Rotair S.p.A.

PRIVACY COMPLIANCE PROGRAM
Manuale di Gestione Privacy

MANUALE DI GESTIONE PRIVACY
ai sensi
del Regolamento UE n. 2016/679

SCHEDA CONTROLLO DOCUMENTO
IDENTIFICAZIONE

TITOLO DEL DOCUMENTO	Manuale di Gestione Privacy di Rotair S.p.A.

VERSIONE	**DATA APPROVAZIONE**
1.0	25 maggio 2018
2.0	
3.0	

Il Manuale di Gestione Privacy (di seguito anche **"Manuale Privacy"**) di Rotair S.p.A. (di seguito anche "**Società**") è stato:

- approvato dal Titolare del Trattamento dei dati in data 25 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 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.

Indice

1. PREMESSA

Con il Regolamento Europeo 2016/679 (di seguito anche **"Regolamento UE"**) 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. OBIETTIVI DEL MANUALE DI GESTIONE PRIVACY

La Società 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 Regolamento UE.

A tal fine la Società 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, la Società 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 Società stessa tramite la protezione dei dati personali.

Infatti, attraverso l'adozione del presente Manuale di Gestione Privacy la Società 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 della Società;

- diffondere ed affermare una cultura d'impresa improntata alla legalità, con l'espressa riprovazione da parte della Società 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 Società 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. DESCRIZIONE DELLA SOCIETA' ROTAIR S.P.A.

La Società vanta ben cinquant'anni di esperienza nella progettazione, produzione e distribuzione di un'ampia gamma di prodotti tecnologicamente avanzati per la costruzione e l'agricoltura.

La Società progetta e produce all'interno dei propri stabilimenti una vasta gamma di prodotti quali compressori diesel, compressori elettrici, martelli idraulici, motocarriole multifunzione. Tutti i prodotti della Società vengono realizzati nel rispetto dell'ambiente e in conformità agli standard europei e internazionali con riferimento alla qualità e ai processi produttivi. La Società mette in evidenza, con fierezza, le sue capacità produttive, certificate da un non indifferente numero di brevetti.

4. LA PRIVACY

"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 dell'informazione.

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;

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

- 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 UE approvato il 14 aprile 2016 dal Parlamento UE.

6. IL REGOLAMENTO UE

Il Regolamento UE 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 UE 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 UE ("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 UE.

- 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 UE

Il Regolamento UE 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 UE 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 Regolamento UE 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 UE 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 trattamento.

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.

6.3 La struttura del Regolamento UE

	Capitoli	Articoli
1	Disposizioni generali: • oggetto e finalità del Regolamento • ambito di applicazione • ambito di applicazione per territorio • definizioni	1-4
2	Principi: • principi generali • liceità • consenso • consenso dei minori • particolari categorie di dati • trattamenti relativi a condanne penali e reati • trattamenti senza identificazione	5-11
3	Diritti dell'interessato	12-23
4	Titolare del Trattamento e responsabile del Trattamento	24-43
5	Trasferimenti dati personali verso paesi terzi o organizzazioni internazionali	44-50

6	Autorità di controllo indipendenti	51-59
7	Cooperazione e coerenza	60-76
8	Mezzi di ricorso responsabilità e sanzioni	77-84
9	Disposizioni relative a specifiche situazioni di trattamento	85-91
10	Atti delegati e atti di esecuzione	92-93

6.4 Le principali definizioni in materia di privacy ai sensi del Regolamento UE 2016/679

Le principali definizioni in materia di Privacy ai sensi del **Regolamento UE** 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 a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- **"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 per-

sonali, 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

Ai sensi del Regolamento UE, 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** a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
- **esatti** e, se necessario, **aggiornati;** devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti 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 UE 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 alle società l'obbligo di avviare un progetto prevedendo, fin da subito, gli strumenti a tutela dei dati personali.

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;
- centralità dell'utente.

