Privacy

Regolamento UE 2016/679 (GDPR) e D. Lgs n° 196 del 30/06/2003 modificato dal D. Lgs n° 101 del 10/08/2018

Titolare del Trattamento

Gastaldi Holding S.p.A.

DATA PROTECTION POLICY

(Regole Generali emanate dalla Holding per la Compliance privacy del Gruppo)

Sommario

1. INFORMAZIONI SUL DOCUMENTO

1.1. SCOPO

Scopo del presente documento è definire una policy - titolata "Data Protection Policy" - volta a richiamare gli obblighi a cui **tutti** i dipendenti e collaboratori (di seguito congiuntamente definiti gli "**Utenti**") di **Gastaldi Holding S.p.A.** e delle società del GRUPPO GASTALDI (congiuntamente a **Gastaldi Holding S.p.A.** definite: "GRUPPO GASTALDI" o "Società del Gruppo") devono attenersi per garantire la conformità dei trattamenti dei dati personali eseguiti rispetto al Regolamento europeo 2016/679 (il "Regolamento Privacy" o "GDPR") ed alla normativa nazionale vigente in materia di privacy.

1.2. AMBITO DI APPLICAZIONE

Il presente documento si applica a tutte le aziende del GRUPPO GASTALDI.

1.3. RIFERIMENTI

La presente policy determina la struttura intersocietaria di presidio e gestione delle tematiche regolate del suddetto Regolamento UE 2016/679 e dalle altre normative applicabili in relazione alla protezione dei Dati Personali.

1.4. RESPONSABILITÀ

Le responsabilità dell'applicazione della presente procedura sono dettagliate nel seguito del presente documento.

L'aggiornamento di questa procedura è responsabilità dell'Unità di Coordinamento Privacy all'interno del GRUPPO GASTALDI.

1.5. ARCHIVIAZIONE

La presente procedura è a disposizione su INTRANET aziendale all'indirizzo: …….. L'originale cartaceo firmato è conservato presso la Segreteria di Direzione della Gastaldi Holding S.p.A.

1.6. ALLEGATI

1. Modello di informativa per dipendenti e collaboratori;
2. Modello di registro dei trattamenti da titolare;
3. Modello di registro dei trattamenti da responsabile;
4. Modello di procedura di gestione dei diritti degli interessati;
5. Modello di registro delle richieste degli interessati;
6. Modello di procedura per la gestione delle violazioni;
7. Modello di procedura Data Breach;
8. Modello di analisi dei rischi per trattamento derivata da ENISA;
9. Modello di accordo sul trattamento dati personali dei Responsabili
10. Modello di Nomina ad "Addetto al Trattamento"
11. Modello di clausole contrattuali Privacy.
12. Modello Organigramma

2. DATA PROTECTION POLICY

2.1. PREMESSE E NOTE APPLICATIVE

Come definito al punto **1.1 "SCOPO"** La presente Data Protection Policy è volta a richiamare gli obblighi a cui tutti i gli "**Utenti**" della GASTALDI HOLDING S.p.A. e delle **Società del Gruppo** e, disgiuntamente da GASTALDI, "**Società Controllata/e**") devono attenersi per garantire la conformità dei trattamenti dei dati personali eseguiti rispetto al Regolamento europeo 2016/679 (il "**Regolamento Privacy**" o "**GDPR**") ed alla normativa nazionale vigente in materia di privacy.

Conseguentemente, tutte le policy aziendali in materia di privacy e trattamento dei dati personali adottate dalle Società del Gruppo dovranno conformarsi ai principi e alle linee guida riportate nella presente Data Protection Policy, ferma restando la possibilità, per ciascuna Società Controllata, di adottare accorgimenti, integrazioni, anche di carattere procedurale, in ragione delle rispettive peculiarità organizzative e di business, per un adeguamento completo ed ottimale alla disciplina vigente.

Si evidenzia che il Regolamento Privacy richiede un livello di diligenza, attenzione e di controllo sulle modalità di trattamento dei dati personali di gran lunga maggiore rispetto a quanto previsto dal previgente Codice Privacy, introducendo sanzioni **sino ad un massimo del 4% del fatturato globale annuo del soggetto che commette la violazione**.

Ne consegue che è **di primaria importanza la revisione e comprensione della presente Data Protection Policy e che tutti i dipendenti, collaboratori, e, in generale, terzi persone fisiche che trattano i dati per conto delle Società del Gruppo si conformino ai suoi contenuti**.

Tutti gli Utenti sono, pertanto, informati e tenuti a adeguarsi ai requisiti della presente Data Protection Policy e ad accettarne espressamente i contenuti.

L'esecuzione di trattamenti di dati personali secondo modalità che contrastino con i principi e le linee guida previste dalla presente Data Protection Policy e dalla Normativa Privacy (si veda a seguire) applicabile potrebbe costituire presupposto dell'adozione di azioni disciplinari e/o dare luogo, nei casi normativamente previsti, a procedimenti civili e penali.

La presente Data Protection Policy è strutturata nelle seguenti sezioni:

- *Regole per il corretto trattamento dei dati personali e per la corretta classificazione e gestione delle informazioni*;
- *Regole per il corretto archivio dei documenti aziendali e per l'utilizzo appropriato e consapevole delle informazioni, dei sistemi e dei servizi*;
- *Monitoraggio e controllo***.**

2.2. RIFERIMENTI

1. Regolamento (UE) 2016/679 del Parlamento e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, di seguito il "**Regolamento Privacy**" o "**GDPR**";
2. D. Lgs. n. 196/2003, emendato dal D. Leg. 101 del 10/08/2018 di seguito il "**Codice Privacy**" come successivamente modificato e integrato dai vari provvedimenti che si sono succeduti dopo agosto 2018;
3. Linee guida dell'European Data Protection Board e del precedente "Gruppo ex art. 29";
4. Provvedimenti dell'Autorità Garante della Protezione Dati Personali;

2.3. DEFINIZIONI

Le definizioni che seguono sono riprese dall'articolo 4 del GDPR che è fonte primaria della definizione.

Dato personale: indica qualsiasi informazione riguardante una persona fisica identificata o identificabile (definito "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 (GDPR art. 4 e Considerando C26, C27, C30).

Il dato personale può riferirsi solo ad una persona fisica (i.e. un individuo) e comprende anche ditte individuali e i liberi professionisti, mentre non comprende i dati delle persone giuridiche (i.e. società). L'indirizzo e-mail aziendale legato ad uno specifico individuo (e.g. nome.cognome@società̀delgruppo.it è un dato personale, mentre l'indirizzo e-mail generico (e.g. info@società̀delgruppo.it) non è considerato un dato personale.

