il monitoraggio delle normative vigenti nei settori di riferimento dell'Ente e della Normativa *Privacy*, al fine di recepire eventuali variazioni e garantirne, pertanto, il costante aggiornamento.

### 7.3.3. Anonimizzazione/Cancellazione dei dati

È fatto divieto di conservare documenti/dati dell'Ente in spazi diversi da quelli indicati e messi a disposizione dall'Ente medesimo. I soggetti che, per necessità contingenti, salvino/copino tali documenti/dati dell'Ente in spazi diversi da quelli previsti sono tenuti ad effettuarne la cancellazione tempestivamente al venir meno delle esigenze che ne hanno determinato il trattamento in deroga alle disposizioni anzidette.

Il Titolare ha la responsabilità di garantire che, in un tempo ragionevole dallo scadere dei Termini di conservazione, i dati siano resi anonimi o cancellati - impedendo, pertanto, in modo irreversibile, ogni possibilità di risalire all'identificabilità dell'interessato - ove possibile in automatico, da ogni sistema, banca dati e/o archivio sia elettronico che cartaceo nonché dai supporti (ove fossero stati eventualmente copiati), e comunque non siano più oggetto di trattamento.

A tal fine l'Ente coinvolge il fornitore di Servizio IT specificando, tra l'altro, l'intervento necessario (anonimizzazione dei dati o cancellazione, ove obbligatoria), le regole (ad es. i campi dato da cancellare o anonimizzare, la frequenza dell'intervento), nonché la pianificazione schedulata dell'intervento stesso.

Il fornitore di Servizio IT ha il compito di realizzare l'intervento secondo le regole, le tempistiche e le modalità concordate con il soggetto richiedente, definendo a tal fine, eventualmente, gli interventi periodici di anonimizzazione/cancellazione.

L'Ente, con il supporto del Referente *Privacy* e del fornitore di Servizio IT, fornisce al DPO, con periodicità annuale, un *report* contenente informazioni in ordine alle misure adottate, agli interventi ancora in corso e al relativo stato di avanzamento. Si precisa che, qualora il trattamento di dati personali sia affidato ad un fornitore terzo, l'Ente è tenuto a comunicare a quest'ultimo i Termini di conservazione di cui all'Allegato 7A: tale adempimento è soddisfatto per mezzo del completamento delle attività previste al par. 4.2.2.1.

**Allegati:**

Allegato 7A - Termini di conservazione categorie di dati trattati

## 8. Gestione delle richieste di esercizio dei diritti da parte degli interessati

Il presente capitolo disciplina il processo di ricezione, gestione e riscontro alle richieste degli Interessati relative al trattamento dei propri dati personali (ad esempio richieste di informazione sulle modalità di trattamento) e aventi ad oggetto l'esercizio dei propri Diritti, come definiti (le "**Richieste**").

### 8.1. Quadro normativo di riferimento

Il presente capitolo è stato redatto ai sensi degli artt. 12 – 22 del GDPR in materia di diritti degli Interessati.

### 8.2. Ruoli e responsabilità

Il Delegato Privacy organizza e predispone misure idonee a garantire, nell'ambito delle funzioni attribuitegli, l'effettivo esercizio dei diritti da parte degli Interessati, collaborando con il DPO e, ove necessario, coinvolgendo il Referente Privacy. Il Delegato *Privacy*, o altro soggetto provvisto di poteri di rappresentanza (il "**Firmatario**"), sottoscrive inoltre il riscontro all'Interessato (ove necessario).

Il Referente *Privacy* è responsabile dell'attività di gestione e di riscontro alle Richieste.

Il DPO è il punto di contatto per le Richieste, collabora con l'Ente nell'attività di riscontro e verifica periodicamente il rispetto delle scadenze normative.

### 8.3. Disposizioni operative

Il processo è articolato nelle seguenti fasi:

1. Ricezione della Richiesta
2. Gestione della Richiesta e predisposizione del riscontro all'Interessato
3. Consulenza del DPO sul riscontro
4. Invio del riscontro all'Interessato

#### 8.3.1. Ricezione della Richiesta

Le Richieste pervengono tramite posta elettronica, alla casella *privacy* dell'Ente, gestito e monitorato dal Delegato e/o dal Referente *Privacy* e/o da soggetti da questi incaricati. Le Richieste possono altresì pervenire tramite posta cartacea presso la sede legale dell'Ente.

Le Richieste possono pervenire alla casella email *privacy* direttamente dagli Interessati o su inoltro da parte di altri soggetti che presidiano altri indirizzi di posta elettronica di competenza dell'Ente.

