ANIMA Holding S.p.A.

Privacy - GDPR

Data Applicazione 20/12/2021

Indice

1. PREMESSA E GENERALITÀ 3
1.1. OBIETTIVO DEL DOCUMENTO 3
1.2. OBIETTIVO DEL PROCESSO 3
1.3. ATTORI E RUOLI 4
2. PROCESSI 5
2.1 ANALISI DEI RISCHI 5
2.2 VALUTAZIONE DI IMPATTO (DATA PRIVACY IMPACT ASSESSMENT, DPIA) 6
2.3 REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO 7
2.4 GESTIONE NOMINE 7
2.4.1 NOMINA DEL DPO 7
2.4.2 NOMINA DEL SOGGETTO AUTORIZZATO DI I LIVELLO 7
2.4.3 NOMINA DEL RESPONSABILE 7
2.4.4 NOMINA DEI SOGGETTI AUTORIZZATI DI II LIVELLO 7
2.4.5 NOMINA DEI SOGGETTI AUTORIZZATI PARTICOLARI DI II LIVELLO 8
2.4.6 NOMINA DELL'AMMINISTRATORE DI SISTEMA 8
2.4.7 GESTIONE DELL'ATTO DI NOMINA 8
2.5 GESTIONE DELLE INFORMATIVE E RACCOLTA DEL CONSENSO 9
2.6 VALUTAZIONE DEI FORNITORI NOMINATI RESPONSABILI DEL TRATTAMENTO 11
2.7 CULTURA AZIENDALE E PROGRAMMI DI FORMAZIONE 12
2.8 GESTIONE DEI DIRITTI DELL'INTERESSATO 12
2.9 NOTIFICHE AL GARANTE PER LA PROTEZIONE DEI DATI 13
2.9.1 NOTIFICA IN CASO DI "DATA BREACH" 13
2.9.2 CONSULTAZIONE PREVENTIVA IN CASO DI RISCHIO RESIDUO ELEVATO A VALLE DELLA DPIA 14
2.10 VERIFICHE PERIODICHE 15
2.11 ACCERTAMENTI E CONTROLLI DA PARTE DEL GARANTE 15

Riferimenti

[1] AH – Ordinamento Societario
[2] AH – Policy Privacy – GDPR
[3] AH – Sicurezza informatica e protezione dei dati aziendali

Modifiche al documento

Versioni	Data	Descrizione delle Modifiche
00	24/09/2018	Prima emissione
01	09/05/2019	Adeguamento Struttura Organizzativa, nuovo DPO e approvazione CdA
02	16/06/2021	Adeguamento Struttura Organizzativa, adeguamento normativo, risoluzione Rilievo Compliance
03	20/12/2021	Revisione per risoluzione rilievo Internal Audit

Definizioni

- ***Garante*** - Autorità amministrativa indipendente che vigila sul corretto trattamento dei dati personali. A tal fine, prescrive modifiche necessarie od opportune per far adeguare i trattamenti alla disciplina vigente, segnala al Parlamento e al Governo l'opportunità di interventi normativi per tutelare gli interessati, esamina reclami, segnalazioni e ricorsi, svolge accertamenti anche su richiesta del cittadino, esegue ispezioni e verifiche.

- ***"Privacy by design" e "privacy by default"*** – protezione dei dati fin dalla progettazione e per impostazione predefinita (art. 25 GDPR).

1. Premessa e Generalità

1.1. Obiettivo del documento

Questo documento disciplina i processi in tema di trattamento dei dati personali in conformità alla politica "AH – Privacy - GDPR" (nel seguito "Policy") e delle norme vigenti in materia in conformità con il quadro normativo di riferimento in materia di protezione dei dati personali disegnato dal Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (nel seguito, "**GDPR**") relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE, come recepito in Italia dal Decreto Legislativo 101/2018.

1.2. Obiettivo del processo

I processi hanno lo scopo di assicurare il rispetto dei principi del GDPR allineando la società agli standard di mercato in materia di protezione dei dati personali.

Le norme operative contenute nel presente documento si applicano nell'espletamento di qualunque forma di trattamento di dati e valgono per tutti i dipendenti e i soggetti terzi coinvolti nel trattamento degli stessi.

Nello svolgimento delle proprie attività tutte le funzioni aziendali o i terzi incaricati sono tenuti a attenersi alle regole di ordinaria diligenza e a porre in essere comportamenti operativi conformi alla normativa vigente.

1.3. Attori e ruoli

Il modello organizzativo adottato da Anima Holding S.p.A. (la "Società") prevede i seguenti ruoli dettagliatamente illustrati nella Policy cui si rimanda.

