MANUALE PER LA GESTIONE E PROTEZIONE DEI DATI PERSONALI DI FURRER SPA

ai sensi del Regolamento UE n. 679/2016

Il "**Manuale per la Gestione e la Protezione dei Dati Personali** "(d'ora in avanti **"***Manuale Privacy***"**) della FURRER S.P.A. (di seguito anche "FURRER") è stato:

- approvato dal Titolare del Trattamento dei dati in data 23 maggio 2018;

Il presente Manuale deve essere aggiornato ogni anno e tempestivamente modificato a cura del Titolare del Trattamento dei dati qualora nel corso dell'anno dovessero insorgere modifiche normative o organizzative della FURRER oppure anomalie applicative delle misure di sicurezza adottate o qualora dovessero ravvisarsi inadeguatezze protettive derivanti dall'emersione di nuovi rischi in materia di Privacy

Sommario

1. PREMESSA

Con il Regolamento Europeo 679/2016 o General Data Protection Regulation cambia radicalmente l'approccio di compliance normativo alla Privacy. A seguito dell'introduzione del Regolamento UE, è stato, infatti, introdotto il concetto della Privacy by Design (Tutela del dato fin dalla progettazione) che riguarda il principio di incorporazione della privacy a partire dalla progettazione di un processo aziendale e della Privacy by Default (Tutela della privacy per impostazione predefinita) che prevede il porre in essere di misure tecniche e organizzative adeguate.

Da ciò scaturisce l'esigenza di implementare uno specifico Sistema di Gestione della Privacy, che si fonda su un adeguato processo di Risk Assessment finalizzato alla valutazione del rischio Privacy (cd. Data Privacy Impact Assessment) e degli specifici principi di "Accountability".

2. OBBIETTIVI DEL MANUALE DI GESTIONE PRIVACY

FURRER è sensibile all'esigenza di assicurare condizioni di liceità, correttezza e trasparenza nella protezione dei dati personali nella conduzione delle sue attività aziendali, a tutela dei diritti dei dipendenti, clienti e fornitori ed è, altresì, consapevole dell'importanza di dotarsi di un Sistema di Gestione Privacy ai sensi del GDPR.

A tal fine, FURRER ha intrapreso un progetto di analisi dei dati trattati, dei propri strumenti organizzativi, di gestione e di controllo, volto a verificare la corrispondenza dei principi comportamentali e delle procedure alle finalità previste dal Regolamento UE e, se necessario, ad integrare quanto già esistente.

Attraverso l'adozione del presente Sistema di Gestione Privacy, FURRER intende, quindi:

- adempiere compiutamente alle previsioni di legge ed ai principi ispiratori del Regolamento UE attraverso l'implementazione di un sistema strutturato ed organico di procedure ed attività di controllo (ex ante ed ex post) volto a prevenire e presidiare i rischi privacy;
- costituire uno strumento efficace di gestione aziendale, riconoscendo al presente Sistema di Gestione anche una funzione di creazione e protezione del valore della FURRER stessa tramite la protezione dei dati personali.

Infatti, attraverso l'adozione del presente Manuale di Gestione Privacy, FURRER propone di:

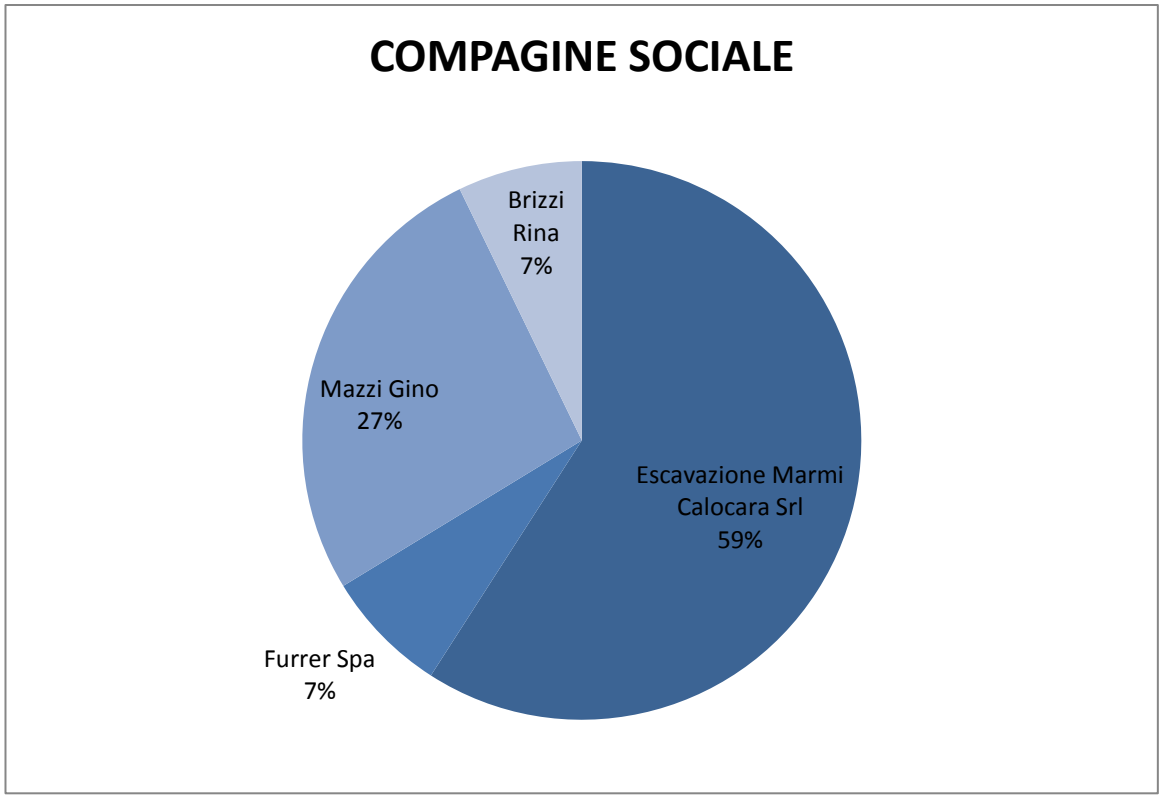
- consolidare una cultura della prevenzione del Rischio Privacy e del controllo nell'ambito del raggiungimento degli obiettivi aziendali;
- fornire adeguata informazione ed istruzioni ai terzi che gestiscono i dati per conto di FURRER;
- diffondere ed affermare una cultura d'impresa improntata alla legalità, con l'espressa riprovazione da parte della FURRER di ogni comportamento contrario alla legge o alle disposizioni interne ed, in particolare, alle disposizioni contenute nel Regolamento UE e nel presene Sistema di Gestione;
- prevedere un sistema di monitoraggio costante dell'attività aziendale volto a consentire alla FURRER di prevenire o impedire la commissione di illeciti in materia di Privacy;

A tal fine, il Manuale prevede misure adeguate a migliorare l'efficienza e l'efficacia nello svolgimento delle attività nel costante rispetto della legge individuando misure dirette ad eliminare tempestivamente situazioni di Rischio di violazioni Privacy.

3. FURRER SPA

La Società, fondata nel 1939, svolge la propria attività nel settore dell'estrazione della lavorazione, della trasformazione e della commercializzazione di prodotti lapidei di produzione nazionale ed estera, marmo, granito e onice.

La compagine sociale è composta dalla Società Escavazione Marmi Calocara S.r.l., che detiene il 59,09% del capitale sociale, dalla stessa Furrer S.p.a., che detiene il 7,2% del capitale, dal Dott. Mazzi Gino, che detiene il 26,52% del capitale e dalla Signora Brizzi Rina, che detiene il restante 7,2%, come di seguito rappresentato.

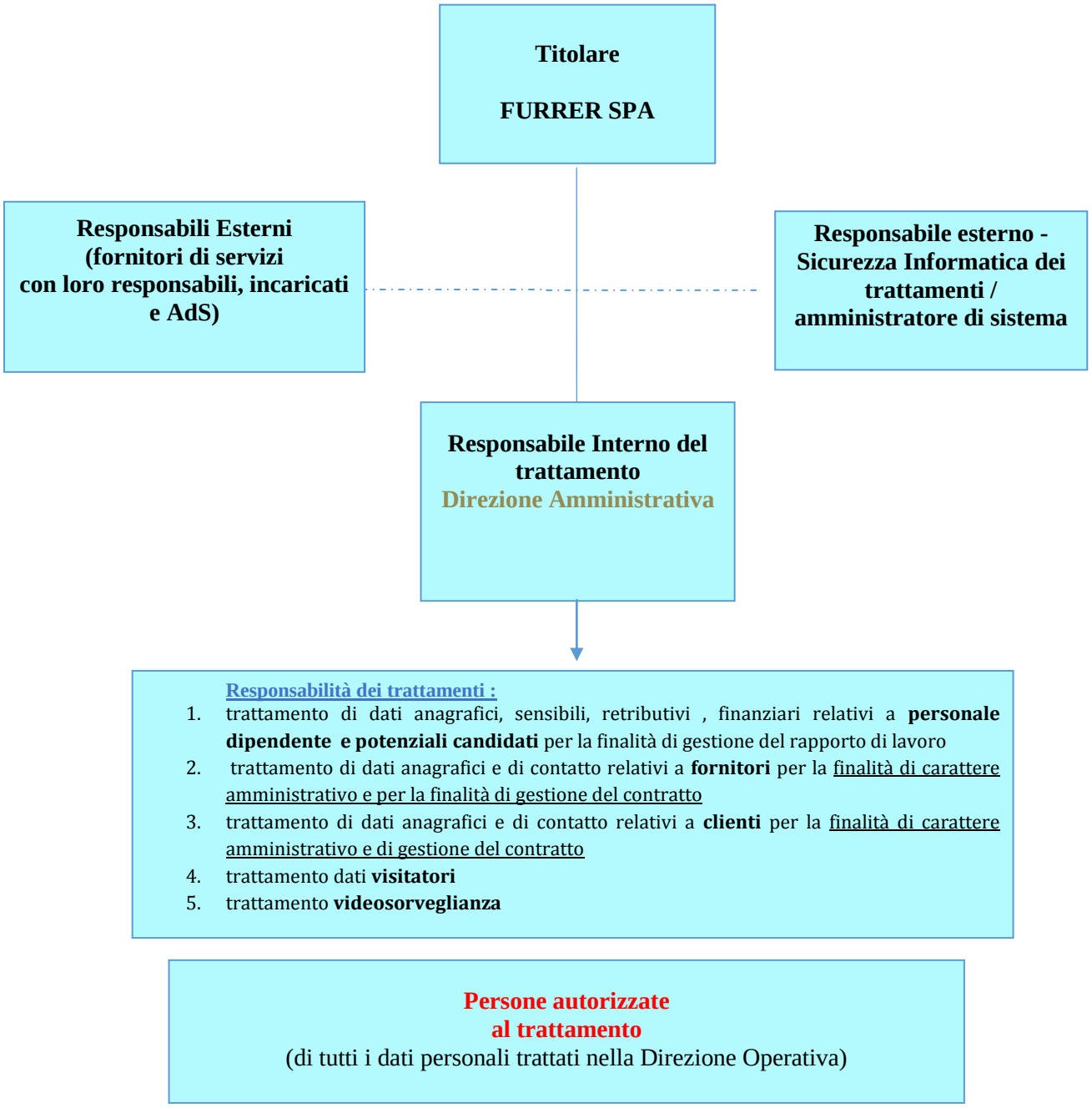

COMPAGINE SOCIALE
Brizzi Rina 7%
Mazzi Gino 27%
Escavazione Marmi Calocara Srl 59%
Furrer Spa 7%

4. ORGANIGRAMMA DELL'AZIENDA

ORGANIGRAMMA PRIVACY

ORGANIGRAMMA "PRIVACY" FURRER SPA

DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITA' NELL'AMBITO DELLE STRUTTURE PREPOSTE AL TRATTAMENTO DEI DATI PERSONALI



Privacy" è un termine inglese equivalente al concetto di "riservatezza", ovvero "diritto alla riservatezza della propria vita privata: "the right to be let alone" (lett. "il diritto di essere lasciati in pace")[1].