Categorie particolari di dati personali: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché 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 (art. 9 GDPR).

Le categorie particolari di dati personali che comprendono anche i:
"**dati relativi alla salute**" intesi come 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;
"**dati genetici**" intesi come 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; e
"**dati biometrici**" intesi come 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.
In caso di trattamento delle categorie particolari di dati personali sopra indicati, il GDPR prevede maggiori e specifici obblighi.

Interessato: indica la persona fisica (ivi comprese le ditte individuali e i liberi professionisti) a cui i dati personali si riferiscono.

Informativa privacy: indica tutte le informazioni di cui agli articoli 13 e 14 del GDPR e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 del GDPR relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori, fornite dal Titolare mediante l'adozione di misure appropriate. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato (art. 12 GDPR, C58-C60,C64).

Trattamento: indica qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (art. 4 GDPR).

Profilazione: indica qualsiasi forma di trattamento automatizzato di dati personali consistente **nell'utilizzo** di tali dati personali per **valutare** determinati aspetti personali relativi ad una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica (art. 4 GDPR, C24,C30,C71-C72).

Consenso al trattamento: indica 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 (art. 4 GDPR, C32, C33).

Titolare del trattamento: indica 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 (art. 4 GDPR, C74); indica, pertanto, il soggetto che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento dei dati personali.

Responsabile del trattamento: indica la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento (art. 4 GDPR); indica, pertanto, il soggetto (società o individuo) che tratta i dati personali per conto del Titolare del trattamento.

La categoria dei Responsabili del trattamento comprende, tra gli altri, società di elaborazione/gestione buste paga e di ricerca e di formazione del personale, fornitori di infrastrutture IT e, più in generale, chiunque tratta dati personali dei clienti, dipendenti e fornitori (nei limiti applicabili) delle società del GRUPPO GASTALDI per conto delle stesse. In tutti i casi in cui una delle società del GRUPPO GASTALDI stipula un contratto che comporta l'accesso, la raccolta o l'utilizzo di dati di clienti, dipendenti o fornitori delle stesse.

Violazione dei dati personali o *data breach*: indica 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 (art. 4 GDPR, C85).

Data Protecion Officer (DPO): Visto l'Art. 37 del Regolamento EU 2016/679 (GDPR) cap. 1. b), c).
In considerazione delle "Linee guida sui responsabili della protezione dei dati (RPD) – WP 243 rev.01" in particolare: il capitolo 2) "Nomina di un RDP", par 2.1. - 2.1.2. - 2.1.3. - 2.1.4. - 2.1.1.5.
Il Titolare del Trattamento, Gastaldo Holding S.p.A. nella persona del suo Legale rappresentante protempore, confrontatosi con il Consulente Privacy, ritiene che non sia necessaria la nomina del DPO.

Coordinamento Privacy: indica la struttura presso la Capogruppo che si interessa, interfacciandosi anche con il Consulente Privacy, delle attività di coordinamento organizzativo sulle tematiche della protezione dati personali, il tutto nell'ottica del mantenimento dell'impegno al rispetto dei principi privacy all'interno del Gruppo. L'obiettivo è la riduzione dell'esposizione al rischio privacy per l'intero Gruppo. Al Coordinamento Privacy possono essere chiamati a partecipare i referenti privacy delle varie società del Gruppo.

Referente/i Privacy: sono i soggetti che, all'interno delle singole Società Controllate, sono il principale referente di ciascuna società per le questioni relative alla conformità alla Normativa Privacy ed i cui compiti sono descritti al successivo paragrafo 2.4.6.2. Le Società del

GRUPPO GASTALDI possono, in considerazione della loro dimensione e/o della complessità dei trattamenti eseguiti, prevedere al proprio interno un'ulteriore articolazione organizzativa, delegando attività del Referente Privacy ad altri soggetti individuati nelle funzioni aziendali coinvolte nel trattamento (le "Funzioni"), ferme restando le responsabilità del Referente Privacy.

Persone autorizzate al Trattamento: ogni Utente che ha accesso a dati personali trattati dal GRUPPO GASTALDI i cui obblighi sono indicati nella presente Data Protection Policy e nelle ulteriori istruzioni collegate.

Amministratori di Sistema: sono particolari persone autorizzate al trattamento ad elevata professionalità deputate alla gestione e alla manutenzione di un sistema di elaborazione o di sue componenti come identificati nel provvedimento dell'Autorità di Controllo del 27 novembre 2008 come revisionata nel 2009 denominato "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", i cui compiti sono meglio indicati negli atti di nomina, ovvero nelle policy e procedure adottate dalle Società del GRUPPO GASTALDI in materia di trattamento dei dati personali.

Autorità di Controllo: indica, per l'Italia, il Garante per il trattamento dei dati personali. In generale, indica l'Autorità Nazionale preposta alla verifica del rispetto delle normative in tema di protezione dei dati personali.

Diritti degli interessati: ai sensi della normativa privacy nella sua interezza tutti gli interessati hanno alcuni diritti fondamentali che vanno rispettati senza alcuna deroga. Tali diritti sono riportati sugli articoli da 15 a 22 del GDPR:

- Diritto di accesso: L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali;
- Diritto di Rettifica: L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa;
- Diritto alla cancellazione (diritto all'obblio): 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;
- Diritto alla limitazione del trattamento: L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento in particolari casi citati dalla legge;
- Diritto di Portabilità: 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
- Diritto di opposizione: L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni;

- L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.
- L'interessato ha diritto di proporre reclamo all'autorità di controllo.

GRUPPO GASTALDI: indica l'insieme delle società controllate da GASTALDI Holding S.p.A.

Normativa Privacy: indica il Codice Privacy, il GDPR, nonché qualsiasi altra normativa sulla protezione dei dati personali applicabile al trattamento dei dati personali, già in vigore o che entrerà in vigore nel corso del termine di efficacia della presente Data Protection Policy, ivi compresi i provvedimenti, le linee guida e le opinioni del Garante per la protezione dei dati personali, del Gruppo di Lavoro di cui all'Art. 29 della Direttiva 95/46/EC, del Comitato Europeo per la Protezione dei Dati di cui all'articolo 63 e seguenti del GDPR e di ogni altra autorità competente.