- **Titolare del Trattamento** – la Società nella figura dell'Amministratore Delegato
- **Contitolari del Trattamento:** due o più Titolari del Trattamento che, congiuntamente, determinano le finalità e i mezzi del trattamento dei dati definendo in un atto scritto le proprie rispettive responsabilità.
- **Responsabile del Trattamento** – soggetti terzi fornitori opportunamente nominati
- **Responsabile della protezione dei dati (DPO)** – consulente esterno
- **Soggetti Autorizzati di I livello** - Responsabile della Divisione Affari Legali e Societari e Responsabile della funzione Information Technology.
- **Soggetti Autorizzati di II livello** - i dipendenti, i prestatori di lavoro temporaneo e gli stagisti
- **Soggetti Autorizzati particolari di II livello** – i Soggetti Autorizzati di II livello impiegati in una delle seguenti funzioni:
  - Affari Legali e Societari
  - Selezione, Formazione e Sviluppo
  - Amministrazione Personale
  - Segreteria di Direzione
  - Internal Audit
  - Compliance
  - Marketing Istituzionale, Comunicazione e Web.

- **Amministratore di Sistema** – personale appartenente alla funzione Information Technology appositamente nominato

Al processo partecipano le funzioni indicate nella tabella sottostante. Il coordinamento e la supervisione è affidata al "process owner".

La gestione dei rapporti con il Garante per la protezione dei dati personali è in capo al DPO, con il supporto della Divisione Affari Legali e Societari.

PRIVACY - GDPR		
PROCESSI	**PROCESS OWNER**	**ALTRI ATTORI**
ANALISI DEI RISCHI	Information Technology	DPO e la funzione aziendale di volta in volta interessata
VALUTAZIONE DI IMPATTO (DPIA)	Affari Legali e Societari DPO	Funzioni aziendali di volta in volta interessate
REGISTRO DELLE ATTIVITA' DI TRATTAMENTO	DPO	Affari Legali e Societari
GESTIONE DELLE NOMINE	Affari Legali e Societari	Amministrazione Personale Amministratori di sistema
GESTIONE INFORMATIVE E RACCOLTA CONSENSO	Affari Legali e Societari	Tabella paragrafo 2.5
VALUTAZIONE FORNITORI NOMINATI RESPONSABILI ESTERNI	Acquisti e Forniture	Affari Legali e Societari DPO e Internal Audit

CULTURA AZIENDALE E PROGRAMMI DI FORMAZIONE	Selezione, Formazione e Sviluppo Amministrazione Personale	-
GESTIONE DEI DIRITTI DELL'INTERESSATO	Affari Legali e Societari	DPO Information Technology
NOTIFICHE AL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI	Affari Legali e Societari Information Technology	DPO
VERIFICHE PERIODICHE	DPO	Soggetti autorizzati di I livello

2. Processi

In accordo alle prescrizioni del Regolamento Generale per la Protezione dei dati personali (nel seguito "**GDPR**"), la Società ha implementato i seguenti processi di conformità:

1. **Analisi dei rischi**
2. **Valutazione di impatto (Data Privacy Impact Assessment, DPIA)**
3. **Registro delle attività di trattamento**
4. **Gestione nomine**
5. **Gestione delle informative e raccolta del consenso**
6. **Valutazione dei fornitori nominati responsabili**
7. **Cultura aziendale e programmi di formazione**
8. **Gestione diritti dell'interessato**
9. **Notifiche al Garante per la protezione dei dati personali**
10. **Verifiche periodiche**

2.1 Analisi dei rischi

Ai sensi dell'art. 32 del GDPR, il Titolare del Trattamento deve dotarsi di misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio. Tali misure devono essere implementate tenendo conto dello stato dell'arte e dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché del probabile rischio per i diritti e le libertà delle persone fisiche.

Pertanto, nel proprio sistema di gestione della Privacy, la Società verifica periodicamente l'implementazione delle misure minime di sicurezza in conformità con il GDPR e con il principio di proporzionalità richiamato dal Garante, effettuando un'analisi sui potenziali rischi in relazione al trattamento dei dati personali (c.d. analisi dei rischi). Qualora necessario, la Società adotta la misura di sicurezza che garantisca la miglior tutela dei diritti e delle libertà delle persone fisiche interessate.

L'analisi dei rischi si svolge secondo le seguenti fasi:
- identificazione degli asset aziendali;
- valutazione delle minacce e delle vulnerabilità e relativi impatti sulla riservatezza, integrità e disponibilità dei dati personali;
- individuazione dell'esposizione al rischio;
- identificazione delle misure di sicurezza per mitigare i rischi.

L'analisi dei rischi viene predisposta dalla funzione Information Technology con cadenza annuale o qualora sia possibile individuare nuove minacce o vulnerabilità a seguito delle verifiche periodiche sui sistemi interni.

Le analisi dei rischi e gli esiti dei controlli di sicurezza sono opportunamente archiviati dal Responsabile dalla funzione Information Technology in apposita cartella di rete.
Per i dettagli sulle misure di sicurezza adottate da Anima Holding consultare la procedura organizzativa *AH – Sicurezza informatica e protezione dei dati aziendali – strumenti e norme di comportamento*.