Nella realtà normativa contemporanea per "Privacy", intesa come "protezione dei dati personali", si intende, invece, il diritto alla protezione e corretta gestione dei dati personali, cioè il diritto di controllare l'uso e la circolazione degli stessi, che costituiscono un diritto fondamentale nell'attuale società.

5. QUADRO NORMATIVO DI RIFERIMENTO

5.1. LE FONTI NORMATIVE COMUNITARIE E INTERNAZIONALI

Le principali fonti Normative Comunitarie ed Internazionali in materia di Privacy possono sintetizzarsi come segue:

- ✓ la Carta dei Diritti Fondamentali dell'Unione Europea (Carta Europea di Nizza del 2001) art. 8 "Protezione dei dati di carattere personale";
- ✓ il Trattato di Lisbona del 1 dicembre 2009;
- ✓ la Direttiva 95/46/CE relativa al trattamento dei dati personali nonché alla libera circolazione dei dati (cd. Direttiva madre);
- ✓ la Direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche;
- ✓ la Direttiva 2006/24/CE riguardante la conservazione dei dati generali o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e modifica della Direttiva 2001/58/CE;
- ✓ la Direttiva 2009/136/CE (cd. Direttiva e-privacy) ha apportato modifiche alla Direttiva 2002/22/CE ed alla Direttiva 2002/58/CE;
- ✓ il Regolamento Europeo n. 679/2016 approvato il 14 aprile 2016 dal Parlamento UE.

[1] Tratto dal trattato del Giudice Thomas Cooley (1824-1898) "A Treatise On the Law of Torts"

6. IL REGOLAMENTO UE 679/2016

Il Regolamento UE per la protezione dei dati personali n. 2016/679 è la normativa di riforma della legislazione europea in materia di protezione dei dati.

Pubblicato nella Gazzetta Ufficiale europea il 4 maggio 2016, è entrato in vigore il 24 maggio 2016, ma è definitivamente applicabile a partire dal 25 maggio 2018.

Il suo scopo è la definitiva armonizzazione della regolamentazione in materia di protezione dei dati personali all'interno dell'Unione Europea.

Il Regolamento pone con particolare enfasi l'accento sulla responsabilizzazione del titolare e dei responsabili del trattamento, che si deve concretizzare nell'adozione di comportamenti proattivi a dimostrazione della concreta adozione del Regolamento ("Accountability"). In particolare si evidenzia la necessità di attuare misure di tutela e garanzia dei dati trattati, con un approccio del tutto nuovo che demanda ai titolari il compito di decidere autonomamente le modalità ed i limiti del trattamento dei dati alla luce dei criteri specifici indicati nel Regolamento:

- principio "privacy by design", in base al quale i prodotti e i servizi devono essere progettati fin dall'inizio in modo da tutelare la Privacy degli utenti, cioè il trattamento deve essere previsto e configurato fin dall'inizio prevedendo le garanzie per tutelare i diritti degli interessati;
- rischio del trattamento, inteso come valutazione dell'impatto negativo sulle libertà e i diritti degli interessati.

Un approccio Risk Based ha l'evidente vantaggio di pretendere degli obblighi che possono andare oltre la mera conformità alla legge, è sicuramente più flessibile e adattabile al mutare delle esigenze e degli strumenti tecnologici.

6.1. AMBITO TERRITORIALE DI APPLICAZIONE DEL REGOLAMENTO

Il Regolamento si applica ad ogni trattamento che ha ad oggetto dati personali e a tutti i Titolari (Controller) e Responsabili (Processor) del trattamento stabiliti nel territorio dell'Unione Europea, ma anche in generale a quelli che, offrendo beni e servizi a persone residenti nell'Unione, trattano dati di residenti nell'Unione Europea (art. 3 del Regolamento).

Il Regolamento non si applica nei seguenti casi:

- trattamenti effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;
- trattamenti effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del Titolo V, capo 2, del Trattato dell'UE (politica estera e sicurezza);
- trattamenti effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse;
- trattamenti effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico.

6.2. BASE GIURIDICA DEL TRATTAMENTO

Con il GDPR i Titolari del trattamento dovranno identificare la base giuridica del trattamento (ad esempio il consenso dell'interessato, il contratto, gli adempimenti di legge) e documentarla, in quanto in relazione alla base giuridica possono variare i diritti.

L'articolo 6 del Regolamento UE enuncia le condizioni in base alle quali il trattamento può dirsi lecito.

1. **Consenso**

   Il consenso dell'interessato autorizza il trattamento dei dati. Il consenso deve essere specifico, cioè legato ad una finalità precisa.

   Se il trattamento è basato sul consenso il Titolare del trattamento deve sempre fornire l'informativa e garantire la portabilità dei dati.

2. **Adempimento di obblighi contrattuali**

   Il trattamento è lecito se è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso. Sostanzialmente è una forma speciale di consenso. Occorre ovviamente sempre fornire l'informativa, e deve essere garantita la portabilità dei dati.

3. **Obblighi di legge cui è soggetto il Titolare del trattamento**

   Nel caso di trattamento dei dati necessario per l'adempimento di obblighi derivanti da legge, Regolamento o normativa comunitaria non occorre

consenso, non si deve garantire la portabilità dei dati, ma occorre sempre fornire l'informativa, nella quale va indicata la base giuridica del trattamento. In questo caso la finalità deve essere specificata per legge.

4. **Interessi vitali della persona interessata o di terzi**

   Il trattamento dei dati è ammesso se è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica.

   Tale base giuridica si può utilizzare solo se nessuna delle altre condizioni di liceità può trovare applicazione. In questo caso non occorre consenso, non si deve garantire la portabilità dei dati, ma occorre fornire l'informativa, nella quale va indicata la base giuridica del tratta mento.

5. **Legittimo interesse prevalente del Titolare o di terzi cui i dati vengono comunicati**

   Quando il trattamento è necessario per il perseguimento dei legittimi interessi del Titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore, non occorre consenso, non si deve garantire la portabilità dei dati ma, occorre fornire l'informativa nella quale va indicata la base giuridica del trattamento.

6. **Interesse pubblico o esercizio di pubblici poteri**

   Il trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento (tramite legge statale o dell'Unione) non richiede consenso, né si deve garantire la portabilità dei dati, ma occorre fornire l'informativa, nella quale va indicata la base giuridica del trattamento. La finalità deve essere specificata per legge.

6.3. LA STRUTTURA DEL REGOLAMENTO UE 679/2016

Capitoli		Articoli
	Disposizioni generali: • oggetto e finalità del Regolamento • ambito di applicazione • ambito di applicazione per territorio • definizioni	1-4
	Principi: • principi generali • liceità • consenso • consenso dei minori • particolari categorie di dati • trattamenti relativi a condanne penali e reati	5-11
	Diritti dell'interessato	12-23
	Titolare del Trattamento e responsabile del Trattamento	24-43
	Trasferimenti dati personali verso paesi terzi o organizzazioni internazionali	44-50
	Autorità di controllo indipendenti	51-59
	Cooperazione e coerenza	60-76
	Mezzi di ricorso responsabilità e sanzioni	77-84

	Disposizioni relative a specifiche situazioni di trattamento	85-91
	Atti delegati e atti di esecuzione	92-93

6.4. LE PRINCIPALI DEFINIZIONI IN MATERIA DI PRIVACY AI SENSI DEL REGOLAMENTO UE 679/2016

Le principali definizioni in materia di Privacy ai sensi del Regolamento UE 679/2016 sono previste dall'art 4, tra le quali si elencano di seguito le principali:

- **"Archivio"**: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- **"Autorità di controllo"**: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;
- **"Consenso dell'interessato"**: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- **"Dati biometrici"**: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- **"Dati genetici"**: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

- **“Dato personale”**: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- **“Dati relativi alla salute”**: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- **“Destinatario”**: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
- **“Gruppo imprenditoriale”**: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;
- **"Impresa”**: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le Società di persone o le Associazioni che esercitano regolarmente un'attività economica;
- **“Limitazione di trattamento”**: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- **“Norme vincolanti d'impresa”**: le politiche in materia di protezione dei dati personali applicate da un Titolare del trattamento o Responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un Titolare del trattamento o Responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

- **“Profilazione”**: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- **“Pseudonimizzazione”**: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti ad un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separata- mente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- **“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;
- **“Terzo”**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il Titolare del trattamento, il Responsabile del trattamento e le persone Autorizzate al trattamento dei dati personali sotto l'Autorità diretta del Titolare o del Responsabile;
- **“Titolare del trattamento”**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il Titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- **“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;

- **“Rappresentante”**: la persona fisica o giuridica stabilita nell'Unione che, designata dal Titolare del trattamento o dal Responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;
- **“Stabilimento principale**”: per quanto riguarda un Titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del Titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;
- **“Violazione dei dati personali”**: 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.

7. I PRINCIPI GENERALI APPLICABILI AL TRATTAMENTO DEI DATI AI SENSI DEL REGOLAMENTO UE 679/2016

Ai sensi del Regolamento UE 679/2016, i dati personali devono essere:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
- adeguati, pertinenti e limitati, quanto necessario, rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
- esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; 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'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente Regolamento a tutela dei diritti e delle libertà dell'interessato («imitazione della conservazione»);

- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

  Si specifica che ai sensi dell'art. 6 del Regolamento UE, il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

1. l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
2. il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
3. il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento;
4. il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; si può invocare tale base giuridica solo se nessuna delle altre condizioni di liceità può trovare applicazione;
5. il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;
6. Il trattamento è necessario per il perseguimento del legittimo interesse del Titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore. In questo caso il bilanciamento fra legittimo interesse del Titolare o del terzo e diritti e libertà dell'interessato non spetta all'Autorità ma è compito dello stesso Titolare; si tratta di una delle principali espressioni del principio di «responsabilizzazione» introdotto dal nuovo pacchetto protezione dati.

8. LA PRIVACY BY DESIGN E PRIVACY BY DEFAULT

Il Regolamento europeo per la protezione dei dati personali impone al Titolare del trattamento l'adozione di misure tecniche ed organizzative adeguate al fine di tutelare i dati da trattamenti illeciti.

L'articolo 25, in particolare, introduce il principio di privacy by design e privacy by default, un approccio concettuale innovativo che impone alla FURRER l'obbligo di avviare un progetto prevedendo, fin da subito, gli strumenti a tutela dei dati personali.

8.1. PRIVACY BY DESIGN

Il concetto di Privacy by Design risale al 2010, già presente negli Usa e Canada e poi adottato nel corso della 32ma Conferenza mondiale dei Garanti privacy. I principi che reggono il sistema sono i seguenti:

- gli aspetti relativi alla protezione dei dati personali devono essere valutati fin dalla fase di progettazione;
- la privacy deve essere incorporata nel progetto;
- è necessario prevedere la sicurezza dei dati durante tutto il processo di attività;
- i dati devono essere trattati in modo trasparente;
- la centralità dell'utente.

8.2. PRIVACY BY DEFAULT

Il principio di Privacy by Default stabilisce, invece, che la FURRER debba trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini. Devono, quindi, essere applicate delle procedure interne che ne regolino le modalità di acquisizione e gestione, in modo da garantirne sempre il rispetto della normativa sulla Privacy, riducendone, a priori, il rischio di diffusione o il trattamento illecito.