2.4. REGOLE PER IL TRATTAMENTO DEI DATI PERSONALI

2.4.1. TRATTAMENTO DEL DATO PERSONALE

I dati personali possono essere trattati unicamente per le finalità indicate nell'Informativa Privacy consegnata all'Interessato. I dati personali devono essere trattati come di seguito indicato:

a) in modo lecito, corretto e trasparente;
b) raccolti e registrati per finalità determinate, esplicite e legittime, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali finalità;
c) adeguati, pertinenti, e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
d) esatti e, se necessario, aggiornati (si veda la Sezione 1, Paragrafo 2.4.4);
e) conservati in una forma che consenta l'identificazione dell'Interessato per un periodo di tempo non superiore a quello necessario alle finalità per i quali essi sono stati raccolti o successivamente trattati (si veda la Sezione 1, Paragrafo 2.4.7);
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche ed organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale.

2.4.1.1. Classificazione dei Dati Personali

I dati personali sono classificati ai sensi del GDPR nelle seguenti categorie:

1) **dati personali**: indica qualsiasi informazione riguardante una persona fisica identificata o identificabile (definito "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;
2) **categorie particolari di dati personali**: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché 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; e

3) **dati personali relativi alle condanne penali e ai reati** o a connesse misure di sicurezza.
4) **dati di profilazione, geolocalizzazione e comportamentali:** insieme di dati che collettivamente consentono di attuare 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;
5) **dati di autenticazione:** codici, password o PIN atti a consentire l'accesso fisico o logico a sistemi, applicazioni o locali e che si presume siano a conoscenza esclusivamente dell'Interessato.

2.4.1.2. Regole per il trattamento

I dati personali di cui al punto possono essere trattati solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'Interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) 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;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'Interessato o di un'altra persona fisica;
e) 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;
f) 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.

Inoltre, nel caso si trattasse di dati che appartengono a **categorie particolari di dati personali**, poiché l'art. 9 impone l'impossibilità di trattamento salvo particolari casi, ogni volta che il dato sia necessario per il trattamento, andranno specificate le eccezioni previste per il trattamento scegliendole opportunamente da quanto citato ai commi dell'art. 9 del GDPR. Tali eccezioni devono essere riportate per singolo trattamento.

Particolare attenzione va posta al trattamento dei **dati personali relativi alle condanne penali e ai reati** che deve avvenire soltanto sotto il controllo dell'autorità pubblica o nei casi specifici citati dall'art 2.octies del Codice Privacy.

Il Regolamento Privacy prevede che il soggetto i cui dati personali si riferiscono sia correttamente informato circa il trattamento dei suoi dati personali mediante l'Informativa Privacy e presti il proprio consenso libero, specifico, informato e inequivocabile ove i dati personali siano trattati per finalità diverse dall'esecuzione del contratto con l'Interessato.

2.4.2. INFORMATIVA PRIVACY

L'Interessato deve ricevere un'adeguata Informativa Privacy in merito al trattamento dei suoi dati personali.

Tale informativa deve essere resa disponibile ai sensi dell'articolo 13 del GDPR al momento in cui i dati personali vengono raccolti, qualora i dati personali siano raccolti direttamente dall'Interessato.

Al contrario, ove i dati personali siano ricevuti per il tramite di terzi, ai sensi dell'articolo 14 del GDPR, l'informativa deve essere fornita:

a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati,
b) nel caso in cui i dati personali siano destinati alla comunicazione con l'Interessato, al più tardi in occasione del primo contatto utile con l'Interessato, o
c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.

L'Informativa Privacy deve contenere le informazioni previste dalla legge, tra le quali:

- l'indicazione del soggetto titolare dei dati personali;
- l'esistenza o meno di un DPO;
- le modalità e finalità per cui il trattamento viene effettuato;
- le basi giuridiche collegate alle finalità;
- i termini di conservazione;
- le modalità di gestione dei diritti degli interessati;
- la possibilità di proporre reclamo all'Autorità di Controllo.

Ogni Società del Gruppo dovrà predisporre, tramite il proprio Referente Privacy, e far approvare al Consulente Privacy, le informative privacy da utilizzare, sulla base della tipologia di dati trattati e del loro trattamento.

L'aggiornamento delle informative è a carico del Referente Privacy competente che si consulterà con il Consulente Privacy per garantire la coerenza delle informative privacy adottate dalle Società del GRUPPO GASTALDI.

Non è possibile apportare alcuna modifica alle informative privacy adottate dalle Società del Gruppo senza una previa approvazione scritta da parte del Referente Privacy in qualità di rappresentante del Titolare e del Consulente Privacy.

2.4.3. CONSENSO DELL'INTERESSATO

Come regola generale, vista la complessità di gestire il consenso e la obbligatorietà di interrompere un trattamento che si basa sul consenso a semplice richiesta, occorre prestare particolare attenzione a raccogliere il consenso a meno che non sia possibile avere altre basi giuridiche per effettuare il trattamento.
Il consenso non è utilizzato nel caso di trattamento dei dati personali dei dipendenti -

Tuttavia, per particolari trattamenti per i quali non sia possibile utilizzare altre basi giuridiche si utilizzerà il consenso tenendo presente che:

- L'adozione di una decisione basata unicamente sul trattamento automatizzato di dati relativi alla salute, ivi inclusa la profilazione, ai fini della fornitura dei servizi contrattuali, richiede il **consenso esplicito e separato** dell'Interessato, fatti salvi casi particolari da valutare specificatamente di volta in volta.
- Il **consenso espresso** da parte dell'Interessato deve essere **documentato** in formato cartaceo, elettronico o tramite una registrazione e tracciato nei sistemi informatici, al fine di poter essere provato e per evitare trattamenti dei dati personali in violazione degli obblighi di cui al Regolamento Privacy;
- Ogni uso di consenso deve essere accuratamente vagliato e segnalato.

2.4.4. DIRITTI DELL'INTERESSATO

Tutte le società del Gruppo devono mettere a disposizione degli Interessati un indirizzo postale e un indirizzo e-mail attraverso i quali gli interessati possano esercitare i diritti previsti dal Capo III del GDPR.
La verifica dell'arrivo di messaggi nelle caselle e-mail e la ricezione della posta ordinaria devono essere assicurate da un presidio continuativo, così da garantire che ogni comunicazione venga inoltrata al Referente Privacy, al fine di assicurare il tempestivo riscontro all'Interessato.
Allo stesso modo, ove la richiesta dell'Interessato venga formulata ad un terzo che tratta i dati personali degli Interessati per conto di una qualunque delle Società del GRUPPO GASTALDI (e.g. un fornitore, un appaltatore), tali terzi dovranno darne immediata comunicazione al Referente Privacy competente e al Consulente Privacy, inviando una e-mail all'indirizzo appositamente creato e comunicato dalla Società all'atto della definizione dell'accordo sul trattamento dati personali o di altre parti della documentazione contrattuale che regola i rapporti con il terzo. In ogni rapporto contrattuale deve essere presente un esplicito punto che parli di trattamento dati personali.