2.2 Valutazione di impatto (Data Privacy Impact Assessment, DPIA)

Ai sensi dell'art. 35 del GDPR, il Titolare del Trattamento effettua una valutazione di impatto o Data Privacy Impact Assessment ("DPIA") quando un tipo di trattamento presenta un rischio elevato per i diritti e le libertà delle persone fisiche, allorché preveda l'uso di nuove tecnologie tenendo conto della natura, dell'oggetto, del contesto e delle finalità del trattamento.

Le attività di valutazione prevedono una preliminare mappatura dei trattamenti di dati personali effettuati all'interno della Società. Per ogni trattamento viene individuato il periodo di conservazione dei dati in base alle finalità del trattamento stesso, viene stabilito un grado di rischio indicato sulla base di stime concordate internamente e conformemente a quanto indicato dall'art. 32 del GDPR.

I trattamenti di dati personali per i quali il grado di rischio ad essi associato risulta elevato sono oggetto di valutazione di impatto.

Qualora i rischi connessi al trattamento oggetto della valutazione di impatto siano mitigati dalle misure tecnico-organizzative poste in essere dal Titolare del Trattamento per conformarsi alle disposizioni del GDPR mitigando o evitando in tal modo i rischi per i diritti e le libertà degli interessati, non è necessario procedere con la consultazione preventiva al Garante ai sensi dell'art. 36 del GDPR (cfr. paragrafo 2.9.2 "Consultazione preventiva in caso di rischio residuo elevato a valle della DPIA"). Viceversa, qualora a valle della valutazione di impatto, il rischio associato al trattamento rimanga elevato pur in presenza di misure tecnico-organizzative, risulta necessario procedere con l'invio della consultazione preventiva.

La responsabilità del processo di valutazione è in carico al Titolare del Trattamento.

La Società si avvale del supporto del DPO circa la necessità di procedere o meno con una valutazione di impatto del trattamento di dati personali e nell'eventuale redazione della documentazione associata, sentito il parere delle strutture interne coinvolte nei processi di trattamento dei dati personali oggetto di valutazione.

La valutazione d'impatto e tutta la documentazione associata viene redatta e condivisa con il DPO e la Divisione Affari Legali e Societari. Al termine della valutazione di impatto, la Divisione Affari Legali e Societari provvede a sottoporre la documentazione alla sigla della funzione aziendale che svolge il trattamento e alla firma del Titolare del Trattamento.

Ad ogni nuovo trattamento di dati personali, la funzione aziendale che svolge la nuova attività di trattamento (non precedentemente censita nel Registro delle attività di trattamento – cfr. paragrafo 2.3) informa tempestivamente la Divisione Affari Legali e Societari circa l'esistenza del nuovo trattamento in azienda.

La Divisione Affari Legali e Societari, a sua volta, informa prontamente il DPO per un parere circa la necessità o meno di procedere con una DPIA ai sensi dell'art. 35 del GDPR e al fine dell'aggiornamento del Registro dei trattamenti.

Le valutazioni di impatto e la relativa documentazione sono opportunamente archiviate dalla Divisione Affari Legali e Societari in apposita cartella di rete.

2.3 Registro delle attività di trattamento

I trattamenti di dati personali individuati dal Titolare del Trattamento sono contenuti nel c.d. Registro delle attività di trattamento (art. 30 GDPR).

Il Registro fornisce un quadro aggiornato dei trattamenti di dati personali in essere all'interno della Società (incluse eventuali attività svolte per conto di un altro Titolare in qualità di Responsabile del Trattamento) ed è indispensabile per ogni valutazione e analisi di rischio.
Esso costituisce, inoltre, uno strumento fondamentale per l'applicazione dei nuovi principi di *accountability* e *privacy by default* previsti dal GDPR (cfr. Policy) diventando parte integrante del sistema di gestione dei dati personali della Società e funge da garanzia di rispetto del GDPR nei confronti delle Autorità competenti.

Il Registro è custodito dal Titolare del Trattamento e, nel caso in cui intervenga un nuovo trattamento di dati personali, il DPO con il supporto della Divisione Affari Legali e Societari provvede prontamente ad aggiornarlo conservandone per sé copia.

2.4 Gestione nomine

2.4.1 Nomina del DPO

La Società si è dotata di un Data Protection Officer (DPO) di Gruppo nominato dal Titolare del Trattamento a seguito di delibera consiliare, così ai sensi dell'art. 37, comma 2 del GDPR. Il soggetto designato è un professionista del settore, esterno al Gruppo Anima.