FURRER adotta specifiche procedure Privacy interne al fine di garantire il rispetto della normativa Privacy fin dall'avvio di ogni singola attività o iniziativa all'interno dei processi aziendali.
Altresì FURRER provvede ad aggiornare le procedure e le istruzioni operative tempestivamente qualora dovessero insorgere modifiche normative o organizzative della Società oppure anomalie applicative delle misure di sicurezza adottate o qualora dovessero ravvisarsi inadeguatezze protettive derivanti dall'emersione di nuovi rischi in materia di Privacy.
Le procedure che sono state implementate fanno parte integrante del presente Manuale nella sezione ALLEGATI E PROCEDURE.

8.3. PRINCIPIO DI "ACCOUNTABILITY"

Tra i principi cardine del Regolamento Ue 679/2016 vi è il principio di "Accountability" (ovvero di "responsabilizzazione")

L'art. 5 del Regolamento individua nel Titolare del Trattamento il soggetto competente a garantire il rispetto dei principi posti dalla nuova disciplina in tema di trattamento dei dati personali, quali quelli di liceità, correttezza e trasparenza, limitazione delle finalità, minimizzazione, esattezza, limitazione della conservazione, integrità e riservatezza.

Il co. 2 dell'art. 5 stabilisce che, oltre a dover garantire il rispetto dei suddetti principi, il Titolare deve essere in grado di "comprovarlo"; ciò costituisce l'essenza del principio di "Accountability", in quanto tale soggetto ha l'onere di porre in essere una serie di adempimenti (ad esempio, la mappatura delle operazioni di trattamento mediante la creazione di un apposito Registro), che rendano i principi posti dalla nuova disciplina dati verificabili nei fatti e non più soltanto obblighi giuridici esistenti sulla carta.

Il concetto di "accountability" è ulteriormente delineato dall'art. 24 del Regolamento, **(Responsabilità del Titolare del Trattamento)** il quale prevede che il Titolare del Trattamento debba mettere in atto (nonché riesaminare ed aggiornare) adeguate misure tecniche ed organizzative, per garantire ed essere in grado di dimostrare che le operazioni di trattamento vengano effettuate in conformità alla nuova disciplina. Le misure da adottare vanno valutate di volta in volta, tenendo in considerazione una serie di elementi tra cui la natura, l'ambito di applicazione, il contesto e le finalità del trattamento, nonché i rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

FURRER in ottemperanza al principio di accountability formalizza:

- il Registro delle attività di trattamento;

tale registro rappresenta:

a. l'organizzazione della Società sotto il profilo delle attività di trattamento a fini di informazione, consapevolezza e condivisione interna;
b. costituisce lo strumento di pianificazione e controllo della politica della sicurezza e disponibilità (Allegato);

- un sistema di procedure e istruzioni operative al fine di gestire il Rischio Privacy (Allegato);
- un piano annuale di formazione specifica in materia di Privacy per Autorizzati al Trattamento dei dati e Responsabili del Trattamento dei dati;
- un piano annuale di verifiche di Compliance Privacy.

9. IL DATA BREACH

I dati personali conservati, trasmessi o trattati possono essere soggetti al rischio di perdita, distruzione o diffusione indebita, ad esempio a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi, come incendi o altre calamità. Si tratta di situazioni che possono comportare pericoli significativi per la privacy degli interessati cui si riferiscono i dati.

Per questa ragione, anche sulla base della normativa europea, il Garante per la protezione dei dati personali ha adottato negli ultimi anni una serie di provvedimenti che introducono in determinati settori l'obbligo di comunicare eventuali violazioni di dati personali (Data Breach) all'Autorità stessa e, in alcuni casi, anche ai soggetti interessati. Il mancato o ritardato adempimento della comunicazione espone alla possibilità di sanzioni amministrative. FURRER ha definito una specifica procedura per la corretta individuazione degli eventi di violazione dei dati personali (Data Breach), nonché per la definizione delle attività e delle responsabilità nelle fasi di gestione di tali eventi secondo quanto prescritto dalla normativa in materia (GDPR, articoli 33 e 34) al fine di minimizzare i rischi per la Privacy degli interessati possibilmente derivanti da tali eventi.

Per violazione di dati personali si intende "una violazione della sicurezza che porta alla distruzione, alla perdita, all'alterazione accidentale o illegale, alla divulgazione non autorizzata o all'accesso dei dati personali trasmessi, memorizzati o altrimenti trattati".

La procedura in questione prevede l'esecuzione delle attività di:

- segnalazione, in cui la potenziale violazione viene intercettata automaticamente o manualmente dal sistema di controllo interno o esterno della FURRER ;
- rilevazione, in cui si acquisiscono quante più informazioni di dettaglio possibili sulla potenziale violazione;
- valutazione, in cui si valutano gli impatti della violazione e le possibili attività di comunicazione da svolgere successivamente;
- comunicazione verso l'Autorità Garante, in cui si dichiarano specifiche informazioni sul Data Breach occorso;
- comunicazione verso gli interessati, in cui si definisce la strategia di comunicazione verso l'interessato del Data Breach occorso;
- inventario delle violazioni, in cui si raccolgono tutte le violazioni occorse, a prescindere dall'impatto associato.

FURRER formalizza una specifica procedura da seguire per eventuali casi di Data Breach, allegata al presente Manuale. All'interno della Procedura sono dettagliate le responsabilità per ciascuna fase.

10. L'INFORMATIVA

10.1. AUTORITÀ DI CONTROLLO

Le disposizioni sui meccanismi amministrativi della protezione dei dati nell'Ue sono fissate nei Capi VI e VII del Regolamento 679/2016.

Il Capo VI, in particolare, prevede la costituzione di un **"Autorità di controllo"** in ciascuno Stato membro, fissa identici compiti e poteri per le autorità (artt. 57 e 58) in tutti i Paesi Ue e introduce (art. 56) la nozione di **"Autorità di controllo capofila"**.

L'Autorità di controllo capofila è, in sintesi, l'autorità dello stabilimento principale o unico nell'Ue del Titolare o Responsabile del trattamento, alla quale viene trasferita la competenza da tutte le altre Autorità di controllo (definite, in questo caso, "Autorità interessate") per quanto riguarda i

"trattamenti transfrontalieri" di dati personali svolti da quel Titolare o Responsabile.

L'obiettivo della devoluzione di competenze a favore dell'autorità capofila è garantire l'esistenza di uno "sportello unico" per i trattamenti transfrontalieri di dati personali: principio sancito dal paragrafo 6 dell'art. 56 ("L'autorità di controllo capofila è l'unico interlocutore del Titolare del trattamento o del Responsabile del trattamento in merito al trattamento transfrontaliero effettuato da tale Titolare o Responsabile").

Occorre ricordare, tuttavia, che il Regolamento stesso prevede alcune eccezioni: l'Autorità di controllo che riceve un reclamo (e quindi è, per definizione, un'Autorità "interessata") può infatti far valere il carattere esclusivamente locale del caso e chiedere all'Autorità capofila di rinunciare alla propria competenza ("se l'oggetto riguarda unicamente uno stabilimento nel suo Stato membro o incide in modo sostanziale sugli interessati unicamente nel suo Stato membro").

La cooperazione fra l'Autorità capofila e le altre Autorità, ma anche fra le autorità di controllo in generale, è disciplinata nel Capo VII del Regolamento, che ha per oggetto appunto "Cooperazione e coerenza".

In particolare, il meccanismo decisionale nei casi di trattamento transfrontaliero (detto "sportello unico", poiché il Titolare o il Responsabile potrà rivolgersi alla sola Autorità di controllo capofila) è regolato dall'art. 60 del Regolamento. Si tratta di un meccanismo di codecisione, in cui l'Autorità capofila è competente a emanare la (unica) decisione finale, ma è obbligata a interpellare tutte le Autorità interessate prima di assumere qualsiasi provvedimento che riguardi un Titolare o Responsabile, e nel farlo deve tenere conto delle "obiezioni pertinenti e motivate" che le Autorità interessate possono sollevare sul progetto di decisione o parere fatto circolare dall'Autorità capofila, secondo una tempistica molto stretta.

Il Garante per la protezione dei dati personali (Garante Privacy) è l'Autorità di controllo nazionale italiana in materia di protezione dei dati personali, un'Autorità amministrativa indipendente istituita dalla legge sulla Privacy (legge 31 dicembre 1996, n. 675), in attuazione della direttiva comunitaria 95/46/CE. Oggi è disciplinata dal Codice in materia di protezione dei dati

personali (D. Lgs. 30 giugno 2003 n. 196). La sua sede è a Piazza di Monte Citorio n. 121 in Roma.

Con il nuovo Regolamento europeo l'Autorità di controllo interviene principalmente ex post, cioè la sua valutazione si colloca successivamente alle valutazioni del Titolare del trattamento (FURRER).

10.2. COMITATO EUROPEO PROTEZIONE DATI

L'Autorità capofila può, in ogni momento, respingere le obiezioni formulate dalle Autorità interessate e adire il Comitato europeo per la protezione dei dati (il "Board") che decide secondo la procedura di cui all'art. 65, ma solo sulla "obiezione pertinente e motivata" qualunque ne sia l'oggetto. La decisione del Comitato è vincolante per l'Autorità capofila e le Autorità interessate.

10.3. LA GESTIONE DELLE RICHIESTE DI INFORMAZIONI E ISPEZIONI DELL'AUTORITÀ GRANTE

Per l'espletamento dei propri compiti il Garante può richiedere al Titolare, al Responsabile, all' Interessato o anche a terzi di fornire informazioni e di esibire documenti.

Il Garante può disporre accessi a banche di dati, archivi o altre ispezioni e verifiche nei luoghi ove si svolge il trattamento o nei quali occorre effettuare rilevazioni comunque utili al controllo del rispetto della disciplina in materia di trattamento dei dati personali.

Il Garante si avvale anche, ove necessario, della collaborazione di altri organi dello Stato **(es. Nucleo Speciale Privacy della Guardia Di Finanza)** tramite un Protocollo di intesa che stabilisce che il Garante per la protezione dei dati personali ed il Comando Reparti Speciali, su delega del Comando Generale della Guardia di Finanza - III Reparto Operazioni - individuino insieme le linee programmatiche dell'attività di collaborazione e ne verifichino periodicamente l'andamento.

In particolare, il Corpo collabora all'attività ispettiva condotta dall'Autorità attraverso:

- il reperimento di dati ed informazioni sui soggetti da controllare;
- il reperimento di dati ed informazioni sui soggetti da controllare;
- l'assistenza nei rapporti con le Autorità Giudiziarie;

- la partecipazione del proprio personale agli accessi delle banche dati, ispezioni, verifiche e alle altre rilevazioni nei luoghi ove si svolge il trattamento;
- lo sviluppo delle attività delegate o sub-delegate per l'accertamento delle violazioni di natura penale o amministrativa;
- la contestazione delle sanzioni amministrative rilevate nell'ambito delle attività delegate;
- l'esecuzione di indagini conoscitive sullo stato di attuazione della citata Legge in settori specifici;
- la segnalazione all'Autorità di tutte le situazioni rilevanti ai fini dell'applicazione del Codice, di cui venga a conoscenza nel corso dell'esecuzione delle ordinarie attività di servizio.

  Gli accertamenti, se svolti **in un'abitazione o in un altro luogo di privata dimora,** sono effettuati con l'assenso informato del Titolare o del DPO o del Responsabile, oppure previa autorizzazione del Presidente del Tribunale competente per territorio in relazione al luogo dell'accertamento, il quale provvede con decreto motivato senza ritardo, al più tardi entro tre giorni dal ricevimento della richiesta del Garante quando è documentata l'indifferibilità dell'accertamento.

  Nel procedere a rilievi e ad operazioni tecniche può altresì estrarre copia di ogni atto, dato e documento, anche a campione e su supporto informatico o per via telematica. Degli accertamenti è redatto un sommario verbale nel quale sono annotate anche le eventuali dichiarazioni dei presenti.