In coordinamento con il Consulente Privacy, il Referente Privacy competente per la richiesta di esercizio dei diritti o un suo incaricato:

a) dovrà verificare l'identità dell'Interessato che ha formulato l'istanza confrontando i dati di cui alla richiesta con i dati già in possesso della Società interessata;
b) ove vengano riscontrate delle discrepanze o in presenza di legittimi dubbi sull'identità del richiedente, dovrà contattare l'Interessato tramite i contatti a disposizione richiedendo allo stesso di inviare una copia del proprio documento di identità;
c) accertata l'identità del richiedente, provvederà a:
    i. coordinarsi con le Funzioni aziendali di volta in volta competenti sulla base della richiesta (IT e/o altre) per poter identificare i dati oggetto della richiesta e garantire che la stessa sia evasa (e.g. in caso di richiesta di cancellazione) con riferimento a tutti i sistemi informatici ed i documenti della Società del Gruppo e dei propri fornitori e/o terzi; e
    ii. dare pronto riscontro al richiedente, in forma scritta, **entro e non oltre 1 mese dalla richiesta**;
d) ove la richiesta sia particolarmente complessa, provvederà:

i. **entro un mese** dalla richiesta a motivare l'eventuale proroga del termine di riscontro all'Interessato; e
ii. **entro due mesi** dalla comunicazione di proroga, fornire riscontro all'Interessato.

Non è possibile applicare alcun corrispettivo per dare seguito alle richieste degli Interessati ad eccezione del caso in cui:

1) la richiesta dell'Interessato sia manifestatamente infondata o eccessiva in ragione del carattere ripetitivo della stessa (tale valutazione dovrà essere effettuata dal Referente Privacy) oppure,
2) con riferimento al diritto di accesso, l'Interessato richieda delle copie aggiuntive rispetto a quelle fornite con la prima richiesta.

La risposta fornita all'Interessato non deve essere solo "intelligibile", ma anche concisa, trasparente e facilmente accessibile, e formulata con un linguaggio semplice e chiaro.

Si rinvia al successivo paragrafo 2.4.4.5 per le modalità di esercizio del diritto di portabilità.
Tutte le richieste di esercizio dei diritti dovranno essere annotate in un registro sotto la responsabilità del Referente Privacy.

2.4.4.1. Diritto di accesso dell'Interessato[1]

L'Interessato può richiedere la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, ottenere:

a) l'accesso ai dati personali;
b) l'accesso alle seguenti informazioni:
    1. le finalità del trattamento;
    2. le categorie di dati personali in questione;
    3. 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;
    4. quando possibile, il periodo di conservazione dei dati personali previsto, oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
    5. 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;
    6. il diritto di proporre reclamo a un'autorità di controllo;
    7. qualora i dati non siano raccolti presso l'Interessato, tutte le informazioni disponibili sulla loro origine;
    8. l'esistenza o meno di un processo decisionale automatizzato, compresa la profilazione, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'Interessato.

[1] Art. 15 del GDPR.

Qualora i dati personali siano trasferiti a un paese terzo o ad un'organizzazione internazionale, l'Interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'art. 46 del GDPR.

L'Interessato deve essere informato riguardo ai propri diritti, così come sanciti dagli artt. 13 e 14 del GDPR.

Il soggetto a cui i dati personali si riferiscono può, altresì, richiedere una copia dei dati trattati purché questo non violi i diritti e le libertà di altri Interessati.

2.4.4.2. Diritto di rettifica e di integrazione[2]

L'Interessato ha il diritto di ottenere la rettificazione dei dati personali inesatti o l'integrazione dei dati personali incompleti.

2.4.4.3. Diritto alla cancellazione[3]

L'Interessato ha il diritto di ottenere la cancellazione senza immotivato ritardo dei dati personali che lo riguardano ove:

a) i dati dell'Interessato non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
b) l'Interessato ha revocato il consenso su cui si basa il trattamento e non sussiste altra base giuridica per il trattamento;
c) l'Interessato si oppone al trattamento ai sensi dell'art. 21, par. 1, del GDPR e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'art. 21, par. 2 del GDPR (si veda il paragrafo 2.4.4.6);
d) i dati personali sono stati trattati illecitamente;
e) i dati personali devono essere cancellati per adempiere un obbligo legale;
f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione ai sensi dell'art. 8 del GDPR.

Sussistono circostanze in cui i dati dell'Interessato dovranno essere conservati per esigenze regolatorie.
In tal caso, di concerto con il Consulente Privacy, il Referente Privacy competente o un suo incaricato, collaboreranno con la Funzione aziendale di riferimento (IT e/o altre) al fine di garantire che i dati rimangano nella disponibilità delle Società del GRUPPO GASTALDI esclusivamente per i fini regolatori e resi disponibili esclusivamente alle Autorità preposte, adottando accorgimenti tecnici a ciò finalizzati.

2.4.4.4. Diritto di limitazione di trattamento[4]

L'Interessato può ottenere la limitazione del trattamento dei dati che lo riguardano ove:

a) l'Interessato contesti l'esattezza dei suoi dati personali; la limitazione si applica per il tempo strettamente necessario alla Società del GRUPPO GASTALDI interessata dalla richiesta per verificare la correttezza dei dati stessi;

[2] Art. 16 del GDPR.
[3] Art. 17 del GDPR.
[4] Art. 18 del GDPR.

b) ove, in presenza di un trattamento illecito, l'Interessato si opponga alla cancellazione dei dati personali, chiedendo che al posto della cancellazione sia disposta la limitazione del loro utilizzo;
c) ove il Titolare del trattamento non abbia più necessità o intenzione di conservare i dati, ma i dati siano necessari all'Interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
d) l'Interessato si sia opposto al trattamento ai sensi dell'art. 21, par. 1, del GDPR, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del Titolare rispetto a quelli dell'Interessato.

Al verificarsi di quanto sopra, la Società del Gruppo tratterà i dati personali dell'Interessato solo ai fini della conservazione secondo modalità definite dal Referente Privacy competente in collaborazione con il Consulente Privacy, e con la collaborazione della Funzione aziendale competente (IT e/o altra) in caso di trattamento effettuato con modalità informatiche.