Gli elementi che devono essere esaminati al momento dell'inizio dell'attività o del processo sono:

- Tipologia di dati trattati;
- Finalità del trattamento;
- Interessati del trattamento;
- Necessità di acquisizione del consenso scritto;
- Necessità della nomina di responsabili esterni;
- Trasferimento dei dati all'estero extra Ue.

Privacy by default

Il principio di privacy by default stabilisce, invece che le società devono 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 sensibilizzati gli Addetti Autorizzati con riferimento alle modalità di acquisizione e gestione, in modo da garantirne sempre il rispetto della normativa sulla privacy, riducendone a priori il rischio di diffusione o trattamento illecito.

La Società ha sensibilizzato gli addetti autorizzati al fine di garantire il rispetto della normativa privacy fin dall'avvio di ogni singola attività o iniziativa all'interno dei processi aziendali.

Il principio di "accountability"

Tra i principi cardine del Regolamento UE vi è il principio di "accountability**"** (ovvero di "responsabilizzazione").

L'art. 5 del Regolamento UE 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. II dell'art. 5 stabilisce, poi 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.

La Società in ottemperanza del principio di accountability ha formalizzato:

- funzionigramma privacy (Allegato 1);
- il Registro delle attività di trattamento ed una PRE-DPIA (Allegato 2);
- un documento che recepisce la Metodologia di analisi dei rischi per i diritti e le libertà degli interessati (Allegato 3);
- un sistema di procedure e istruzioni operative al fine di gestire il rischio privacy (Allegato 4).

La Società garantisce lo svolgimento delle attività di formazione del personale in materia di protezione dei dati personali, al fine di garantire il rispetto della normativa applicabile da parte di chiunque ponga in essere attività di trattamento dei dati personali all'interno della struttura aziendale sotto l'autorità del titolare del trattamento e abbia accesso ai dati personali. A consolidamento della formazione svolta, possono essere promosse iniziative periodiche di awareness (i.e., flash test o invio di comunicazioni ad hoc) al fine di sensibilizzare i soggetti coinvolti nelle attività di trattamento sui temi correlati alla privacy e a rafforzare la consapevolezza circa la necessità di protezione dei dati personali.

Inoltre, la Società effettuerà degli audits annuali al fine di verificare il rispetto del Regolamento UE e della normativa privacy applicabile.

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.

La Società ha definito una specifica procedura per la corretta individuazione degli eventi di violazione dei dati personali (data breach) (Allegato 4), 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 illecito dei dati personali trasmessi, memorizzati o altrimenti trattati".

10. L'AUTORITA' DI CONTROLLO ED IL COMITATO EUROPEO DELLA PROTEZIONE DEI DATI PERSONALI

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.
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 UE 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 co-decisione, 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. La sua sede è a Piazza di Monte Citorio n. 121 in Roma.
Con il nuovo Regolamento UE l'Autorità di controllo interviene principalmente ex post, cioè la sua valutazione si colloca successivamente alle valutazioni del titolare del trattamento.

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 Garante

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 di proprio personale agli accessi alle 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 normativa Privacy, 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** o nelle relative appartenenze, 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 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 da 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 Privacy. 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 il Garante Privacy, 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 Addetti autorizzati;

- 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 provvedimenti specifici per trattamenti particolari (i.e. 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.
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.

La Società ha formalizzato una specifica procedura per la corretta gestione delle Visite Ispettive del Garante Privacy (Allegato 4).

11. LE LINEE GUIDA DELL'AUTORITA' GARANTE E DEL GRUPPO DI LAVORO EX ART. 29 SPECIFICHE PER LE AREE DI ATTIVITA' DEL GRUPPO.