  Ai soggetti presso i quali sono eseguiti gli accertamenti è consegnata copia dell'autorizzazione del Presidente del Tribunale, ove rilasciata. I medesimi soggetti sono tenuti a farli eseguire e a prestare la collaborazione a tal fine necessaria. In caso di rifiuto, gli accertamenti sono comunque eseguiti e le spese in tal caso occorrenti sono poste a carico del Titolare con il provvedimento che definisce il procedimento, che per questa parte costituisce titolo esecutivo ai sensi degli articoli 474 e 475 del codice di procedura civile.

  Gli accertamenti, se effettuati presso il Titolare o il Responsabile, sono eseguiti dandone informazione a quest'ultimo o, se questo è assente o non è designato, agli incaricati. Agli accertamenti possono assistere persone

indicate dal Titolare o dal Responsabile. Se non è disposto diversamente nel decreto di autorizzazione del Presidente del Tribunale, l'accertamento non può essere iniziato prima delle ore sette e dopo le ore venti, e può essere eseguito anche con preavviso quando ciò può facilitarne l'esecuzione. Le informative, le richieste e i provvedimenti possono essere trasmessi anche mediante posta elettronica e telefax. Quando emergono indizi di reato si osserva la disposizione di cui all'articolo 220 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale.

Per i trattamenti di dati personali indicati nei titoli I, II e III della Parte II, gli accertamenti sono effettuati per il tramite di un componente designato dal Garante.

Se il trattamento non risulta conforme alle disposizioni di legge o di Regolamento, il Garante indica al Titolare o al Responsabile le necessarie modificazioni ed integrazioni e ne verifica l'attuazione. Se l'accertamento è stato richiesto dall'interessato, a quest'ultimo è fornito in ogni caso un riscontro circa il relativo esito, se ciò non pregiudica azioni od operazioni a tutela dell'ordine e della sicurezza pubblica o di prevenzione e repressione di reati o ricorrono motivi di difesa o di sicurezza dello Stato. Gli accertamenti non sono delegabili. Quando risulta necessario in ragione della specificità della verifica, il componente designato può farsi assistere dal personale specializzato tenuto al segreto. Gli atti e i documenti acquisiti sono custoditi secondo modalità tali da assicurarne la segretezza e sono conoscibili dal presidente e dai componenti del Garante e, se necessario, per lo svolgimento delle funzioni dell'organo, da un numero delimitato di addetti all'Ufficio individuati dal Garante.

Per gli accertamenti relativi agli organismi di informazione e di sicurezza e ai dati coperti da segreto di Stato, il componente designato prende visione degli atti e dei documenti rilevanti e riferisce oralmente nelle riunioni del Garante. Nell'effettuare gli accertamenti di cui al presente articolo nei riguardi di uffici giudiziari, il Garante adotta idonee modalità nel rispetto delle reciproche attribuzioni e della particolare collocazione istituzionale dell'organo procedente. Gli accertamenti riferiti ad atti di indagine coperti dal segreto sono differiti, se vi è richiesta dell'organo procedente, al momento in cui cessa il segreto.

La validità, l'efficacia e l'utilizzabilità di atti, documenti e provvedimenti nel procedimento giudiziario basati sul trattamento di dati personali non conforme a disposizioni di legge o di regolamento restano disciplinate dalle pertinenti disposizioni processuali nella materia civile e penale.

10.4. LE MODALITÀ DELLE ISPEZIONI DELL'AUTORITÀ GARANTE PRIVACY

Attualmente l'Autorità Garante, mediante proprio personale ispettivo oppure attraverso la Guardia di Finanza, effettua ispezioni e controlli, che possono estendersi fino a 2-3 giorni di durata, principalmente mirati ai seguenti aspetti:

- titolarità dei dati (verifica notificazioni effettuate);
- nomine di Responsabili o Incaricati;
- categorie dei dati trattati e descrizione dettagliata dei trattamenti (finalità, modalità, soggetti);
- informative (devono essere chiare e semplici);
- consensi richiesti e prestati (devono essere liberi);
- tipologia, modalità' e tempi di conservazione;
- misure di sicurezza;
- rispetto dei provvedimenti specifici per trattamenti particolari (es. videosorveglianza, geolocalizzazione, biometria, trattamenti mediante web, profilazione);
- rispetto principi di pertinenza, non eccedenza, proporzionalità e necessità.

Prima dell'ispezione vengono verificate le eventuali notificazioni effettuate ed i siti web dell'azienda/ente.

Durante l'ispezione è opportuno fornire collaborazione attiva e tutte le notizie, informazioni e documentazione richieste in modo veritiero, per evitare di incorrere in sanzioni ed in reati.

FURRER formalizza una specifica procedura per la corretta gestione delle Visite Ispettive dell'Autorità Garante. La procedura in questione ha definito le diverse fasi del processo della visita ispettiva del Garante, quali:

- la definizione delle responsabilità nella gestione della visita ispettiva;
- la gestione della fase di accoglienza degli ispettori;
- le modalità di collaborazione nelle attività;
- la stesura del verbale di ispezione;
- le modalità di archiviazione della documentazione in materia.

11. LE LINEE GUIDA DELL'AUTORITA' GARANTE SPECIFICHE PER LE AREE DI ATTIVITA' DI FURRER

Nella tabella che segue si elencano tutte le principali Linee Guida di interesse per FURRER :

✓ **Linee guida in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali**
✓ **Linee guida del Garante per posta elettronica e Internet**
✓ **Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di**

12. I DIRITTI DELL'INTERESSATO

Di seguito si elencano alcuni dei principali Provvedimenti dell'Autorità Garante che potrebbero essere di interesse anche indiretto per FURRER .

Imprese

Provvedimento in ordine all'applicabilità alle persone giuridiche del Codice in materia di protezione dei dati personali a seguito delle modifiche apportate dal d.l.g n. 201/2011 - 20 settembre 2012.

Prescrizioni in materia di operazioni di fusione e scissione - 8 aprile 2009.

Informazioni commerciali

Modifica parziale del provvedimento di esonero dall'informativa per l'Associazione nazionale tra le imprese di informazioni commerciali e di

gestione del credito (ANCIC) del 14 maggio 2009 - 22 maggio 2014.

Diritto di accesso - Prescrizioni di carattere generale per le 'centrali rischi private' - 31 luglio 2002.

Internet e social media

Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie - 8 maggio 2014.

Lavoro

Sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro - 4 ottobre 2011.

Lavoro e previdenza sociale - Cartellini identificativi dei lavoratori - 11 dicembre 2000.

Marketing

Provvedimento generale a carattere prescrittivo sulle c.d. 'chiamate mute' - 20 febbraio 2014.

Consenso al trattamento dei dati personali per finalità di "marketing diretto" attraverso strumenti tradizionali e automatizzati di contatto - 15 maggio 2013.

Prescrizioni per il trattamento di dati personali per finalità di marketing, mediante l'impiego del telefono con operatore, a seguito dell'istituzione del registro pubblico delle opposizioni 19 gennaio 2011.

Spamming. Regole per un corretto uso dei sistemi automatizzati e l'invio di comunicazioni elettroniche - 29 maggio 2003.

Data breach

Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. data breach) 4 aprile 2013.

Misure di sicurezza

Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento - 25 giugno 2009.

Semplificazione delle misure di sicurezza contenute nel disciplinare tecnico di cui all'Allegato B) al Codice in materia di protezione dei dati personali - 27 novembre 2008.

Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008.

Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali - 13 ottobre 2008.

Videosorveglianza

Provvedimento in materia di videosorveglianza - 8 aprile 2010 Videosorveglianza - Provvedimento generale - 29 aprile 2004.

Videosorveglianza - Il decalogo delle regole per non violare la privacy - 29 novembre 2000.

13. TIPOLOGIE DI DATI E TRATTAMENTO DEI DATI

13.1. IL DATO E LE TIPOLOGIE DI DATI

Il Dato è un'informazione.

Sono **dati personali** le informazioni, inclusi suoni ed immagini, che identificano o rendono identificabile una persona fisica sia in modo diretto che indiretto, ottenuto cioè per connessione con altra informazione o con un semplice numero di identificazione personale, quale potrebbe derivare da un indirizzo, da un numero telefonico, da un certificato, da una carta di credito.

Tra i dati personali si distinguono:

- **dato personale identificativo:** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o

indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o ad uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

- **categorie particolari di dati personali** (ex dati sensibili): dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
- **dati personali relativi alle condanne penali o reati:** il trattamento di tali dati deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale Registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'Autorità pubblica.

13.2. IL TRATTAMENTO DELLE CATEGORIE PARTICOLARI DI DATI PERSONALI

Il Regolamento UE supera la definizione di dati sensibili e prevede il Trattamento di categorie particolari di dati personali disponendo che è vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Il divieto non si applica se si verifica uno dei seguenti casi:

a. l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto;
b. il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del Titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto

collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;

c. il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
d. il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;
e. il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
f. il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
g. il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;
h. il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale, ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3;
i. il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate

e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;

j. il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

13.3. DATI RELATIVI A CONDANNE PENALI ED A REATI

Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale Registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'Autorità pubblica.

14. IL TRATTAMENTO DEI DATI PERSONALI E LE SUE FASI E MODALITA'

Ai sensi dell'art. 4 del Regolamento UE, il trattamento dei dati personali è *"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 di dati, anche se non registrati in una banca dati".*

Le operazioni di Trattamento dei dati possono essere suddivise in quatto fasi:

a. **fase preliminare** (raccolta e registrazione);
b. **fase di elaborazione**: l'organizzazione, la strutturazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, il raffronto o l'interconnessione, la limitazione;

c. **fase di circolazione**: la comunicazione mediante trasmissione, la diffusione o qualsiasi altra forma di messa a disposizione;
d. **fase residuale** (conservazione, blocco, cancellazione, distruzione, consultazione).

Nell'effettuare qualsivoglia trattamento, al fine di mantenersi entro gli ambiti della legittimità fissati dal Regolamento UE i Responsabili dovranno verificare che il trattamento si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale ed al diritto alla protezione dei dati personali.

14.1. MODALITÀ DEL TRATTAMENTO DEI DATI PERSONALI

In ogni caso, i dati personali devono essere:

a. trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
b. 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'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
c. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
d. 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»);
e. 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'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);

f. 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»).

FURRER tratta categorie particolari di dati in alcuni processi aziendali.

Tali dati con i relativi trattamenti e finalità sono stati dettagliati nel Registro delle attività di Trattamento.

I soggetti che trattano i dati in oggetto hanno specifica nomina a Responsabile interno e ad autorizzato del Trattamento dei dati personali e sono formati in ordine alle modalità con le quali deve essere acquisito specifico consenso scritto e sulle modalità di archiviazione degli stessi in maniera cartaceo o informatica.

14.2. PRIVACY E COOKIE

FURRER sul proprio sito web utilizza cookies tecnici ai fini della navigazione, di cui alla apposita informativa presente nel sito stesso. Si ritiene importante ricordare brevemente la disciplina dei cookie in materia di Privacy. Tra le finalità dei cookie, sono previste anche quelle di profilazione, per questo motivo è importante che sia prevista una tutela dal punto di vista della Privacy. I cookie si definiscono come piccole stringhe di testo e numeri, che vengono scaricati nella memoria del browser, quando viene visitato un sito web o utilizzato un social network attraverso un pc, uno *smartphone* o un *tablet*.

Per quanto riguarda le fonti normative, è necessario il contenuto del Provvedimento Generale del Garante del 2014, intitolato "***Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie***" oltre a quanto definito negli art. 13 e 14 del Regolamento Europeo. I cookie svolgono numerose e diverse funzioni

nell'ambito della rete (esecuzione di autenticazioni informatiche, memorizzazione delle preferenze). I cookie possono essere di vario tipo:

- **Cookie di prima e di terza parte:**

  Sotto il profilo soggettivo, occorre fare una prima distinzione riguardo i soggetti, che installano i cookie sul terminale dell'utente. Se è lo stesso gestore del sito, si parla di cookie di prima parte. Il provvedimento del Garante definisce il gestore del "sito" anche "editore". Nel caso in cui il cookie sia installato da un sito diverso, per il tramite del primo, si parla di cookie di terza parte.