La Società del GRUPPO GASTALDI, oltre alla conservazione, potrà, diversamente, trattare i dati dell'Interessato - in pendenza della limitazione del trattamento - unicamente quando:

i. l'Interessato abbia fornito il proprio consenso;
ii. per l'accertamento, l'esercizio o la difesa, in sede giudiziaria, di un diritto da parte della Società stessa che agisce come Titolare del trattamento;
iii. per garantire la tutela dei diritti di un terzo (persona fisica o giuridica);
iv. per rilevanti motivi di interesse pubblico.

Il diritto alla limitazione prevede che il dato personale sia "contrassegnato" in attesa di determinazioni ulteriori; pertanto, è opportuno che i Titolari prevedano nei propri sistemi informativi (elettronici o meno) misure idonee a tale scopo.

2.4.4.5. Diritto alla portabilità[5]

L'Interessato può richiedere alla società Titolare del trattamento di:

a) ottenere i dati personali che lo riguardano e
b) richiedere la trasmissione diretta di tali dati ad altro Titolare del trattamento

nel caso in cui:

i. il trattamento sia effettuato con mezzi automatizzati;
ii. il trattamento si basi sul consenso dell'interessato ai sensi dell'art. 6, par. 1, lettera a), o dell'art. 9, par. 2, lettera a), del GDPR o sull'esistenza di un contratto di cui l'interessato è parte ai sensi dell'art. 6, par. 1, lettera b) del GDPR; e
iii. i dati oggetto di portabilità siano stati forniti dall'Interessato (a titolo esemplificativo, si rileva che sono inclusi i dati che sono diventati oggetto di trattamento a seguito di attività svolte dal soggetto, quali la fruizione di un servizio o l'utilizzo di un dispositivo, e sempre che siano trattati attraverso

[5] Art. 20 del GDPR (C68).

strumenti automatizzati - sono quindi esclusi gli archivi e registri cartacei e, in generale, ogni dato trattato mediante intervento umano).

2.4.4.6. Diritto di opposizione[6]

L'Interessato ha il diritto di opporsi, in qualsiasi momento, al trattamento di dati personali che lo riguardano nel caso in cui lo stesso abbia a oggetto, tra gli altri:

a) finalità di marketing diretto, ivi inclusa la profilazione se connessa a tale marketing diretto;
b) finalità di ricerca storica o finalità statistiche.

Nelle circostanze sopra indicate, il Titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al Trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'Interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

2.4.4.7. Diritto a non subire decisioni unicamente basate su trattamenti automatizzati[7]

L'Interessato ha, infine, la possibilità di richiedere di non essere sottoposto a una decisione che sia basata unicamente su trattamenti automatizzati, ivi inclusa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona, ad eccezione del caso in cui:

a) è necessaria ai fini della conclusione o l'esecuzione di un contratto tra l'Interessato e il Titolare;
b) è autorizzata dalla normativa nazionale o europea cui è soggetto il Titolare del trattamento;
c) è basata sul consenso esplicito dell'interessato.

2.4.5. GESTIONE DEI DATI PERSONALI

I dati personali non possono essere comunicati a terzi – ivi incluse altre Società del Gruppo diverse dal relativo Titolare - salvo che l'Interessato sia stato correttamente informato circa la base giuridica utilizzata per permettere il trasferimento.
In tale caso si trovano tutti i soggetti che svolgono attività per conto del titolare (Responsabili del trattamento, ad esempio non esaustivo: responsabili della gestione/elaborazione delle buste paga, consulenti sul lavoro, consulenti direzionali, auditor, ma anche gestori di servizi in cloud, gestori delle piattaforme informatiche in uso.).
Di tali comunicazioni deve essere dato apposito risalto nelle informative.

In particolare, per tutti i dipendenti deve esistere una specifica voce che indichi che avviene un trasferimento dei dati sulla base del legittimo interesse della Società verso le altre società del Gruppo con particolare riferimento alla società capogruppo[8].

[6] Art. 21 del GDPR (C69, C70)
[7] Art. 22 del GDPR
[8] Inserimento nella informativa dei dipendenti e collaboratori nella sezione comunicazione dei dati personali.

In generale, salve le specifiche eccezioni previste dalla Normativa Privacy, i dati personali non possono essere trasferiti al di fuori dei paesi membri dello Spazio economico europeo, a meno che non siano stati sottoscritti con il soggetto che riceverà i dati specifici accordi che garantiscano un adeguato livello di protezione dei dati trattati anche fuori dal territorio dell'Unione Europea, come previsto dalla normativa italiana e comunitaria.

2.4.6. RUOLI PRIVACY

In conformità con quanto previsto dall'articolo 37(2) del GDPR, la società capo GRUPPO GASTALDI ha deciso di NON nominare un DPO ma avvalersi di un **Consulente Privacy esterno,** il quale funge da referente per tutti gli uffici privacy delle singole società, ove esistenti.
Il **Consulente Privacy** della Capogruppo e i Referenti Privacy di ogni società condividono una modalità di scambio delle informazioni per omogeneizzare il comportamento rispetto alle domande degli interessati e per determinare gli schemi privacy più opportuni da utilizzare in caso di particolari attività o particolari contratti con soggetti terzi.

In particolare, per garantire un presidio efficace sul corretto trattamento dei dati personali da parte del GRUPPO GASTALDI si prevede almeno la nomina di:

1) un **Consulente Privacy** per la capo GRUPPO GASTALDI;
2) un Referente Privacy per ciascuna Società del GRUPPO GASTALDI, questo collabora con il Consulente Privacy per le attività di coordinamento interno della singola società, in caso di Data breach si adopera in modo fattivo per fornire al consulente tutto il supporto necessario per la gestione del Data breach fungendo da collegamento tra consulente e azienda/reparto interessato.

Occorre inoltre ricordare che:

1) Il Titolare è la società nella sua interezza di persona giuridica anche se intesa come rappresentata dai dirigenti di vertice, ciascuno con le proprie responsabilità organizzative;
2) I responsabili del trattamento sono soggetti esterni (altre società interne o esterne al gruppo cui sono delegati particolari trattamenti) con cui è formalizzato un accordo sul trattamento dati personali ai sensi dell'art. 28 del GDPR;
3) ciascun dipendete o collaboratore è Persona autorizzata al Trattamento ai sensi dell'art. 29 del GDPR (rientrano in questa funzione privacy anche i dirigenti tutti);
    - Verrà posta specifica attenzione all'individuazione di particolari "autorizzati al trattamento" quali sono gli Amministratori di Sistema cioè le figure professionali incaricate della gestione e della manutenzione di un impianto di elaborazione o di sue componenti, che rientrano nelle fattispecie di cui al provvedimento del Garante del 27 novembre 2008 (pubblicato sulla Gazzetta Ufficiale n. 300 del 24 dicembre 2008) e sue successive modifiche ed integrazioni ("Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema") – Tenendo sempre presente che le misure di

sicurezza e controllo devono essere descritte, applicate e giudicate sufficienti dal Titolare.