2.4.2 Nomina del Soggetto Autorizzato di I livello

La decisione di designare uno o più Soggetti Autorizzati di I livello compete al Titolare del Trattamento il quale individua tra il personale della Società chi per esperienza, capacità ed affidabilità fornisce idonea garanzia del pieno rispetto della legge in materia.

2.4.3 Nomina del Responsabile

La nomina del **Responsabile** (come alternativa all'assunzione da parte del soggetto terzo del ruolo privacy di titolare autonomo del trattamento in aggiunta alla Società già Titolare del Trattamento) è definita in sede di contrattualizzazione con il soggetto terzo fornitore delle attività e/o dei servizi che comportano il trattamento di dati. La nomina è successiva alla verifica indicata al paragrafo 2.6 circa le garanzie del Responsabile del Trattamento richieste dall'art. 28 del GDPR. La verifica è curata dalla funzione Acquisti e Forniture.

2.4.4 Nomina dei Soggetti Autorizzati di II livello

La nomina a Soggetto Autorizzato di II livello è prevista per policy aziendale al momento di avvio della prestazione lavorativa presso la Società per tutti i dipendenti, i prestatori di lavoro temporaneo e gli stagisti (si veda Policy).

2.4.5 Nomina dei Soggetti Autorizzati particolari di II livello

La nomina a **Soggetto Autorizzato particolare di II livello** è prevista per policy aziendale al momento di avvio della prestazione lavorativa presso la Società per tutti i dipendenti, i prestatori di lavoro temporaneo e gli stagisti i quali prestino la propria attività lavorativa in uno dei seguenti Funzioni:
- Affari Legali e Societari
- Selezione, Formazione e Sviluppo
- Amministrazione Personale
- Segreteria di Direzione
- Internal Audit
- Compliance
- Marketing Istituzionale, Comunicazione e Web

2.4.6 Nomina dell'Amministratore di Sistema

La nomina ad **Amministratore di Sistema** è valutata dal Responsabile della funzione Information Technology in funzione dei soggetti che per esperienza, capacità e affidabilità sono ritenuti idonei per accedere in modo esclusivo e privilegiato alle risorse del sistema informativo aziendale.

2.4.7 Gestione dell'atto di nomina

La redazione del c.d. "atto di designazione" (nel caso di nomina del Soggetto Autorizzato di I livello) o del c.d. "atto di nomina" (negli altri casi), così come la sua modifica o la redazione dell'atto di revoca, è curata dalla Divisione Affari Legali e Societari. L'atto contiene i compiti e le istruzioni operative cui il soggetto designato/nominato deve attenersi.

Ciascun atto è firmato dal Titolare del Trattamento.

Ciascun atto è consegnato al soggetto interessato da parte di:
- **Servizio Amministrazione Personale** per la nomina del:
  - Titolare del Trattamento per la designazione dei Soggetti Autorizzati di I livello;
  - Soggetto Autorizzato di II livello e Soggetto Autorizzato Particolare di II livello.
- **Divisione Affari Legali e Societari** al Titolare del Trattamento per la designazione a Responsabile della protezione dei dati (DPO);
- **Responsabile Funzione Information Technology** per la nomina ad Amministratore di Sistema;
- **Funzione aziendale che detiene il rapporto con il soggetto terzo**, per la nomina a Responsabile del Trattamento.

I medesimi soggetti sopraelencati coordinano l'acquisizione dell'atto controfirmato per ricezione e accettazione da parte del soggetto nominato.

Le nomine sono conservate dalla **Divisione Affari Legali e Societari**, ad eccezione:
- dell'atto di nomina del Soggetto Autorizzato di I e II livello e del Soggetto Autorizzato particolare di II livello particolare, la cui conservazione è curata dalla funzione Amministrazione Personale;
- dell'atto di nomina di Amministratore di Sistema, la cui conservazione è curata dalla funzione Information Technology.

La lista degli incaricati - nel rispetto del principio di minimizzazione enunciato dal GDPR - è aggiornata con periodicità almeno annuale da parte della Servizio Amministrazione Personale al fine di:

- individuare il trattamento consentito all'incaricato,
- gestire il profilo utente e autorizzare gli accessi alle cartelle di rete e applicativi aziendali.

Ogni job rotation e nuova assunzione viene tempestivamente comunicata dal Servizio Amministrazione Personale all'Amministratore di Sistema per la creazione delle utenze con relativi accessi autorizzati dal Responsabile dell'ufficio di riferimento sulla base di quanto disciplinato nella procedura "*AH - Sicurezza Informatica e Protezione dei dati Aziendali - Strumenti e norme di comportamento*" a cui si rimanda per dettagli.
I permessi alle cartelle del fileserver, una volta autorizzati, possono essere modificati solamente attraverso richiesta scritta alla casella helpdesk@animasgr.it o dal responsabile della cartella o mettendo in conoscenza il responsabile stesso.
Con periodicità annuale, gli amministratori di sistema effettuano la riconciliazione dei permessi inviando una e-mail al responsabile della cartella che può confermare o chiedere di modificare i permessi assegnati.