  A seconda delle finalità, i cookie possono essere raggruppati nelle seguenti categorie:

- **Cookie tecnici**: sono quei cookie che consentono di navigare o di fornire un sevizio all'utente. Rientrano in questa categoria i cookie che riconoscono in automatico la lingua che l'utente utilizza, quelli che facilitano gli acquisti online o quelli che rendono meno complesse e più sicure le procedure di home banking, come l'esecuzione dei bonifici. Per l'installazione di questi cookie non è richiesto il preventivo consenso degli utenti, tuttavia resta l'obbligo per l'editore di informare l'utilizzatore del sito della presenza dei cookie tecnici, ai sensi dell'art. del D. lgs 196/2003;
- **Cookie analytics:** sono una particolare tipologia di cookie utilizzati dai gestori dei siti web per raccogliere informazioni in maniera aggregata di natura statistica;
- **Cookie di profilazione:** sono quei cookie che controllano la navigazione dell'utente, tracciandola al fine di monitorare e profilare l'utente. Tramite l'uso di tali cookie, è possibile sapere quali siti vengono letti dall'utente oppure quali siano i suoi gusti o abitudini.

  La particolare invasività dei cookie di profilazione, che sono in grado di carpire informazioni a fini pubblicitari all'insaputa degli utenti, ha indotto l'Autorità garante ad adottare un provvedimento di carattere generale, emanato **l'8 Maggio 2014,** con il quale detta le modalità per delimitare l'utilizzo di tali cookie. In particolare, il sito della FURRER deve contenere un'adeguata Privacy Policy, prevedendo un banner, che possa essere visualizzato immediatamente dall'utilizzatore del cliente e che deve contenere un'informativa breve, contenente le seguenti indicazioni:

1. Che il sito utilizza cookie di profilazione al fine di inviare messaggi pubblicitari in linea con le preferenze manifestate dall'utente nell'ambito della navigazione in rete;
2. Che il sito consente anche l'invio di cookie "terze parti" (laddove ovviamente questi vengano utilizzati);
3. Il link all'informativa estesa, ove vengono fornite indicazioni sull'uso dei cookie tecnici e analytics: viene data la possibilità di scegliere quali specifici cookie autorizzare;
4. L'indicazione che alla pagina dell'informativa estesa è possibile negare il consenso all'installazione di qualunque cookie;
5. L'indicazione che la prosecuzione della navigazione mediante accesso ad altra area del sito o selezione di un elemento dello stesso (ad esempio di un'immagine o di un link) comporta la prestazione del consenso all'uso dei cookie.

L'**informativa estesa** deve:

1. Contenere tutti gli elementi previsti dall'art. 13 del Regolamento UE;
2. Descrivere in maniera specifica ed analitica le caratteristiche e le finalità dei cookie installati dal sito;
3. Descrivere in maniera specifica e analitica le caratteristiche e le finalità dei cookie installati dal sito;
4. Consentire all'utente di selezionare e deselezionare i singoli cookie;
5. Essere raggiungibile mediante un link inserito nell'informativa breve, come pure attraverso un riferimento su ogni pagina del sito, collocato in calce alla medesima.

Inoltre all'interno di tale informativa deve essere inserito il link aggiornato alle informative e ai moduli di consenso delle terze parti, con le quali l'editore ha stipulato accordi per l'installazione di cookie tramite il proprio sito; e che sia richiamata la possibilità per l'utente di manifestare le proprie opzioni in merito all'uso dei cookie da parte del sito anche attraverso le impostazioni del browser, indicando almeno la procedura da eseguire per configurare tali impostazioni.

In materia di cookie, di seguito, si indicano gli atti principali emanati dal garante:

- Provvedimento 8 Maggio 2014 "**Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie**";
- Comunicato Stampa 4 Giugno 2014 "***Internet: Garante privacy, no ai cookie di profilazione senza consenso***";
- **Informativa e consenso per l'uso dei cookie**: domande più frequenti;
- **Chiarimenti** in merito all'attuazione della normativa in materia di cookie del 5 Giugno 2015.

FURRER non opera profilazione della clientela on line tramite il sito www.furrer.it.

Il sito prevede sia l'informativa breve che l'informativa estesa (predisposte ai sensi dell'art. 13 del Regolamento Europeo 679/2016), di modo che l'utente/visitatore del sito sia edotto delle tipologie di cookie utilizzate da FURRER. In particolare, la medesima, utilizza solo cookie tecnici, finalizzati a garantire un corretto funzionamento del sito.

14.3. CESSAZIONE DEL TRATTAMENTO DEI DATI

In caso di cessazione, per qualsiasi causa, di un trattamento, i dati sono:

- distrutti;
- ceduti ad altro Titolare, purché destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti;
- conservati per fini esclusivamente personali e non destinati ad una comunicazione sistematica o alla diffusione;
- conservati o ceduti ad altro Titolare, per scopi storici, statistici o scientifici, in conformità alla legge, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e di buona condotta.

  La cessione dei dati in violazione di quanto previsto dal comma 1, lettera b), o di altre disposizioni rilevanti in materia di trattamento dei dati personali è priva di effetti.

15. I SOGGETTI CHE EFFETTUANO IL TRATTAMENTO DEI DATI

15.1. IL TITOLARE DEL TRATTAMENTO DEI DATI

Il Titolare del trattamento (Data Controller) è "la persona fisica, giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro Titolare, le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali ed agli strumenti utilizzati, ivi compreso il profilo della sicurezza".

L'introduzione del nuovo regolamento generale europeo ha creato qualche problema nella traduzione dei termini, in quanto il termine Data Controller va tradotto, come stabilito dal Garante italiano, con Titolare del trattamento, cioè colui il quale è Responsabile per il trattamento medesimo. Questo ha creato qualche confusione col Responsabile del trattamento, che invece più correttamente è la traduzione di Data Processor. Il Titolare nomina con contratto o atto giuridicamente valido, il Responsabile del trattamento, insieme al quale pone in atto le misure tecniche ed organizzative congrue per garantire un livello di sicurezza adeguato al rischio. Ed è, ovviamente, al Titolare del trattamento effettivo, anche se il trattamento è illecito, al quale vanno indirizzate le richieste di tutela dei propri dati in caso di violazione dei diritti dell'interessato. Inoltre, il Titolare del trattamento, e il Responsabile, sono tenuti alla redazione del Registro di Trattamenti.

Nel caso di gruppi di fondazioni, la Società madre e le controllate sono distinti Titolari del trattamento, avendo una personalità giuridica distinta. In tal caso il trasferimento dei dati tra le fondazioni del gruppo deve essere autorizzata dagli interessati.

15.2. CONTITOLARITÀ (JOINT CONTROLLERS)

E' possibile che coesistano più Titolari del trattamento (contitolari o Jointes Controllers) che decidano congiuntamente di trattare i dati per una finalità comune. In tale caso, la normativa impone ai contitolari di definire specificamente (con un atto giuridicamente valido) il rispettivo ambito di responsabilità e i compiti. In ogni caso, però, gli interessati possono rivolgersi indifferentemente ad un qualsiasi contitolare.

La figura del contitolare del trattamento è prevista all'art. 26 "Contitolari del trattamento" GDPR, il quale articolo precisa che i contitolari possono anche essere più di due, che devono determinare congiuntamente le finalità e i mezzi del trattamento. Si ipotizza quindi la necessità della sussistenza di una codecisione in merito alle finalità (perché) e ai mezzi (come) di un determinato trattamento.

Tramite accordo interno, i contitolari hanno l'obbligo di determinare, in modo trasparente, le rispettive responsabilità e compiti sull'osservanza degli obblighi derivanti dal GDPR con particolare riferimento ai diritti dell'interessato e gli obblighi di fornire le informazioni previste al momento della raccolta (Art.13 – Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato; Art.14 – Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato).

15.3. IL RESPONSABILE "ESTERNO" DEL TRATTAMENTO EX REG. UE 679/2016 E IL RESPONSABILE "INTERNO" NOMINATO DAL TITOLARE

Il responsabile del trattamento (nel nuovo regolamento europeo "Data Processor") è la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del Titolare del trattamento.

Il Titolare del trattamento, quindi, nomina uno o più Responsabili.

In base all'art. 28 la nomina del Responsabile deve avvenire tramite contratto o altro *"atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il Responsabile del trattamento al Titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento"*.

Con tale contratto il titolare delega al responsabile la concreta gestione del trattamento, affidandogli uno o più compiti specifici oppure una serie di compiti dettagliati in generale. Il responsabile a sua volta può nominare responsabili di secondo livello, a meno che non sia vietato dalle istruzioni del titolare. E' comunque il Responsabile principale a rispondere dell'operato degli altri da lui nominati, di fronte al Titolare del Trattamento.

Il Titolare del trattamento rimane, a sua volta, Responsabile della gestione effettuata dai responsabili, dovendo garantire che le loro decisioni siano

conformi alle leggi, e in particolare il Titolare deve scegliere Responsabili del trattamento che offrano garanzie sufficiente ed adeguate nell'adozione di idonee misure tecniche e organizzative volte alla protezione dei dati personali. Il Titolare deve sempre poter sindacare le decisioni dei responsabili.

Nel caso in cui il Responsabile del trattamento ecceda i limiti di utilizzo dei dati fissati dal Titolare, il Responsabile diventa Titolare della gestione illecita dei dati e ne risponde come tale, insieme all'effettivo Titolare (in sostanza è come se diventassero contitolari).

Il Responsabile del trattamento ha obblighi specifici, quali: la tenuta del Registro dei Trattamenti svolti (ex art. 30, paragrafo 2, del Regolamento Generale); l'adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti (ex art. 32 regolamento); la designazione di un Data Protection Officer, nei casi previsti dal Regolamento o dal diritto nazionale (si veda art. 37 del Regolamento).

Sia il Titolare del trattamento che il Responsabile, sono tenuti ad attuare le misure tecniche ed organizzative tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche. Si tratta di specifici requisiti previsti dal GDPR, che indica alcune misure di sicurezza utili per ridurre i rischi del trattamento, quali la pseudonimizzazione e la cifratura dei dati personali, la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

FURRER ha formalizzato la nomina dei Responsabili esterni del trattamento dei dati ex art. 28 del Reg. UE 679/2016 (di cui all'elenco aggiornato presso gli uffici della Società).

FURRER ha anche formalizzato la nomina di Responsabili interni del trattamento nella sua facoltà societaria di effettuare nomine e conferire deleghe di funzioni e procure.

15.4. IL DATA PROTECTION OFFICER (DPO)

Il soggetto preposto dalla disciplina comunitaria a sovraintendere ad un dato modello di gestione Privacy è il Data Protection Officer (DPO) o Responsabile della Protezione dei Dati (RDP) ai sensi degli artt. 37, 38, 39 del Regolamento UE.

I Titolari del Trattamento, nel caso sia previsto come obbligatorio o opportuno, dovranno designare come "Data Protection Officer" un professionista che possieda un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali, che sia in grado di adempiere alle proprie funzioni in piena indipendenza e in assenza di conflitti di interesse, operando come dipendente, oppure anche sulla base di un contratto di servizi in outsourcing.

15.5. AUTORIZZATO AL TRATTAMENTO (EX INCARICATO DEL TRATTAMENTO DEI DATI PERSONALI)

Il Regolamento UE 679/02016 non prevede espressamente la figura dell'incaricato, ma non ne esclude la nomina, facendo riferimento a persone Autorizzate al trattamento dei dati sotto l'Autorità diretta del Titolare o del Responsabile (art. 4 del Regolamento UE).