Tutti i dipendenti e collaboratori dovranno tempestivamente e adeguatamente coinvolgere il Referente Privacy di riferimento in tutte le questioni riguardanti la protezione dei dati personali. Il Referente Privacy dovrà sempre coordinarsi con il Consulente Privacy se presente ed eventualmente con il Consulente Privacy di gruppo.

Le Società Controllate, sulla base della propria dimensione e complessità e delle caratteristiche dei trattamenti effettuati, possono prevedere una articolazione che preveda o no il DPO, in ogni caso devono esistere dei referenti privacy che prendono in carico l'intera attività di Protezione dei Dati Personali della società.

2.4.6.1. Compiti del Consulente Privacy della Capogruppo

Il Consulente Privacy, con la collaborazione dei Referente Privacy, dovrà:

a) predisporre le modifiche e i correttivi alla presente Data Protection Policy e alle altre procedure definite dal GRUPPO GASTALDI in materia di trattamento dei dati personali, anche al fine di preservare la coerenza delle policy e procedure in materia di trattamento dei dati personali da parte delle diverse Società del GRUPPO GASTALDI;
b) mantenere l'elenco dei Referenti privacy delle singole società del Gruppo;
c) supervisionare - tramite i Referenti Privacy - la conformità del GRUPPO GASTALDI alla Normativa Privacy;
d) coordinare e supervisionare, anche attraverso il tavolo collaborativo, l'attività dei Referenti Privacy;
e) informare e consigliare i Referenti Privacy in relazione ai loro obblighi ai sensi della Normativa Privacy;
f) monitorare le attività formative e informative verso i soggetti autorizzati al trattamento in relazione ai loro obblighi ai sensi della Normativa Privacy;
g) collaborare con i Referenti Privacy nella predisposizione delle informative, formule del consenso, nomine a responsabile del trattamento e su ogni altra questione rilevante concernente il trattamento dei dati personali, fermo restando che il **Consulente Privacy** e i **Referenti privacy** dovranno essere il principale contatto di ciascuna Società del Gruppo in relazione a questioni concernenti il trattamento dei dati personali;
h) procedere alle contestazioni interne delle violazioni della Normativa Privacy da parte dei soggetti che operano sotto l'autorità del Titolare, in collaborazione con il Referente Privacy della particolare Società del Gruppo e la rispettiva Funzione HR se presente;
i) verificare periodicamente la corretta tenuta da parte dei Referenti Privacy di:
    a. registro dei trattamenti,
    b. registro delle richieste degli interessati;
    c. registro degli eventi che possono diventare violazioni (data breach);
    d. registro dei *data breach*
    e. elenco dei responsabili del trattamento delle singole Società del Gruppo;
    f. ……

j) collaborare con i Referenti Privacy, ove si riveli necessario il suo coinvolgimento, nel rispondere alle richieste di esercizio dei diritti da parte degli Interessati e assicurarsi che siano evase tempestivamente;
k) verificare, periodicamente o se richiesto dai Referenti Privacy, i testi delle informative, delle formule di consenso
l) verificare la correttezza delle nomine a "Responsabile del Trattamento" già in essere sempre nel rispetto degli accordi contrattuali sottoscritti.
m) effettuare, audit diretti o tramite questionario per valutare l'affidabilità dei nuovi responsabili del trattamento individuati;
n) mantenere l'elenco delle Informative privacy in uso da parte di ciascuna società del Gruppo;
o) collaborare, con il supporto e per tramite dei Referenti Privacy, con le Funzioni aziendali delle Società del Gruppo competenti al fine di garantire l'osservanza dei principi di privacy *by design* e *by default*;
p) fornire la propria raccomandazione nell'ambito della valutazione d'impatto sulla protezione dei dati ("DPIA") di cui all'articolo 35 del GDPR, come prevista al successivo, Paragrafo 2.4.11, e sorvegliarne lo svolgimento;
q) cooperare con l'Autorità di Controllo e agire come punto di contatto dell'Autorità di Controllo su questioni relative al trattamento dei dati personali e, se del caso, su qualsiasi altra materia inclusa la consultazione preventiva di cui all'articolo 36 del GDPR;
r) svolgere le altre attività previste come di sua competenza dalla Normativa Privacy, ivi inclusa la presente Data Protection Policy e le altre procedure e policy interne sul trattamento dei dati personali.

Presso l'ufficio del Consulente Privacy di Gruppo saranno archiviate tutte le eventuali comunicazioni all'Autorità di Controllo competente relative a tutte le Società del Gruppo.

2.4.6.2. Compiti del Referente Privacy o Consulente Privacy delle controllate

I Referenti Privacy dovranno garantire il rispetto, da parte della singola Società del Gruppo che li ha individuati, delle prescrizioni della Normativa Privacy e delle policy emanate dal GRUPPO GASTALDI. I Referenti Privacy svolgeranno, inoltre, attività di collaborazione con il Consulente Privacy e, in particolare, dovranno:

a) informare e fornire consulenza alle società del GRUPPO GASTALDI di appartenenza e agli Utenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR nonché da altre disposizioni relative alla protezione dei dati personali;
b) predisporre le Informative, formule del consenso, nomine a responsabile del trattamento e ogni altra documentazione relativa al trattamento dei dati personali e assicurarsi che essa sia correttamente inserita nei processi e nei prodotti aziendali;
c) tenere:
    i. registro dei trattamenti,
    ii. registro delle richieste degli interessati;
    iii. registro degli eventi che possono diventare violazioni (data breach);
    iv. registro dei *data breach*
    v. elenco dei responsabili del trattamento delle singole Società;
    vi. …