L'elenco dei Responsabili del Trattamento, dei Titolari autonomi del trattamento e dei Contitolari del trattamento, è aggiornato periodicamente e conservato dalla Divisione Affari Legali e Societari. L'elenco è reso disponibile a fronte di richieste da parte degli Interessati.

L'elenco degli amministratori di sistema è conservato dal Responsabile della funzione Information Technology e riportato in apposito documento consultabile nell'area intranet aziendale nella sezione "Privacy". Esso viene reso disponibile al Garante in caso di accertamenti.

2.5 Gestione delle informative e raccolta del consenso

Come previsto dalla normativa vigente, ed in particolare dall'art. 5 GDPR, i dati personali oggetto di raccolta sono:

1. trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
2. raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'art.89, paragrafo 1 GDPR, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
3. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
4. esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
5. 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; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'art. 89, paragrafo 1 GDPR, fatta salva l'attuazione di misure tecniche e

organizzative adeguate richieste a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);

6. 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»).

Affinché un trattamento possa ritenersi lecito deve essere verificata almeno una delle seguenti condizioni:

- l'interessato abbia espresso il consenso per una o più specifiche finalità;
- sia necessario all'esecuzione di un contratto con l'interessato;
- sia necessario per adempiere a un obbligo legale incombente sul titolare;
- sia necessario per la salvaguardia degli interessi vitali dell'interessato o di altra persona fisica;
- sia necessario per l'esecuzione di un compito di interesse pubblico;
- sia necessario per il perseguimento di un legittimo interesse del titolare.

A tal fine, è sufficiente fornire all'interessato idonea informativa relativamente al trattamento dei dati personali, conformemente a quanto previsto dal GDPR (cfr. artt. 12 - 14).

Il consenso da parte dell'interessato è comunque necessario nelle seguenti ipotesi:

- i dati sono trattati per finalità diverse da quelle necessarie all'esecuzione del contratto con l'interessato e ad adempiere ad obblighi di legge (ad esempio, la comunicazione dei dati a terzi)
- l'oggetto del trattamento sono i dati personali c.d. particolari (art. 9 GDPR)

La Società ha previsto varie tipologie di informative e moduli per il consenso al trattamento dei dati personali, diversificate a seconda della finalità di trattamento, esposte nella tabella seguente:

INFORMATIVA E MODULO CONSENSO	FUNZIONE AZIENDALE RESPONSABILE DEL RAPPORTO CON L'INTERESSATO
Informativa privacy generica (pubblicata sul sito web della Società**)**	• Marketing Istituzionale, Comunicazione e Web
Informativa e consenso per la registrazione nell' area riservata del sito web della Società	• Marketing Istituzionale, Comunicazione e Web
Informativa newsletter e consenso (area riservata del sito web della Società**)**	• Marketing Istituzionale, Comunicazione e Web
Informativa e modulo consenso per esponenti aziendali	• Div. Affari Legali e Societari
Informativa e modulo consenso per i candidati alle posizioni di lavoro (primo contatto successivo all'invio del curriculum vitae)	• Risorse Umane (Selezione, Formazione e Sviluppo)
Informativa e modulo consenso per consulenti aziendali	• Funzione aziendale presso cui il consulente svolge l'attività
Informativa e modulo consenso per i dipendenti, gli stagisti e i prestatori di lavoro temporaneo	• Amministrazione Personale
Informativa e modulo consenso per incaricati c.d. particolari	• Amministrazione Personale
Informativa e modulo consenso per i fornitori di beni o servizi (se persona fisica, ditta individuale, professionista)	• Acquisti e Forniture

Il processo si articola nelle seguenti fasi:

- Redazione
- Consegna informativa
- Raccolta consenso
- Archiviazione

È compito della Divisione Affari Legali e Societari predisporre e tenere aggiornate le informative per gli interessati al trattamento e la modulistica per il consenso, previa condivisione dei contenuti con la funzione aziendale di competenza, in base al diverso ambito operativo.

Le informative sono firmate dal Titolare del Trattamento.

La consegna dell'informativa al soggetto interessato e, ove previsto, del modulo per il consenso al trattamento, avviene a cura della struttura aziendale responsabile del rapporto con il soggetto terzo, in relazione al diverso ambito operativo (cfr. tabella di cui sopra).
La raccolta del consenso dell'Interessato è curata dal servizio aziendale che detiene il rapporto con il soggetto destinatario dell'informativa.
Alla ricezione del modulo di informativa è necessario verificare che sia stato sottoscritto e sia completo della manifestazione del consenso al trattamento dei dati.

Una copia del consenso/modulo di informativa è conservata dal servizio aziendale che ha curato la raccolta del consenso.