La persona autorizzata è, in sintesi, colui che effettua materialmente le operazioni di trattamento sui dati personali.

E' fondamentale tenere presente che in assenza della nomina, qualsiasi operazione svolta dai dipendenti o collaboratori del Titolare non è qualificata come un utilizzo interno dei dati, bensì come una comunicazione a terzi, con le problematiche del caso (in particolare occorre un consenso specifico).

La normativa non prevede requisiti quantitativi, per cui anche la semplice presa visione di un dato personale si qualifica come trattamento, e quindi necessita di una nomina perché non sia considerato illecito.

FURRER in compliance alla normativa in oggetto formalizza la nomina delle persone Autorizzate al Trattamento dei dati ai sensi dell'art. 4 del Regolamento UE di tutti i propri dipendenti, in modo differenziato a seconda che nelle proprie mansioni trattino solo dati personali o anche categorie particolari di dati personali.

La nomina delle persone addette avviene al momento dell'assunzione e vengono adeguatamente formate secondo il Piano formativo.

15.6. L'AMMINISTRATORE DI SISTEMA (PROVV. GARANTE PRIVACY 27/11/2008, MODIFICATO DA PROVV.25/06/2009)

La figura dell'Amministratore di Sistema così come non compariva nel Codice Privacy, ma solamente menzionato all'interno dell'Allegato B del Codice medesimo, non compare attualmente neppure nel Regolamento UE.

In data 27 novembre 2008 l'Autorità Garante ha emanato uno specifico provvedimento denominato *"Misure e accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema".* E' quindi l'Autorità Garante che in detto provvedimento prevede che *con la definizione di* ***"Amministratore di Sistema"*** *si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del provvedimento del Garante vengono considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi".*

L'Amministratore di Sistema è assunto quale figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui

vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise Resource Planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali.

Non rientrano invece nella definizione quei soggetti che solo occasionalmente intervengono (per esempio per scopi di manutenzione a seguito di guasti o malfunzioni) sui sistemi di elaborazione e sui sistemi software.

FURRER in compliance alla normativa in oggetto nomina Responsabile esterno con funzioni di amministratore di sistema che si occupa di gestire il Sistema Informatico della Società.

16. L'INTERESSATO

16.1. I DIRITTI DELL'INTERESSATO

L'interessato (**data subject**) del trattamento è la persona fisica a cui si riferiscono i dati personali, o più esattamente il proprietario dei suoi dati.

La normativa attribuisce specifici diritti all'interessato, il quale, per l'esercizio di tali diritti, può rivolgersi direttamente al Titolare del trattamento.

L'interessato può esercitare i suoi diritti anche in un momento successivo a quello in cui ha prestato il consenso, potendo così revocare un consenso già prestato.

I diritti esercitabili dall'interessato sono i seguenti:

- esercitare l'opposizione al trattamento in tutto o in parte;
- ottenere la cancellazione dei dati in possesso del Titolare;
- ottenere l'aggiornamento o la rettifica dei dati conferiti;
- chiedere ed ottenere in forma intellegibile i dati in possesso del Titolare (diritto di accesso);
- chiedere ed ottenere la trasformazione in forma anonima dei dati;

- chiedere ed ottenere il blocco o la limitazione dei dati trattati in violazione di legge e quelli dei quali non è più necessaria la conservazione in relazione agli scopi del trattamento.

16.2. DIRITTO DI OPPOSIZIONE

L'opposizione al trattamento è operazione diversa dalla quella della cancellazione dei dati. In base ad essa l'interessato può impedire il trattamento che non è compatibile con le finalità del consenso.

E' il Titolare del trattamento che deve dare riscontro alla richiesta dell'interessato, **entro un mese** dall'esercizio del diritto. In casi particolarmente complessi la risposta può essere fornita **entro 3 mesi.** La risposta deve avere in forma scritta, anche in formato elettronico, tranne nel caso in cui l'interessato la richieda oralmente. La risposta deve essere coincisa, accessibile ed intellegibile. L'unico obbligo per l'interessato è di fornire i dati per la sua identificazione. La risposta in genere dovrebbe essere senza costi, tranne l'eventuale rimborso del costo del supporto utilizzato.

16.3. DIRITTO DI INFORMAZIONE

L'interessato del trattamento ha il diritto a ricevere una corretta informazione in relazione ai dati raccolti e trattati, alle finalità del trattamento, alla base giuridica del trattamento e ai diritti che gli sono attribuiti, nonché le modalità per esercitarli. Tutto ciò avviene a mezzo dell'informativa, il cui scopo è informare l'interessato che così possa rendere un valido consenso.

Nel caso in cui ai dati sia applicato un trattamento automatizzato comprendente profilazione il Titolare deve informare l'interessato, esplicitando le modalità e le finalità della profilazione, nonché la logica inerente il trattamento e le conseguenze previste per l'interessato a seguito di tale tipo di trattamento.

16.4. DIRITTO DI ACCESSO

L'art. 15 del Regolamento europeo prevede il diritto di accesso, cioè il diritto di conoscere quali dati personali relativi all'interessato il Titolare sta trattando, con quali finalità e modalità, e di ricevere una copia (gratuita) dei dati.

I Titolari possono eventualmente anche consentire un accesso diretto ai dati da remoto.

L'interessato ha il diritto di conoscere:

- le finalità del trattamento;
- le categorie di dati personali trattate;
- i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
- quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'esistenza del diritto dell'interessato di chiedere al Titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
- il diritto di proporre reclamo a un'Autorità di controllo;
- qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate rispetto alla tutela fornita nel paese terzo.

16.5. DIRITTO DI RETTIFICA

Il diritto di rettifica consiste nel diritto dei soggetti di cui siano state diffuse informazioni, immagini o ai quali siano stati attribuiti atti, pensieri o affermazioni che non siano rispondenti al vero, di ottenere la diffusione delle proprie dichiarazioni di replica in condizioni paritarie rispetto alla comunicazione che si intende rettificare.

Si tratta di uno strumento volto a consentire la tutela dell’identità personale degli individui e il loro diritto affinché le dichiarazioni ad essi riferite siano veritiere, non siano inesatte e non siano idonee ad alterare l’identità

personale, morale e ideale, che nel corso della vita hanno costruito mediante i propri comportamenti.

Il diritto di rettifica trova nel Regolamento europeo sulla Privacy un'autonoma affermazione all'art. 16, ove è definito quale diritto dell'interessato di ottenere dal Titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano.

Il Regolamento afferma chiaramente che l'interessato ha diritto di richiedere al Titolare che siano modificati, corretti o aggiornati i dati che lo riguardano, nonché che siano integrati i dati personali incompleti.

16.6. DIRITTO ALLA CANCELLAZIONE DEI DATI (DIRITTO ALL'OBLIO)

Il diritto di cancellazione (anche detto diritto "all'oblio") è il diritto di ottenere la cancellazione dei propri dati personali in casi particolari. Esso può essere esercitato anche dopo la revoca del consenso.

Il diritto all'oblio, inizialmente riconosciuto soltanto a livello giurisprudenziale, sia in campo europeo che nazionale, con l'entrata in vigore del nuovo Regolamento Generale sulla Protezione dei Dati Personali (RGPD, Regolamento UE 2016/679) riceve finalmente un'espressa regolamentazione che ne indica la portata e i limiti.

In base a tale previsione l'interessato ha il diritto di ottenere dal Titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il Titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali.

16.7. DIRITTO ALLA PORTABILITÀ DEI DATI

Il diritto alla portabilità dei dati è un nuovo diritto previsto dal Regolamento europeo. Si applica solo ai trattamenti automatizzati e sono previste specifiche condizioni per il suo esercizio.

L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un Titolare del trattamento e ha il diritto di trasmettere tali dati a un altro Titolare del trattamento senza impedimenti da parte del Titolare del trattamento cui li ha forniti qualora:

a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b);

b) il trattamento sia effettuato con mezzi automatizzati.

Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un Titolare del trattamento all'altro, se tecnicamente fattibile.

L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento.

Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui.

16.8. DIRITTO DI LIMITAZIONE DEL TRATTAMENTO

Il diritto di limitazione (art. 18 del Regolamento) consente all'interessato di ottenere il blocco del trattamento in caso di violazione dei presupposti di liceità, ma anche se chiede la rettifica dei dati o si oppone al loro trattamento, in attesa della decisione del Titolare. In caso di esercizio di tale diritto ogni trattamento, tranne la conservazione, è vietato. Si prevede quindi di contrassegnare il dato in attesa di determinazioni ulteriori. L'interessato ha il diritto di ottenere dal Titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:

a. l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;
b. il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
c. benché il Titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
d. l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del Titolare del trattamento rispetto a quelli dell'interessato.

Se il trattamento è limitato a norma del paragrafo 1, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

L'interessato che ha ottenuto la limitazione del trattamento a norma del paragrafo 1 è informato dal Titolare del trattamento prima che detta limitazione sia revocata.

17. TUTELA DEI DIRITTI DELL'INTERESSATO

L'interessato può rivolgersi direttamente al Titolare (o al Responsabile) del trattamento per l'esercizio dei suoi diritti (interpello). In caso di mancata risposta, o di risposta inadeguata, può rivolgersi all'autorità amministrativa (Garante) o giudiziaria per la tutela dei suoi diritti.

I diritti dell'interessato sono indicati all'art. 15 del Regolamento UE il quale prevede che lo stesso ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.

Nonché l'indicazione:

a) dell'origine dei dati personali;
b) delle finalità e modalità del trattamento;
c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
d) degli estremi identificativi del Titolare, dei Responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di Responsabili o incaricati.

L'interessato ha diritto di ottenere:

a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;

b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;

c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi sproporzionato rispetto al diritto tutelato.

L'interessato ha, inoltre, il diritto di opporsi, in tutto o in parte:

a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;

b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Detti diritti, sopra menzionati sono esercitati con richiesta rivolta, senza formalità, al Titolare o al Responsabile, anche per il tramite di un incaricato.

Alla richiesta deve essere fornito idoneo riscontro senza ritardo.

La richiesta può essere trasmessa anche mediante fax o posta elettronica o semplicemente formulata in via orale.

Quando essa riguarda la mera richiesta di informazioni relative al trattamento eventualmente in atto, può essere formulata anche oralmente; in tal caso è annotata sinteticamente a cura del Responsabile o dell'incaricato.

Al fine di esaudire la richiesta dell'interessato, il Responsabile, o un incaricato all'uopo individuato, dovrà:

a) comunicare oralmente le informazioni richieste; oppure,

b) consentire la visione delle informazioni mediante strumenti elettronici; oppure,

c) se richiesto, provvedere alla trasposizione dei dati su supporto cartaceo o informatico o all'invio per via telematica.

FURRER in ottemperanza alla Privacy by Default implementa una procedura di Gestione delle istanze degli interessati , una procedura per il Data Breach, una procedura per gestire le visite ispettive da parte dell'Autorità Garante, una procedura flussi informativi, che regola le segnalazioni in materia di Privacy dalle varie funzioni aziendali che vengono inviate al Responsabile interno del trattamento o al DPO (qualora venga nominato).

18. L'INFORMATIVA

La normativa europea e nazionale, prevede che, in base alla finalità del trattamento il titolare deve fornire agli interessati, prima del trattamento, le informazioni richieste dalle norme.

L'informativa è una comunicazione rivolta all'interessato finalizzata ad informarlo, così che possa rendere un valido consenso.

L'informativa può anche essere orale, ma è preferibile sia data per iscritto al fine di provarne l'esistenza e per consentire alle Autorità di vigilanza di verificarne la completezza e correttezza.