d) mantenere un archivio storico delle versioni delle informative sul trattamento dati personali in uso e delle nomine a responsabile del trattamento;
e) sorvegliare sul rispetto della Normativa Privacy al fine di evitare eventuali violazioni e conseguenti rischi e responsabilità per le Società del Gruppo, anche favorendo la sensibilizzazione e la formazione del personale che partecipa al trattamento e alle connesse attività di controllo in merito alla rilevanza della conformità con gli obblighi in materia di trattamento dei dati personali;
f) predisporre, con l'ausilio delle appropriate Funzioni aziendali, la valutazione d'impatto sulla protezione dei dati ("DPIA") di cui alla presente Sezione 1, Paragrafo 2.4.111 e farne approvare il contenuto al Legale Rappresentante della Società;
g) collaborare con le Funzioni aziendali competenti al fine di garantire l'osservanza dei principi di privacy *by design* e *by default*;
h) coordinare la gestione delle eventuali politiche privacy specifiche e particolari delle singole aziende, fornendo, di concerto con il Consulente Privacy, le indicazioni su questioni relative al trattamento dei dati personali;
i) assicurarsi che vengano soddisfatti gli obblighi di reportistica circa le modalità di trattamento dei dati personali;
j) qualora vengano a conoscenza o sospettino che il comportamento degli incaricati della propria società non si conformi con gli obblighi a loro carico, raccogliere ulteriori informazioni e collaborare con il Consulente Privacy al fine di procedere alla contestazione della violazione nei confronti degli stessi;
k) sottoporre all'attenzione del Consulente Privacy e collaborare con lo stesso in relazione alle problematiche più rilevanti in materia di trattamento dei dati personali;
l) svolgere le altre attività previste come di loro competenza dalla presente Data Protection Policy e dalle altre procedure e policy interne sul trattamento dei dati personali.

Al fine di consentire al Consulente Privacy di Gruppo l'attività di controllo, i Referenti Privacy avranno inoltre la responsabilità di:

a) inviare al Consulente Privacy con cadenza almeno semestrale entro il 15 gennaio e il 15 luglio di ogni anno solare e in caso di emergenze (i.e. qualora si verifichi un data breach), un report redatto sulla base di modulo allegato, relativo alle modalità di trattamento dei dati personali;
b) effettuare, di concerto con il Consulente Privacy, controlli periodici, con cadenza almeno semestrale, presso le funzioni aziendali in cui lo riterranno opportuno, richiedendo copia della documentazione a supporto delle proprie attività di audit;
c) adottare, di concerto con il Consulente Privacy, le misure volte a correggere eventuali mancate conformità con la Normativa Privacy applicabile o i rischi di mancata conformità, sulla base delle informazioni contenute nei report, derivanti dagli audit o in altro modo acquisite;
d) effettuare le verifiche periodiche sugli amministratori di sistema. Nel caso di amministratori di sistema appartenenti ad altre società del gruppo il controllo deve essere effettuato dalla società di appartenenza.

Qualora siano riscontrate non conformità alla Normativa Privacy da parte delle Società del Gruppo o, in generale, nel trattamento dei dati personali effettuate all'interno di una delle società, il Consulente Privacy e i rispettivi Referenti Privacy competenti hanno l'obbligo

di attivare il tavolo di verifica che dovrà concludersi con apposita relazione che dovrà riportare il piano delle azioni effettuate per rendere conforme il trattamento. La relazione sarà definita relazione di accountability del trattamento dovrà essere posta all'attenzione del titolare della singola società e del gruppo.

Il Referente Privacy è competente per le questioni relative alla conformità con la Normativa Privacy di ciascuna Società del Gruppo. Qualora siano riscontrate violazioni della Normativa Privacy, è possibile contattare direttamente il Referente Privacy competente e il Consulente Privacy agli indirizzi appositamente comunicati.

2.4.6.3. Compiti del Team Privacy

Ciascuna Società può definire, sulla base della propria complessità organizzativa, delle categorie dei dati trattati, della numerosità degli interessati un Team Privacy di cui fa parte anche Responsabile IT locale.
Il Team Privacy Locale stesso può essere integrato nella sua composizione, in ragione delle esigenze e dell'articolazione privacy della Società del Gruppo coinvolta e, a seconda delle fattispecie e delle circostanze specifiche, anche dal Responsabile della Funzione aziendale competente in relazione alla questione da analizzare.
Alcuni membri del Team Privacy confluiscono nel Comitato Privacy di GRUPPO GASTALDI che è coordinato dal Consulente Privacy di Gruppo.

Il "Comitato Privacy" è formato dal referente Privacy di Gruppo dal Consulente Privacy e dal legale rappresentante della società interessata.

Il Comitato Privacy di Gruppo ha la responsabilità di analizzare fattispecie complesse non codificate nonché di valutare eventuali violazioni riguardanti il trattamento dei dati personali (e.g. data breach) in conformità con la procedura di data breach adottata in linea con il Modello standard.

2.4.6.4. Altri ruoli

Le **Persone autorizzate al Trattamento** sono tutti i dipendenti e collaboratori che hanno accesso a dati personali trattati dal GRUPPO GASTALDI che ricevono istruzioni dettagliate sulle modalità di trattamento dei dati personali.

Gli **Amministratori di Sistema** nominati dalle società sono le figure professionali incaricate della gestione e della manutenzione di un impianto di elaborazione o di sue componenti che rientrano nelle fattispecie di cui al provvedimento del Garante del 27 novembre 2008 (pubblicato sulla Gazzetta Ufficiale n. 300 del 24 dicembre 2008) e sue successive modifiche ed integrazioni ("Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema") e i cui compiti sono illustrati in un'apposita istruzione, predisposta da ciascuna Società secondo le sue peculiarità.

Ogni dipendente deve visionare l'elenco dei Referenti Privacy per l'individuazione del referente principale per le questioni in materia di privacy.

All'atto dell'assunzione o della sottoscrizione del contratto di collaborazione, ogni dipendente o collaboratore deve ricevere e accettare espressamente, oltre all'informativa che attesta le finalità del Trattamento dei propri dati personali, anche la presente Data Protection Policy, che è volta a informarlo degli obblighi a suo carico nel trattamento dei dati personali per conto delle società del GRUPPO GASTALDI, nonché eventuali integrazioni predisposte dalle singole Società controllate.
La sottoscrizione del contratto equivale ad autorizzazione al trattamento dei dati personali del proprio ruolo organizzativo secondo le istruzioni di dettaglio del titolare diretto.

È prevista un'attività di formazione degli Utenti rispetto agli obblighi previsti dal Regolamento Privacy e dalla presente Data Protection Policy per assicurare il rispetto della Normativa Privacy. Nello specifico, ciascun Utente dovrà effettuare i corsi in tema di privacy che saranno messi a disposizione dalla società.

É responsabilità di ogni dipendente svolgere periodicamente la formazione in tema di privacy resa disponibile dalle Società del Gruppo. La violazione di questo obbligo potrà dare luogo all'adozione di provvedimenti disciplinari.

Gli Utenti, in particolare, dovranno tempestivamente e adeguatamente coinvolgere il Referente Privacy in tutte le questioni riguardanti la protezione dei dati personali.