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

✓ **Linee guida in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (26 luglio 2012)**
✓ **Linee guida del Garante per posta elettronica e Internet (1 marzo 2007)**
✓ **Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati (23 novembre 2006)**
✓ **Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del Regolamento (UE) 2016/679 (13 dicembre 2016)**
✓ **Linee guida sul diritto alla portabilià dei dati (4 aprile 2017)**

12. I PROVVEDIMENTI DELL'AUTORITA' GARANTE DI INTERESSE SPECIFICO PER LA SOCIETA' ROTAIR S.P.A.

Di seguito si elencano alcuni dei principali Provvedimenti del Garante Privacy di interesse per la Società (che resteranno validi fino a quando non saranno revisionati a seguito del Regolamento):

- **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. n. 201/2011 - 20 settembre 2012.

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

- **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.

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.

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 a 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

Ai sensi dell'art. 4 del Regolamento UE 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"

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, conforme-

mente 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»).

14.2 Cessazione del trattamento dei dati

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

a) distrutti;

b) ceduti ad altro titolare, purché destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti;

c) conservati per fini esclusivamente personali e non destinati ad una comunicazione sistematica o alla diffusione;

d) 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 società, la Capo Gruppo e le controllate sono distinti titolari del trattamento, avendo una personalità giuridica distinta. In tal caso il trasferimento dei dati tra le società del Gruppo deve essere autorizzata dagli interessati.

La Società Rotair S.p.A. è Titolare del trattamento dei dati.

15.2 Contitolarità (Joint controllers)

E' possibile che coesistano più titolari del trattamento (contitolari o jointes controllers) che decidono 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 uno qualsiasi dei contitolari.
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 mezzi del trattamento. Si ipotizza quindi la necessità della sussistenza di una codecisione in merito alle finalità (perché) e a i 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 del trattamento

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, ha la facoltà di nominare uno o più responsabili esterni.

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 sufficienti 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); 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.

La Società ha formalizzato la nomina dei Responsabili esterni del trattamento dei dati.
Sono stati nominati **Responsabili esterni** tutti quei soggetti partner esterni della Società che nell'ambito della partnership contrattuale trattano dati personali per conto della Società (Allegato 5).
La Società inserisce una specifica clausola all'interno dei relativi contratti che, mediante la sottoscrizione del contratto stesso, comporta la accettazione della nomina a responsabile esterno da parte dell'*outsourcer* (Allegato 6).

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)(art. 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.

E' richiesto, inoltre che il Titolare metta a disposizione del DPO le risorse umane e finanziarie necessarie all'adempimento dei suoi compiti.

Il Data Protection Officer ha il compito di informare e consigliare il Titolare o il Responsabile del trattamento, nonché i dipendenti, in merito agli obblighi derivanti dal Regolamento Europeo e dalle altre disposizioni dell'UE o delle normative locali degli Stati membri relative alla protezione dei dati.

Deve verificare che la normativa vigente e le policy interne del Titolare siano correttamente attuate ed applicate, incluse le attribuzioni delle responsabilità, la sensibilizzazione e la formazione del personale, ed i relativi audit. Su richiesta del titolare deve fornire pareri in merito alla valutazione d'impatto sulla protezione dei dati, sorvegliandone poi i relativi adempimenti.

Il Data Protection Officer è altresì un punto di contatto sia con il Garante della Privacy che con gli interessati, che possono rivolgersi a lui anche per l'esercizio dei loro diritti.

Ai sensi dell'Art. 37 del Regolamento UE il Titolare del trattamento ed il Responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:

- il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
- le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
- le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 del Regolamento o di dati relativi a condanne penali e a reati di cui all'articolo 10.

Un Gruppo imprenditoriale può nominare un unico responsabile della protezione dei dati, a condizione che un responsabile della protezione dei dati sia facilmente raggiungibile da ciascuno stabilimento.

Il DPO è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39 del Regolamento UE.

Il Titolare del trattamento o il Responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo.

Il Titolare del trattamento e il Responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

Il Titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione dei suoi compiti. Il Responsabile della Protezione dei dati non è rimosso o penalizzato dal Titolare del Trattamento o dal Responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.

Gli interessati possono contattare il DPO per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.