L'informativa deve avere il seguente contenuto minimo (articoli 13 e 14 del Regolamento europeo):

- finalità e modalità del trattamento (non come vengono trattati i dati ma quali dati vengono trattati, divisi per categorie, a quale fine, per quanto tempo sono trattati, se i dati verranno trasferiti all'estero e, in questo caso, attraverso quali strumenti);
- natura obbligatoria o facoltativa del conferimento dei dati (se il soggetto può rifiutare il consenso e le conseguenze di tale rifiuto, specificando che è possibile rifiutare il consenso aI singoli trattamenti, quali quelli ai fini di marketing diretto);
- soggetti e categorie di soggetti ai quali i dati possono essere comunicati e l'ambito di diffusione dei dati medesimi (l'indicazione di soggetti terzi non può essere generica);
- i diritti dell'interessato (diritto di chiedere se dati personali sono presenti nella banca dati, diritto di prenderne visione e di chiederne la modifica,

diritto di presentare reclamo all'Autorità di controllo, eventuale diritto alla portabilità);

- dati identificativi (nome, denominazione o ragione sociale, domicilio o sede) del Titolare del trattamento e, se designato, del Responsabile per la protezione dei dati (DPO), quindi un recapito al quale gli interessati potranno rivolgersi per esercitare i propri diritti;
- quale è la base giuridica del trattamento, quindi se si tratta di trattamento basato su consenso o giustificato da leggi, legittimi interessi (in questo caso specificando quale è il legittimo interesse);
- se il trattamento comporta processi decisionali automatizzati (come la profilazione) deve essere specificato indicando anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

  Nel caso in cui i dati non siano raccolti direttamente presso l'interessato (art. 14 del Regolamento), l'informativa deve essere fornita entro un termine ragionevole, e comunque non oltre un mese dalla raccolta dei dati; oppure va fatta al momento della comunicazione dei dati a terzi.

  Comunque, in questo caso spetta al Titolare valutare se la prestazione dell'informativa agli interessati comporti uno sforzo sproporzionato.

  Il Regolamento specifica molto più in dettaglio rispetto al Codice le caratteristiche dell'informativa, che deve avere forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile; occorre utilizzare un linguaggio chiaro e semplice, e per i minori occorre prevedere informative idonee (si veda anche il Considerando 58).

  L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico (soprattutto nel contesto di servizi online: si vedano art. 12, paragrafo 1, e Considerando 58), anche se sono ammessi "altri mezzi", quindi può essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra (art. 12, paragrafo 1).

  Il Regolamento ammette, soprattutto, l'utilizzo di icone per presentare i contenuti dell'informativa in forma sintetica, ma solo "in combinazione" con l'informativa estesa (art. 12, paragrafo 7); queste icone dovranno essere identiche in tutta l'UE e saranno definite prossimamente dalla Commissione europea.

Sono, inoltre, parzialmente diversi i requisiti che il Regolamento fissa per l'esonero dall'informativa (si veda art. 13, paragrafo 4 e art. 14, paragrafo 5 del Regolamento, oltre a quanto previsto dall'articolo 23, paragrafo 1, di quest'ultimo), anche se occorre sottolineare che spetta al Titolare, in caso di dati personali raccolti da fonti diverse dall'interessato, valutare se la prestazione dell'informativa agli interessati comporti uno sforzo sproporzionato (si veda art. 14, paragrafo 5, lettera b)) – a differenza di quanto prevede l'art. 13, comma 5, lettera c) del Codice.

FURRER in compliance alla normativa in oggetto formalizza informative specifiche, quali ad esempio:

- informativa ai dipendenti;
- informativa ai clienti;
- informativa ai fornitori.
- Informativa visitatori e videosorveglianza

I template delle informative in questione sono reperibili in allegato al presente Manuale di Gestione Privacy nella sezione ALLEGATI E FORMULARIO.

19. I RISCHI IN MATERIA DI PRIVACY

La normativa stabilisce che i dati personali devono essere custoditi e controllati in modo da ridurre al minimo rischi di:

- **distruzione o perdita, anche accidentale, dei dati;**
- **accesso non autorizzato;**
- **trattamento non consentito, tale rischio si riferisce a qualsiasi trattamento non lecito o corretto;**
- **trattamento non conforme** ;
- **modifica dei dati in conseguenza ad interventi non autorizzati o non conformi alle regole**.

Alcuni rischi possono avere natura diversa ad esempio consistere in un reclamo, una segnalazione o addirittura un ricorso al Garante per la protezione dei dati personali da parte della persona fisica alla quale i dati si riferiscono (il cd. **Interessato**).

L'Interessato, infatti, può richiedere la conferma dell'esistenza dei suoi dati e ottenere se lecito, la cancellazione, la trasformazione in forma anonima o il blocco del trattamento dei suoi dati personali trattati in violazione di legge o per motivi di marketing.

Il Garante per la protezione dei dati personali fornisce, inoltre, una lista di possibili rischi a cui sono soggetti i sistemi e che sono mitigabili attraverso le misure previste dal **Disciplinare tecnico in materia di misure minime di sicurezza** (Allegato B al Codice Privacy) o con misure cosiddette necessarie (es. quelle prescritte per il controllo degli Amministratori di Sistema). Nello specifico, sono state individuate le seguenti macro aree e per ognuna di esse sono state associate delle situazioni di rischio:

- ✓ **Comportamenti degli operatori:**
- ✓ furto di credenziali di autenticazione;
- ✓ carenza di consapevolezza;
- ✓ disattenzione o incuria;
- ✓ comportamenti sleali o fraudolenti;
- ✓ errore materiale;
- ✓ **Eventi relativi agli strumenti informatici**:
- ✓ azione di virus o di codici malevoli;
- ✓ spam o altre tecniche di sabotaggio;
- ✓ malfunzionamento;
- ✓ indisponibilità o degrado degli strumenti;
- ✓ accessi esterni non autorizzati;
- ✓ intercettazione di informazioni in rete;
- ✓ **Eventi relativi al perimetro fisico:**
- ✓ accessi non autorizzati a locali/reparti ad accesso ristretto;
- ✓ asportazione e furto di strumenti contenenti dati;
- ✓ eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria, guasto ai sistemi complementari (impianto elettrico, climatizzazione, etc..), errori umani nella gestione della sicurezza fisica.

In conclusione, una attività di auditing qualificata non può prescindere dai risultati dell'analisi e della gestione dei rischi e dalla loro applicazione nelle diverse fasi dell'attività.

20. IL DATA PROTECTION IMPACT ASSESSMENT NEL REGOLAMENTO UE

Il **Data Protection Impact Assessment** (DPIA) o semplicemente Privacy Impact Assessment (PIA) o valutazione d'impatto sulla Privacy rappresenta uno strumento per le aziende, previsto dal Regolamento UE, per rispettare gli obblighi della protezione dei dati ed al contempo assecondare le aspettative degli utenti sul tema Privacy.

Un Privacy Impact Assessment efficace permette alle fondazioni di identificare e risolvere problemi in una fase preliminare, riducendo eventuali costi e danni di reputazione.

Nel Privacy Impact Assessment il livello di rischio può essere, infatti, tradotto in un valore numerico che "misura" gli eventi di rischio di non conformità in materia di Privacy in base alla loro probabilità e sulla base dell'impatto delle loro conseguenze sull'organizzazione; infatti, agli eventi rischiosi in materia di Privacy più probabili e che potrebbero avere un impatto più grave sulla FURRER , sarà associato un livello di rischio più elevato.

Predisporre una valutazione d'impatto Privacy è un obbligo previsto per i trattamenti che comportano elevati rischi per i diritti e le libertà degli interessati.

Per stabilire se un trattamento comporta rischi elevati per i diritti e le libertà degli interessati è necessario prendere in considerazione i seguenti elementi:

1. La valutazione e profilazione di un soggetto, assegnazione di un punteggio o previsione di aspetti personali di un soggetto;
2. Le decisioni automatizzate con conseguenze giuridiche o effetti significativi sulla persona, come ad esempio discriminazioni o esclusioni;
3. Il monitoraggio sistematico, controllo e sorveglianza di soggetti interessati, anche in spazi pubblici;
4. Le categorie di dati particolari (stato di salute, opinioni politiche, credo religioso, etc.) o che possano accrescere potenziali rischi per i diritti e le libertà degli interessati (dati di localizzazione, finanziari, dati strettamente personali e confidenziali, etc.);

5. I dati trattati su larga scala, ovvero relativi ad un elevato numero di soggetti interessati o comprendenti enormi quantità di dati personali;
6. I datasets provenienti da diversi trattamenti e/o da differenti Titolari del trattamento, combinati insieme;
7. I dati relativi a soggetti vulnerabili per proprie condizioni particolari o in quanto non liberi di esprimere il consenso o opporsi ad un trattamento (dipendenti, bambini, pazienti, etc.);
8. I'utilizzo di soluzioni e tecnologie innovative che potrebbero implicare nuove forme di trattamento di dati personali;
9. Il trasferimento di dati personali verso Paesi Extra UE;
10. La natura del trattamento che impedisce agli interessati di esercitare un diritto, ad esempio quando coinvolge aree pubbliche, o di accedere ad un servizio o contratto, ad esempio un'attività di credit scoring che può impedire la ricezione di un prestito.

FURRER dopo avere redatto il Registro delle attività di trattamento in conformità all'art. 30, ha effettuato una valutazione del rischio in relazione ai trattamenti che presentano un maggior rischio Privacy (allegati al Manuale).

21. LA SICUREZZA DEL TRATTAMENTO NEL REGOLAMENTO UE

In ottemperanza all'art. 32 del GDPR, FURRER si prefigge di identificare le misure di sicurezza e valutarne l'adeguatezza. Tale concetto è legato al fatto che le misure di sicurezza devono essere valutate in relazione al rischio del trattamento che si prefiggono di mitigare e sono definite adeguate se saranno efficaci nell'abbassare il livello di rischio collegato al trattamento in questione fino al livello considerato "accettabile" da parte di FURRER .

L'identificazione delle più appropriate misure di sicurezza per un dato trattamento deve avvenire tramite una valutazione dei rischi presentati dal trattamento stesso, i quali derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. Per i dettagli in merito alla metodologia di valutazione

degli impatti Privacy, si rimanda al paragrafo “Il Data Protection Impact Assessment (DPIA)”.

Nella valutazione dell'adeguatezza, FURRER considera anche la tecnologia utilizzata al momento per poter chiaramente identificare i possibili costi da sostenere per modificare le attuali misure di sicurezza. Altre valutazioni riguardano la natura, l'oggetto, il contesto e le finalità del trattamento.

Per rispondere a quanto richiesto dal GDPR nell’art. 32, FURRER richiede al proprio gestore del Sistema Informatico di implementare le seguenti misure di sicurezza:

- la cifratura di dati personali identificati come particolarmente critici per gli interessati (ad esempio i dati delle carte di credito);
- misure di sicurezza logica, di sicurezza fisica, di gestione della rete e di sicurezza perimetrale per assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento (cfr. allegati “Procedura gestione accessi fisici”, “Procedura gestione accessi logici”, “Procedura gestione della rete sicurezza perimetrale”);
- la memorizzazione sistematica dei dati aziendali tramite backup schedulati delle applicazioni, dei database e dei sistemi operativi aziendali al fine di poter ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- controlli II e di III livello che verifichino l’implementazione e l’efficacia delle misure delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento (cfr. allegati “Procedura gestione accessi fisici”, “Procedura gestione accessi logici”, “Procedura gestione della rete sicurezza perimetrale”).

  Le considerazioni relative all’adeguatezza delle misure di sicurezza ha portato FURRER alla definizione di una baseline degli aspetti di sicurezza. Tale baseline prevede l’adozione di misure di sicurezza “minime” per i trattamenti che presentano un rischio basso. In caso di trattamenti con rischio superiore al basso sono definite ulteriori misure di sicurezza da aggiungere alle misure minime, secondo quanto identificato nell’analisi del rischio (rif. “Il Data Protection Impact Assessment DPIA”).