2.6 Valutazione dei fornitori nominati Responsabili del Trattamento

La nomina a Responsabili del Trattamento ai sensi dell'art. 28 GDPR è effettuata a cura della Divisione Affari Legali e Societari, che la formalizza all'interno del contratto di fornitura.

Nel rispetto del dettato normativo, il ruolo di Responsabile del Trattamento è valutato al momento della stipula del contratto e, successivamente, viene verificata la rispondenza dello stesso ai requisiti previsti dal citato articolo 28, con le modalità sotto riportate.

Laddove il fornitore dichiari di aderire ad un codice di condotta approvato ai sensi dell'art. 40 del GDPR o a un meccanismo di certificazione approvato di cui all'art. 42 del GDPR, tale circostanza, riportata nella documentazione contrattuale, può essere utilizzata come sufficiente elemento di garanzia del responsabile esterno. In questo caso non è necessario procedere con la verifica.

Modalità di verifica dei requisiti del Responsabile del Trattamento

La verifica tende ad accertare che il Responsabile del Trattamento risponda ai requisiti previsti dall'art. 28 del GDPR e, di conseguenza:

- sia impegnato a rispettare le previsioni del GDPR;
- tratti i dati personali in conformità alle istruzioni documentate del Titolare del Trattamento;
- garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- adotti tutte le misure richieste ai sensi dell'articolo 32;
- rispetti le condizioni previste dalla nomina per ricorrere a un altro Responsabile del Trattamento;
- tenga conto della natura del trattamento, assistendo il Titolare del Trattamento con misure tecniche e organizzative adeguate, al fine di soddisfare l'obbligo del Titolare del Trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
- assista il Titolare del Trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

Annualmente la Divisione Affari Legali e Societari , in collaborazione con il Servizio Acquisti e Forniture, selezionerà almeno due fornitori da sottoporre a verifica.

Tale verifica si svolgerà attraverso l'invio di un questionario da parte del Servizio Acquisti e Forniture, che è tenuto ad assicurarsi della sua compilazione da parte del fornitore, per poi inoltrarlo al DPO. Le risposte del questionario saranno analizzate dal DPO che esprimerà il suo parere formalizzandolo in un report da condividere con la Divisione Affari Legali e Societari.

In caso di risposte non esaurienti la Divisione Affari Legali e Societari richiederà al Servizio Internal Audit di intervenire presso il fornitore per risolvere, in collaborazione con il DPO, le problematiche riscontrate. Al termine delle attività il Servizio Internal Audit predisporrà una relazione da inoltrare alla Divisione Affari Legali e Societari, tenuta alla conservazione della documentazione relativa alla verifica ex art. 28 GDPR.

I fornitori nominati Responsabili del Trattamento sono riportati in un apposito elenco tenuto dalla Divisione Affari Legali e Societari.

Al fine di monitorare la lista dei fornitori nominati Responsabili del Trattamento, la Divisione Affari Legali e Societari richiede trimestralmente la lista dei contratti attivi, aggiornata dal Servizio Acquisti e Forniture ogni qualvolta la società sottoscrive un contratto con un nuovo fornitore.

2.7 Cultura aziendale e programmi di formazione

In accordo con quanto previsto dall'art. 29 del GDPR, il personale incaricato e i profili di responsabilità in tema Privacy devono essere opportunamente formati dal Titolare del Trattamento.
Un'adeguata formazione dei soggetti deputati a trattare dati personali è considerata misura organizzativa necessaria per garantire un livello adeguato di sicurezza nel trattamento di dati personali.

La Società approva un piano formativo annuale rivolto a tutti gli incaricati del trattamento dei dati.
La formazione in tema Privacy è obbligatoria e sottoposta al personale in fase di assunzione.
In caso di necessità sono previsti corsi di aggiornamento online.

2.8 Gestione dei diritti dell'interessato

L'interessato può esercitare i propri diritti rispettando le condizioni e i limiti di legge.

Secondo il GDPR i diritti dell'interessato sono:

- Diritto di accesso ai dati
- Diritto di rettifica
- Diritto all'oblio
- Diritto di limitazione del trattamento
- Diritto alla portabilità dei dati
- Diritto di opposizione

Per le definizioni si rimanda alla Policy Privacy aziendale.

In aggiunta a quanto sopra indicato, l'art. 22 del GDPR enuncia che – laddove non richiesto per altre finalità elencate al comma 2 del medesimo articolo - l'interessato ha il diritto a non essere sottoposto a 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 sua persona.

Le istanze per l'esercizio di tali diritti possono essere inoltrate alla casella di posta elettronica dedicata dpo@animasgr.it governato dal DPO che avviserà prontamente la Divisione Affari Legali e Societari, oppure alla casella privacy@animasgr.it gestita e monitorata dalla Divisione Affari Legali e Societari.