Qualora la Richiesta pervenga direttamente al DPO, quest'ultimo la trasmette al Referente *Privacy*.

Nei casi in cui una Richiesta contenga più argomenti anche su tematiche diverse dalla *privacy*, il Referente *Privacy* si coordina il DPO al fine di stabilire le modalità più opportune per procedere.

Qualora pervengano alla casella email *privacy* richieste che non hanno alcuna attinenza con le tematiche *privacy*, il Referente *Privacy* provvede all'inoltro delle stesse ai soggetti competenti.

### 8.3.2. Gestione delle Richieste e predisposizione del riscontro all'Interessato

L'Ente, nella persona del Delegato supportato dal Referente *Privacy*, una volta ricevuta la Richiesta e dopo averne valutato la pertinenza, provvede a:

1. assegnare alla Richiesta un numero di protocollo interno, utilizzando apposito file in formato *Excel* dedicato (Allegato 8A), specificando:
   - la tipologia di richiesta pervenuta (ad es. esercizio del Diritto di accesso);
   - la data di arrivo della Richiesta[5]; l'inserimento della data di arrivo è essenziale per il conteggio del termine di un mese prescritto dal GDPR (*cfr.* art. 12, co. 3) quale termine ultimo per fornire riscontro all'Interessato;
2. identificare l'Interessato, il soggetto eventualmente delegato o, qualora l'Interessato sia un minore, gli esercenti la potestà genitoriale, richiedendo ulteriori informazioni necessarie a confermarne l'identità qualora nutra ragionevoli dubbi, anche richiedendo un documento di riconoscimento in corso di validità. In caso di delega, inoltre, il Referente *Privacy* acquisisce copia della delega stessa;
3. richiedere l'integrazione documentale qualora la Richiesta risulti carente di qualche elemento essenziale a dare corso alla stessa;
4. condividere con il Delegato Privacy le decisioni da assumere in merito per garantire la corretta e completa gestione della Richiesta;
5. predisporre il riscontro all'Interessato in versione provvisoria;
6. trasmettere al DPO alla casella email supportodpo@unipol.it, entro 15 giorni dall'arrivo, la Richiesta, i relativi documenti che ritiene pertinenti e la versione provvisoria del riscontro di cui al punto precedente.

Qualora la Richiesta abbia ad oggetto l'esercizio del Diritto alla cancellazione, il riscontro all'Interessato tiene conto di quanto disciplinato dal presente Manuale in materia di termini di conservazione (rif. Capitolo 7).

### 8.3.3. Consulenza del DPO sul riscontro

Il DPO esamina la versione provvisoria del riscontro pervenuta e restituisce:

- entro 5 giorni, l'eventuale richiesta di integrazione e/o di chiarimenti, a cui il Referente *Privacy* fornisce tempestivo riscontro, in modo da poter concludere l'*iter* nei termini previsti dal GDPR;
- entro 10 giorni, la versione condivisa del riscontro.

### 8.3.4. Invio del riscontro all'Interessato

Il Referente *Privacy*, dopo aver sottoposto la versione condivisa del riscontro alla sottoscrizione del Firmatario, provvede all'invio all'Interessato **entro 30 giorni** dalla data di ricezione della richiesta:

- mediante comunicazione che riscontra la Richiesta;

[5] Se la Richiesta perviene tramite PEC o tramite lettera raccomandata all'indirizzo dell'Ente, si riporta la data di ricevimento sulla PEC o la data indicata nel timbro che viene apposto dall'ufficio posta dell'Ente. Per le Richieste ricevute tramite altri canali di comunicazione, si indica la data di arrivo presso l'ufficio del Referente *Privacy*.

- mediante comunicazione interlocutoria, con la quale si proroga il riscontro definitivo per ulteriori 2 mesi, qualora vi siano giustificate ragioni (complessità o numerosità delle richieste) da rappresentare all'Interessato.

La risposta (unitamente alle informazioni richieste) è trasmessa con mezzi elettronici se pervenuta tramite tale canale e salva diversa indicazione dell'Interessato.

Successivamente, il Referente *Privacy* invia al DPO alla casella email supportodpo@unipol.it copia della risposta inviata.

In casi particolari, su richiesta del DPO, il riscontro all'Interessato, sottoscritto dal Firmatario, è trasmesso direttamente dal medesimo.

**Allegati**

Allegato 8A - Format Protocollo richieste di esercizio dei diritti