Il DPO è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri e può svolgere altri compiti e funzioni, ma il titolare del trattamento o il responsabile del trattamento si assicurano che tali compiti e funzioni non diano adito a un conflitto di interessi.

15.5 Autorizzato al trattamento (ex incaricato del trattamento dei dati personali)

Il Regolamento UE 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).
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.

La Società in compliance alla normativa in oggetto formalizza la nomina delle persone autorizzate al trattamento dei dati ai sensi dell'art. 4 del Regolamento UE nelle persone di tutti i dipendenti che trattano i dati all'interno della Società (Allegato 7)
La nomina delle persone addette avviene al momento dell'assunzione delle persone che vengono adeguatamente formate.

15.6 L'Amministratore di Sistema (provv. garante privacy 27/11/2008, modificato da provv.25/06/2009)

La figura dell'Amministratore di Sistema 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 alla 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 però 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 (i.e. per scopi di manutenzione a seguito di guasti o malfunzioni) sui sistemi di elaborazione e sui sistemi software.
Di seguito sono riportati i profili e l'elenco delle attività possibili svolte dagli amministratori di sistema.

- **Amministratore di Sistema di Riferimento**
  E' l'amministratore di riferimento per il trattamento. A lui fanno capo tutte le attività di coordinamento e delega verso gli altri amministratori di sistema dei server/servizi.
- **Amministrazione Sistema Operativo**
  Questo profilo comprende tutte le attività necessarie ad amministrare un sistema operativo e la sua sicurezza informatica. L'amministratore è responsabile della messa in sicurezza del sistema operativo, dell'applicazione delle patch di sicurezza e della verifica con cadenza periodica dei log file di sistema.

- **Amministrazione Database Server**
  Questo profilo comprende tutte le attività necessarie ad amministrare un database server e la sua sicurezza informatica. L'amministratore è responsabile della messa in sicurezza del Database server, dell'applicazione delle patch di sicurezza e della verifica con cadenza periodica dei log file/transaction log.
- **Amministrazione Dati**
  Questo profilo comprende tutte le attività necessarie ad amministrare un'application server ed i suoi dati in esso contenuto. L'amministratore è responsabile della messa in sicurezza del sistema, dei processi e applicazioni utili al sistema e all'applicazione delle patch di sicurezza e della verifica con cadenza periodica dei log file.
- **Installazione Patch**
  Questo profilo comprende tutte le attività relative alla verifica ed installazione delle patch di sicurezza indicate dal vendor software/hardware.
  Le patch di sicurezza permettono di risolvere lacune di sicurezza del sistema e proteggere l'accesso ai dati da terze parti.
- **Gestione Aspetti di Sicurezza**
  Questo profilo comprende tutte le attività di hardening svolte sul sistema operativo, application server, database server e applicazioni.
  Le attività sono molteplici e dipendenti dal sistema/servizio. L'amministratore di sistema deve seguire le best practicies rilasciate dai vendor software, contestualizzare ed applicare secondo la situazione aziendale.

La Società in compliance alla normativa in oggetto formalizza la nomina degli Amministratori di Sistema mediante specifica lettera ai singoli AdS, che prevede la designazione in base alla valutazione delle competenze professionali, l'indicazione dei sistemi ai quali gli Amministratori di Sistema stessi sono preposti, le loro responsabilità e incombenze e l'espressa accettazione della nomina stessa (Allegato 8)

16. L'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.

16.1 I diritti dell'interessato

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 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 aversi 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 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

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 s'intende rettificare.
Si tratta di uno strumento volto a consentire di tutelare l'identità personale degli individui e il loro diritto a che 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 UE afferma, oggi, 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. 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 portata e 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 at-

tesa 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 addetti autorizzati.

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 manifestamente 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 oralmente.

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/addetto autorizzato 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 ovvero all'invio per via telematica.