La ricezione e la gestione della risposta all'interessato avvengono a cura della Divisione Affari Legali e Societari entro i termini previsti dal GDPR.

La Divisione Affari Legali e Societari recupera tutti i dati e le informazioni utili per poter fornire riscontro all'Interessato, avvalendosi, ove necessario, della collaborazione di altre funzioni aziendali le quali devono fornire per iscritto e con sollecitudine le informazioni in loro possesso.

Il riscontro all'Interessato è responsabilità della Divisione Affari Legali e Societari, il quale conserva la corrispondenza con l'interessato al trattamento, unitamente a tutti gli elementi conoscitivi utilizzati per fornire riscontro per un termine di dieci anni.

La replica all'Interessato viene fornita entro un mese dalla ricezione della richiesta (dunque va documentata la data di ricezione). Il termine può essere prorogato fino ad ulteriori due mesi (tre mesi totali), se necessario, tenuto conto della complessità e del numero delle richieste. Il Titolare del Trattamento informa l'Interessato di tale proroga e dei motivi del ritardo entro un mese dal ricevimento della richiesta.

Nel fornire riscontro si devono rispettare i seguenti principi:
a) facilitare l'esercizio dei diritti degli Interessati
b) fornire una risposta tempestiva
c) identificare gli Interessati qualora il Titolare del Trattamento nutra ragionevoli dubbi
d) pagamento per l'esercizio dei diritti: a seconda della richiesta, si dovrà fornire una copia dei Dati Personali oggetto di Trattamento, gratuitamente; in caso di ulteriori copie richieste dall'Interessato, il Titolare del Trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi (preferibilmente predeterminati e resi noti all'Interessato); se le richieste dell'Interessato sono manifestamente infondate o eccessive (come dimostrabile dal Titolare), in particolare per il loro carattere ripetitivo, si può: i) addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; ii) rifiutare di adempiere alla richiesta.

Le richieste dell'interessato sono archiviate dalla Divisione Affari Legali e Societari dopo aver acquisito il parere del DPO

2.9 Notifiche al Garante per la protezione dei dati

2.9.1 Notifica in caso di "data breach"

Costituisce "data breach" ai sensi del GDPR la violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

In caso di violazione (art. 33 GDPR), il Titolare del Trattamento dovrà svolgere una serie di valutazioni volte a capire se il "data breach" comporti un rischio per i diritti e le libertà delle persone fisiche coinvolte e se comporti un rischio elevato per il soggetto interessato.
A seguito di tali valutazioni, il Titolare del Trattamento dovrà:

- se la violazione comporta un rischio per i diritti e le libertà delle persone fisiche: notificare il data breach al Garante senza ingiustificato ritardo e ove possibile entro le 72 ore dal momento in cui è venuto a conoscenza della violazione;
- se la violazione comporta anche un rischio elevato per la libertà e i diritti degli interessati, comunicare, in modo tempestivo e comunque senza ingiustificato ritardo, l'evento a questi ultimi;
- se non si rilevano rischi per i diritti e le libertà delle persone fisiche, non notificare il data breach all'Autorità competente, ma tenerne traccia su un apposito registro delle violazioni ("Registro delle Violazioni"), conservando adeguata documentazione relativa all'evento e indicando le ragioni per cui si è scelto di non inviare la relativa notifica.

È compito della Divisione Affari Legali e Societari aggiornare il Registro delle Violazioni.
La funzione aziendale che venga a conoscenza di una violazione dei dati personali, la comunica preventivamente alla Divisione Affari Legali e Societari che si consulterà tempestivamente con il DPO.

Inoltre, le violazioni di sicurezza IT sono presidiate dalla funzione Information Technology tramite periodici controlli automatici e manuali di primo livello.
In caso di violazione presso i sistemi dell'outsourcer nominato Responsabile, la violazione deve essere tempestivamente comunicata dall'outsourcer alla funzione Information Technology.

La valutazione circa la necessità di inviare la notifica al Garante viene condotta secondo le seguenti logiche e considerazioni:

- identificazione del tipo di violazione (perdita, manomissione, divulgazione dei dati personali);
- valutazione della natura, sensibilità e volume dei dati personali coinvolti;
- valutazione della facilità di identificazione delle persone fisiche interessate;
- valutazione della gravità delle conseguenze per le persone fisiche interessate;
- considerando le caratteristiche delle persone fisiche interessate;
- considerando il numero di persone fisiche coinvolte;
- considerando le caratteristiche del titolare del Trattamento e della tipologia di dati personali trattati.

La notifica al Garante viene curata dal Titolare del Trattamento che si avvarrà dell'ausilio del DPO in conformità a quanto richiesto dalla normativa.