21.1. LA VIDEOSORVEGLIANZA

I sistemi di Videosorveglianza trattano dati personali come la voce e l'immagine che sono da considerarsi, in base alla Direttiva 95/46/CE ed alla normativa italiana, informazioni riferite ad una persona identificata o identificabile.

Nel novembre 2000 il Garante ha emanato delle linee guida contenenti gli indirizzi per garantire che l'installazione di dispositivi per la videosorveglianza rispetti le norme sulla Privacy e sulla tutela della libertà delle persone, in particolare assicurando la proporzionalità tra mezzi impiegati e fini perseguiti.

La materia è stata poi ulteriormente regolata da due provvedimenti generali del Garante, emanati rispettivamente nel 2004 e nel 2010, che contengono prescrizioni vincolanti per tutti i soggetti che intendono avvalersi di sistemi di videosorveglianza e precise garanzie per la privacy dei soggetti i cui dati vengano eventualmente raccolti e trattati tramite tali sistemi.

Il provvedimento dell'**8 aprile 2010**, in particolare, sostituisce il precedente e lo integra tenendo conto delle più recenti disposizioni normative in materia e delle possibilità offerte dalla nuove tecnologie. Una speciale attenzione è dedicata alle garanzie sul fronte dell'informazione ai soggetti che transitano in aree videosorvegliate (sempre obbligatori i cartelli informativi, salvo nel caso di telecamere installate a fini di sicurezza pubblica) e ai limiti per la conservazione dei dati raccolti tramite telecamere e videosorveglianza, che può superare le 24 ore solo in casi particolari (indagini di polizia e giudiziarie, sicurezza degli istituti di credito, etc.).

21.2. SINTESI DELLE REGOLE SU PRIVACY E VIDEOSORVEGLIANZA E LEGGI

La raccolta, la registrazione, la conservazione e, in generale, l'utilizzo di immagini configura un trattamento di dati personali.

È considerato dato personale, infatti, qualunque informazione relativa alla persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione.

La videosorveglianza è utilizzata a fini molteplici, alcuni dei quali possono essere raggruppati nei seguenti ambiti generali:

1. protezione e incolumità degli individui, ivi ricompresi i profili attinenti alla sicurezza urbana, all'ordine e alla sicurezza pubblica, alla prevenzione, all'accertamento o alla repressione dei reati svolti dai soggetti pubblici, alla razionalizzazione e miglioramento dei servizi al pubblico volti anche ad accrescere la sicurezza degli utenti, nel quadro delle competenze ad essi attribuite dalla legge;
2. protezione della proprietà;
3. rilevazione, prevenzione e controllo delle infrazioni svolti dai soggetti pubblici, nel quadro delle competenze ad essi attribuite dalla legge;
4. acquisizione di prove.

   La necessità di garantire, in particolare, un livello elevato di tutela dei diritti e delle libertà fondamentali rispetto al trattamento dei dati personali consente la possibilità di utilizzare sistemi di videosorveglianza, purché ciò non determini un'ingerenza ingiustificata nei diritti e nelle libertà fondamentali degli interessati.

   L'installazione di sistemi di rilevazione delle immagini deve avvenire nel rispetto, oltre che della disciplina in materia di protezione dei dati personali, anche delle altre disposizioni dell'ordinamento applicabili, quali ad esempio le vigenti norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata sul controllo a distanza dei lavoratori.

   In tale quadro, pertanto, è necessario che:

a. il trattamento dei dati attraverso sistemi di videosorveglianza sia fondato su uno dei presupposti di liceità;
b. ciascun sistema informativo ed il relativo programma informatico vengano conformati già in origine in modo da non utilizzare dati relativi a persone identificabili quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi;
c. l'attività di videosorveglianza venga effettuata nel rispetto del c.d. principio di proporzionalità nella scelta delle modalità di ripresa e dislocazione (es. tramite telecamere fisse o brandeggiabili, dotate o meno di zoom), nonché nelle varie fasi del trattamento che deve comportare, comunque, un trattamento di dati pertinenti e non eccedenti rispetto alle finalità perseguite.

   FURRER utilizza sistemi di Videosorveglianza nella propria sede.

Sono state espletate tutte le formalità relative all'accordo sindacale o in alternativa all'ottenimento dell'autorizzazione della DTL al fine di poter installare l'impianto.

Sono state altresì predisposte le informative "minime", indicante il Titolare del trattamento la finalità perseguita e l'informativa estesa.

I cartelli contenenti l'informativa minima:

a. sono stati collocati prima del raggio di azione della telecamera o nelle sue immediate vicinanze;
b. devono avere un formato ed un posizionamento tale da essere chiaramente visibili in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno.

Per le informative si vedano riportate nel formulario Allegato.

FURRER utilizza sistemi di Videosorveglianza nella propria sede. Il trattamento si svolge secondo le modalità definite dal Provvedimento dell'Autorità Garante 8 aprile 2010. Sono state effettuate le nomine delle persone autorizzate al trattamento.

22. SANZIONI

In materia di protezione dei dati personali, il Regolamento GDPR richiede all'azienda di adottare un sistema di policy, misure organizzative e tecniche che consentano di avere un controllo continuo sulla conformità dell'azienda stessa alla normativa. Qualora ciò non accadesse o anche nel caso si evidenziasse la mancanza della conformità a quanto disposto dal Regolamento, sono previste precise **sanzioni** amministrative pecuniarie.

22.1. SANZIONI GRADUALI

Va da sé che le sanzioni seguono un approccio graduale riguardo i criteri per l'imposizione (secondo quanto riportato nell'art. 83, paragrafo 2 del GDPR) e per la determinazione dell'ammontare massimo imponibile. In termini generali, la violazione delle disposizioni può prevedere sanzioni amministrative pecuniarie fino a 20 milioni di euro, oppure per le imprese,

fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore alla predetta cifra.

23. CODICI DI CONDOTTA

Il Regolamento europeo, in caso di sanzioni, prevede l'onere della prova in capo al Titolare e al Responsabile del trattamento: questi quindi dovranno essere in grado di dimostrare di aver messo in atto misure organizzative e di sicurezza adeguate sia alla particolare tipologia di dati che trattano sia agli specifici trattamenti che effettuano. Alla luce di questo codici di condotta e certificazioni possono, di conseguenza, essere utilizzati come elementi di prova. Secondo il Regolamento, l'elaborazione di codici di condotta dovrebbe essere incoraggiata dagli Stati membri. In particolare, questi dovrebbero essere redatti dalle associazioni e dalle organizzazioni che rappresentano categorie di Titolari del trattamento o di Responsabili del trattamento e dovrebbero tenere conto delle caratteristiche specifiche dei settori di riferimento e delle diverse esigenze connesse alle dimensioni aziendali.

In particolare, secondo l'art. 40 del Regolamento, potrebbero concernere:

- il trattamento corretto e trasparente dei dati;
- i legittimi interessi perseguiti dal Responsabile del trattamento in contesti specifici;
- la raccolta dei dati personali;
- la pseudonimizzazione;
- l'informazione fornita al pubblico e agli interessati;
- l'esercizio dei diritti degli interessati;
- la protezione del minore e le modalità con cui è ottenuto il consenso dei Titolari della Responsabilità genitoriale sul minore;
- le misure di sicurezza;
- la notifica dei Data Breach e la relativa comunicazione agli interessati;
- il trasferimento di dati personali verso paesi terzi;
- le procedure stragiudiziali di composizione delle controversie.

Il progetto di codice dovrà essere sottoposto all'Autorità garante nazionale e questa esprimerà un parere sul progetto. Se il parere è positivo e l'applicazione del Codice riguarda solamente lo Stato membro in cui è

presentato, l'Autorità registrerà e pubblicherà il Codice realizzato. Nel caso in cui, invece, il progetto di codice di condotta si riferisca a trattamenti realizzati in vari Stati membri, prima che vi sia approvazione definitiva, occorre un secondo esame a livello europeo, con il coinvolgimento del Comitato europeo per la protezione dei dati. Qualora anche a seguito di tale controllo, il progetto ottenga un parere favorevole, sarà registrato e pubblicato. Ai sensi del Regolamento, inoltre, la Commissione ha il potere di decidere che il codice di condotta abbia validità generale all'interno dell'Unione; in tal modo, il codice è reso applicabile a tutto il settore di riferimento, in tutto il territorio dell'Unione Europea.

Tutti i Codici di condotta sono raccolti dal Comitato in un apposito registro e la Commissione è tenuta a dare pubblicità a quelli che hanno acquisito validità generale.

24. LE CERTIFICAZIONI

Il Regolamento inoltre, incoraggia l'istituzione di meccanismi di certificazione, sigilli e marchi di protezione dei dati che consentano agli interessati di valutare rapidamente il livello di protezione dei dati.

La certificazione è:

- volontaria;
- accessibile tramite una procedura trasparente;
- rilasciata al Titolare o al Responsabile del trattamento da appositi organismi di certificazione o dall'Autorità garante – per un periodo massimo di tre anni, rinnovabili.

Gli organismi di certificazione devono possedere un livello di conoscenza della materia adeguato, essere indipendenti ed essere accreditati. Per poter ottenere l'accreditamento, gli organismi devono dimostrare indipendenza e competenze specifiche e presentare le procedure che intendono seguire ai fini della verifica del rispetto dei criteri. L'aver aderito ad un codice di condotta o l'essersi certificato, non libera il Titolare né il Responsabile del trattamento dalla responsabilità di conformità al Regolamento e lascia impregiudicati i compiti e i poteri delle autorità di controllo competenti. Alla luce di quanto fino ad ora descritto, al momento di decidere se infliggere una sanzione amministrativa pecuniaria e fissare l'ammontare

della stessa, si terrà in conto anche dell'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'art. 42. Nei tavoli di lavoro a Bruxelles, tra le proposte delle delegazioni italiane, vi sarebbe quella di imporre un obbligo di certificazione privacy per poter accedere alla partecipazione di specifici bandi di gara delle Pubbliche Amministrazioni. Altre delegazioni si sono spinte anche oltre, proponendo certificazioni obbligatorie anche sui prodotti. Ad oggi nessuno può sapere con certezza quanto tempo potrà essere necessario a che il gruppo dei garanti europei decida di attivare le certificazioni e i codici di condotta. Prima che possano essere emanate le linee guida dal comitato europeo dei garanti infatti, si rendono necessari almeno due passaggi:

- la piena attuazione del Regolamento, con costituzione e insediamento del Gruppo dei Garanti Europei, le cui linee guida saranno vincolanti per le Autorità degli Stati membri;
- la definizione da parte del comitato dei criteri di certificazione e di quelli relativi agli enti che potranno essere certifica.

ALLEGATI E PROCEDURE

ALLEGATO 1. ELENCO DELLE PROCEDURE

a. Procedura data retention policy
b. Procedura data breach
c. Procedura gestione visite ispettive
d. Procedura gestione istanze degli interessati
e. Procedura flussi informativi

ALLEGATO 2. ELENCO DELLE NOMINE

a. Nomina a Responsabile interno al trattamento dei dati
b. Nomina a Responsabile esterno
c. Nomina Autorizzato al trattamento dei dati personali comuni
d. Nomina Responsabile Videosorveglianza
e. Nomina Incaricato Videosorveglianza
f. Nomina Amministratore di Sistema
g. Nomina a Responsabile esterno Medico competente

ALLEGATO 3. ELENCO DELLE INFORMATIVE

a. Informativa al dipendente
b. Informativa Privacy Visitatori con Videosorveglianza
c. Informativa ai clienti e fornitori

ALLEGATO 4. REGOLAMENTO EUROPEO N.2016/679