La Società in compliance alla normativa in oggetto al fine di gestire correttamente la gestione delle istanze degli interessati ha formalizzato una specifica procedura per

la gestione delle istanze degli interessati (Allegato 4) che definisce le istruzioni operative per la gestione delle singole richieste.

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 venga rilasciata 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 a singoli trattamenti quali quelli a 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;
- qual è la base giuridica del trattamento, quindi se si tratta di trattamento basato su consenso o giustificato da leggi, legittimi interessi (art. 6 del Regolamento);
- 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).

La Società in compliance alla normativa in oggetto formalizza informative specifiche quali ad esempio:

- informativa ai dipendenti;
- informativa ai fornitori;
- informativa ai candidati;
- informativa ai clienti;
- Informativa per la richiesta di informazioni tramite il sito internet;
- informativa estesa cookies.

I template delle informative in questione sono reperibili in allegato al presente Manuale di Gestione Privacy (Allegato 9).

19. Privacy e cookie

La Società sul proprio sito utilizza cookie tecnici. Si ritiene perciò importante dare un inquadramento breve sulla disciplina dei cookie, in materia di 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 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, che l'utente sta visitando ad installare il cookie, 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 servizio 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 società 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.

Il sito internet della Società utilizza esclusivamente cookie tecnici e cookie di terze parti (Google Analytics) a fini statistici.
La Società ha predisposto un'informativa estesa sul trattamento dei dati chiara, completa ed esaustiva (Allegato 9).

20. 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 di 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.

21. 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 Società 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 Società, 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 (i.e. stato di salute, opinioni politiche, credo religioso) o dati aventi carattere altamente personale;
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 (i.e. dipendenti, bambini, pazienti);
8. l'utilizzo di soluzioni e tecnologie innovative che potrebbero implicare nuove forme di trattamento di dati personali;
9. 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.

Il documento "*Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*" adottato in data **4 ottobre 2017** dal Working Party (nel seguito anche "**WP29**") ribadisce come la DPIA, anche in caso di non obbligatorietà, sia un importante strumento per comprovare la conformità del Titolare del trattamento al Regolamento UE e per determinare l'adozione di misure di sicurezza realmente adeguate al trattamento e ai rischi.
Per poter essere uno strumento efficace, il PIA necessita di un aggiornamento costante, in funzione dei cambiamenti apportati al trattamento, del contesto in mutamento, dell'evoluzione tecnologica, dei rischi, etc.
Le linee guida del WP29 individua in ogni caso un periodo massimo di 3 anni per la revisione della DPIA.
Il soggetto a cui compete la redazione e l'aggiornamento di una DPIA è il Titolare del trattamento, eventualmente supportato ove previsto dal Data Protection Officer.
Nel caso in cui il trattamento sia affidato ad un Responsabile esterno del trattamento, quest'ultimo è tenuto a collaborare con il Titolare del trattamento per svolgere correttamente la valutazione d'impatto.
Per quanto concerne la metodologia da utilizzare per l'elaborazione della valutazione d'impatto, il WP29 lascia libertà di scelta per la forma e la struttura da utilizzare, purché contenga gli elementi previsti dal Regolamento Ue ed esplicitati all'interno dell'Annex 2 delle linee guida del WP29 e quindi:

1. descrizione sistematica del trattamento (natura, scopo, contesto e finalità del trattamento, categorie di dati e di soggetti interessati, gli strumenti in uso per il trattamento, adesioni a Codici di condotta);
2. valutazione delle misure che contribuiscono a garantire la necessità e la proporzionalità del trattamento (i.e. legittime e specifiche finalità, liceità del trattamento, minimizzazione dei dati, conservazione limitata dei dati, informative,

consensi, rispetto dei diritti, destinatari, responsabili, garanzie per il trasferimento dei dati extra UE);

3. analisi dei rischi per i diritti e le libertà degli interessati (origine e natura dei rischi, impatti potenziali alle libertà e ai diritti in caso di perdita di riservatezza, integrità e disponibilità dei dati, minacce che incombono sui dati, probabilità e gravità dei rischi, misure previste per ridurre e gestire i rischi);
4. coinvolgimento delle parti interessate (supporto del DPO e parere dei soggetti interessati in relazione alla valutazione d'impatto del trattamento).