2.9.2 Consultazione preventiva in caso di rischio residuo elevato a valle della DPIA

Secondo il GDPR, il Titolare del Trattamento deve obbligatoriamente consultare l'autorità di controllo – prima di procedere con il trattamento - qualora l'esito della valutazione d'impatto sulla protezione dei dati (a norma dell'art. 35 del GDPR e disciplinata dai processi al paragrafo 2.2 della presente procedura) evidenzi un rischio residuo elevato (c.d. consultazione preventiva).

Il Titolare del Trattamento comunica al Garante:
- ove applicabile, le responsabilità del Titolare del Trattamento, dei contitolari e dei Responsabili del Trattamento;
- le finalità e i mezzi del trattamento previsto;
- le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati;
- i dati di contatto del titolare della protezione dei dati;
- la valutazione d'impatto sulla protezione dei dati di cui all'articolo 35;
- ogni altra informazione richiesta dall'autorità di controllo

L'autorità di controllo fornisce, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto al Titolare del Trattamento e al Responsabile del Trattamento.
L'autorità di controllo può prorogare di sei settimane il periodo predetto, tenendo conto della complessità del trattamento previsto. L'autorità di controllo ha tuttavia il dovere di informare il Titolare del Trattamento e, ove applicabile, il Responsabile del Trattamento di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione.

Fino all'ottenimento del parere da parte dell'Autorità di controllo non è possibile procedere al trattamento dei dati personali oggetto della consultazione preventiva.

2.10 Verifiche periodiche

Ai sensi del GDPR, è compito del DPO, con il supporto dei Soggetti Autorizzati di I livello (per le parti di rispettiva competenza) effettuare, nell'ambito di una pianificazione annuale condivisa con il Titolare del trattamento, delle attività di verifica[1] al fine di individuare eventuali carenze di conformità delle policy e delle prassi aziendali, assicurandosi del buon esito delle azioni correttive poste a carico delle funzioni interne di volta in volta coinvolte.

2.11 Accertamenti e controlli da parte del Garante

In virtù dei poteri di accertamento e controllo di cui è dotato, il Garante privacy può:

- richiedere informazioni e documenti;
- accedere a banche dati e archivi ed effettuare ispezioni e verifiche nei luoghi dove si svolgono i trattamenti;
- ingiungere al Titolare del Trattamento e al Responsabile del Trattamento di fornire ogni informazione di cui necessiti per l'esecuzione dei suoi compiti;
- condurre indagini sotto forma di attività di revisione sulla protezione dei dati;
- notificare al Titolare del Trattamento o al Responsabile del Trattamento le presunte violazioni del presente regolamento;
- ottenere, dal Titolare del Trattamento o dal Responsabile del Trattamento, l'accesso a tutti i dati personali e a tutte le informazioni necessarie per l'esecuzione dei suoi compiti;
- ottenere accesso a tutti i locali del Titolare del Trattamento e del Responsabile del Trattamento, compresi tutti gli strumenti e mezzi di trattamento dei dati, in conformità con il diritto dell'Unione o il diritto processuale degli Stati membri.

Inoltre, il Garante ha i seguenti poteri correttivi:
- rivolgere avvertimenti al Titolare del Trattamento o al Responsabile del Trattamento sul fatto che i trattamenti previsti possono verosimilmente violare le disposizioni del presente regolamento
- rivolgere ammonimenti al Titolare e del Trattamento o al Responsabile del Trattamento ove i trattamenti abbiano violato le disposizioni del presente regolamento;
- ingiungere al Titolare del Trattamento o al Responsabile del Trattamento di soddisfare le richieste dell'interessato di esercitare i diritti loro derivanti dal presente regolamento;
- ingiungere al Titolare del Trattamento o al Responsabile del Trattamento di conformare i trattamenti alle disposizioni del presente regolamento, se del caso, in una determinata maniera ed entro un determinato termine;

[1] Tali verifiche dovranno prevedere un'informativa da rilasciare nel corso dell'anno ai Soggetti Autorizzati di I livello informando altresì la funzione Internal Audit.

- ingiungere al Titolare del Trattamento di comunicare all'interessato una violazione dei dati personali;
- imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento;
- ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento a norma degli articoli 16, 17 e 18 e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali ai sensi dell'articolo 17, paragrafo 2, e dell'articolo 19;
- infliggere una sanzione amministrativa pecuniaria
- ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.

Le attività possono avere origine da:

- segnalazioni o reclami ricevuti dal Garante da parte degli interessati;
- esigenze di ulteriori approfondimenti emerse nell'ambito dell'esame di ricorsi;
- iniziativa dell'Autorità;
- controlli a campione, per verificare lo stato di attuazione della legge in determinati settori.

La tenuta dei rapporti con il Garante Privacy e il coordinamento delle attività derivanti dagli eventuali accertamenti e controlli richiesti, compete al DPO con il supporto della Divisione Affari Legali e Societari, coadiuvato se necessario da altre funzioni aziendali in base all'ambito di competenza.