La Società, dopo aver redatto il Registro delle attività di trattamento in conformità all'art. 30 del Regolamento (UE), ha effettuato una PRE- DPIA (Allegato 2) da cui non sono emersi dei trattamenti per cui è necessaria una valutazione del rischio. Al contrario sono emersi dei trattamenti che soddisfano un solo criterio tra i nove criteri elencati e la Società ha deciso di non condurre la DPIA per tali trattamenti (Allegato 3).

22. LA CONSULTAZIONE PREVENTIVA

Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.
Se ritiene che il trattamento previsto violi il Regolamento, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, l'autorità di controllo fornisce, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto al titolare del trattamento e, ove applicabile, al responsabile del trattamento e può avvalersi dei poteri di cui all'articolo 58.
Tale periodo può essere prorogato di sei settimane, tenendo conto della complessità del trattamento previsto. L'autorità di controllo informa il titolare del trattamento e, ove applicabile, il responsabile del trattamento di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione. La decorrenza dei termini può essere sospesa fino all'ottenimento da parte dell'autorità di controllo delle informazioni richieste ai fini della consultazione.
Al momento di consultare l'autorità di controllo ai sensi del paragrafo 1, il titolare del trattamento comunica all'autorità di controllo:

a) ove applicabile, le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un Gruppo imprenditoriale;
b) le finalità e i mezzi del trattamento previsto;
c) le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del presente regolamento;
d) ove applicabile, i dati di contatto del titolare della protezione dei dati;

e) la valutazione d'impatto sulla protezione dei dati di cui all'articolo 35;
f) ogni altra informazione richiesta dall'autorità di controllo.

Gli Stati membri consultano l'autorità di controllo durante l'elaborazione di una proposta di atto legislativo che deve essere adottato dai parlamenti nazionali o di misura regolamentare basata su detto atto legislativo relativamente al trattamento.
Nonostante il paragrafo 1, il diritto degli Stati membri può prescrivere che i titolari del trattamento consultino l'autorità di controllo, e ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica.

23. IL TRATTAMENTO DEL RISCHIO PRIVACY

Una volta che il rischio Privacy è stato analizzato e valutato, occorre procedere alla gestione dello stesso.
La gestione del rischio può essere definita come il processo di identificazione, controllo, eliminazione o riduzione degli eventi che possono avere un impatto negativo sulle risorse del sistema.
La scelta del metodo di Gestione del Rischio è legata alle dimensioni del **SGSI** (Sistema di gestione della Sicurezza delle informazioni) ed al tipo di Business della Società.
Il Garante della Privacy ha precisato come l'analisi dei rischi che incombono sui dati debba analizzare i principali eventi potenzialmente dannosi per la sicurezza degli stessi e ne debba valutare le possibili conseguenze e la gravità in relazione al contesto fisico-ambientale di riferimento ed agli strumenti elettronici utilizzati.
Il Regolamento UE si occupa del tema della sicurezza alla Sezione 2 "Sicurezza **dei dati personali", all'art. 32** intitolato **"Sicurezza del trattamento"**.

24. LA SICUREZZA DEL TRATTAMENTO NEL REGOLAMENTO UE

In ottemperanza all'art. 32 del Regolamento UE, la Società 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 efficaci nell'abbassare il livello di rischio collegato al trattamento in questione fino al livello considerato "accettabile" dalla Società.
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, la Società 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.

25. SANZIONI

In materia di protezione dei dati personali, il Regolamento 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 specifiche **sanzioni** amministrative pecuniarie.

25.1 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.

26. CODICI DI CONDOTTA

Il Regolamento UE, 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.

27. LE CERTIFICAZIONI

Il Regolamento UE 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 UE 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'articolo 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 UE, 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 certificati