2.4.7. DATA BREACH

Chiunque rilevi un caso (anche solo sospetto) di eventi rilevanti sui dati personali ha l'obbligo di segnalazione al Referente Privacy di riferimento nel più breve tempo possibile, integrando la comunicazione con quanti più dettagli possibili sulla base del Modello di allegato alla procedura di gestione delle violazioni adottata in azienda.
Sarò compito del Referente Privacy della società attivarsi per comunicare al Consulente Privacy l'evento e attivare il comitato privacy affinché si possa, analizzare il dettaglio dell'evento ed eventualmente, dare seguito a tutte le indagini necessarie a stabilire se va fatta la notifica all'Autorità di Controllo (limite di tempo 72 ore dalla scoperta del potenziale breach) e, se necessario, all'Interessato.

Il Referente Privacy attiva immediatamente il Comitato Privacy e si attiva per completare la raccolta delle informazioni affinché il Comitato abbia quanti più elementi per valutare la gravità dell'evento.
Il Comitato Privacy decide se sia necessaria la comunicazione all'Autorità di Controllo e delega al Privacy Office della società, sotto la supervisione del Consulente Privacy di Gruppo, la stesura della segnalazione come previsto dal portale di comunicazione dell'Autorità di Controllo.
Sarà compito del Titolare (la società coinvolta) controfirmare la presentazione della segnalazione e verificare che l'iter sia completato nei tempi previsti dalla legislazione vigente.
Sarà compito del Consulente Privacy di Gruppo effettuare le verifiche necessarie affinché gli eventuali remediation plan di recupero siano attivati nei tempi previsti.

2.4.8. TEMPI DI CONSERVAZIONE

I dati personali devono essere trattati per il tempo strettamente necessario al fine di dare esecuzione alla finalità specifica indicata nell'Informativa Privacy, resa disponibile all'interessato cui i dati stessi si riferiscono, e indicato nell'Informativa stessa.

In relazione a ciascuna categoria di dati personali, le Società del GRUPPO GASTALDI valutano i termini di conservazione che segnalano sul documento "Linea guida sulla conservazione dei dati personali della società X". Alla scadenza del termine di conservazione, i dati sono cancellati e/o anonimizzati nelle modalità previste dall'applicazione software in uso.

Sarà compito del Referente Privacy redigere un documento di accountability che riporti tutti i tempi di conservazione e che deve confluire sul massimario di conservazione di gruppo e deve armonizzarsi fra le varie società. Il massimario potrà prevedere la anonimizzazione o la completa deindicizzazione al posto della cancellazione.

2.4.9. CONTRATTI: LINEE GUIDA PER LA REDAZIONE DI ACCORDI A RESPONSABILI DEL TRATTAMENTO

Ogni qualvolta un fornitore o, in generale, un soggetto esterno abbia accesso a dati personali trattati dalle Società del GRUPPO GASTALDI, sarà necessario procedere alla verifica dell'idoneità di tale soggetto a trattare dati personali per conto delle stesse in conformità con la Normativa Privacy applicabile, tramite controlli ulteriori eventualmente richiesti dal Referente Privacy di concerto con il Consulente Privacy.

Le modalità di verifica andranno inserite nella richiesta di offerta al soggetto esterno. Potranno essere valutate le conformità solo se specificate antecedentemente alla presentazione di una offerta formale del soggetto esterno.

L'accordo per il trattamento dati standardizzato dovrà essere personalizzato dalla funzione aziendale delegante e deve specificare i termini del trattamento trasferito al soggetto esterno.

La insufficienza di garanzie accettabili comporta l'impossibilità di affidare l'attività a quel particolare fornitore.
Se tale fornitore, pur non dando sufficienti caratteristiche sulla protezione dati personali, risulta unico per prestazioni tecniche e strategico per le attività di una delle società del GRUPPO GASTALDI occorrerà riunire il Comitato privacy per stabilire le modalità di effettuazione del trattamento attivando tutti i meccanismi di tutela degli interessati procedendo, se del caso ad una pseudonimizzazione, gestita direttamente dalla società.

Ove, invece, il fornitore (o il terzo) risulti in grado di prestare garanzie sufficienti, dal punto di vista tecnico ed organizzativo, circa il trattamento dei dati personali, il responsabile della Funzione aziendale competente a gestire il rapporto contrattuale dovrà procedere alla definizione dell'accordo su trattamento dati personali (nomina) in linea con lo standard definito all'interno del GRUPPO GASTALDI.

Alla firma dell'accordo il Referente Privacy aggiornerà il registro dei trattamenti e l'elenco dei responsabili del trattamento e notificherà l'avvenuta nomina al Consulente Privacy di Gruppo.
Una copia originale (se cartacea) o la lettera di nomina firmata elettronicamente dovrà, poi, essere conservata a cura della Società del Gruppo e messa a disposizione su richiesta del Referente Privacy competente e/o del Consulente Privacy.

Non è possibile stipulare nessun contratto o conferire alcun incarico che comporti il trattamento di dati personali per conto delle Società del GRUPPO GASTALDI senza la previa autorizzazione scritta del Referente Privacy competente e/o del Consulente Privacy nel caso in cui siano utilizzati dei modelli di nomina diversi dai modelli standard approvati dal medesimo Referente Privacy.

2.4.10. OSSERVANZA DEI PRINCIPI DI PRIVACY BY DESIGN E PRIVACY BY DEFAULT

Il Consulente Privacy / Referente Privacy della singola società, direttamente o tramite la struttura che lo supporta, dovrà monitorare il corretto trattamento dei dati personali, la loro esattezza, affidabilità e aggiornamento, sia in fase di acquisizione che durante il trattamento, all'interno della propria funzione e inviare, sulla base delle istruzioni fornite nella nomina o su richiesta, un report periodico al Consulente Privacy di Gruppo relativo alle modalità di trattamento dei dati personali all'interno della Società del Gruppo che lo ha nominato.

Ogni nuovo trattamento dei dati personali effettuato da uffici aziendali dovrà essere segnalato al Referente Privacy, che valuterà il coinvolgimento del Comitato privacy o del Consulente Privacy di Gruppo ai fini delle attività per la privacy *by design* di seguito indicate e/o dell'eventuale aggiornamento del registro delle attività di trattamento.

Qualora un Utente di una delle Società del Gruppo intenda compiere una nuova attività, sviluppare un nuovo prodotto o servizio o aggiornare un prodotto o servizio, che comporti il trattamento di dati personali, dovrà attenersi ai seguenti principi:

i) **Principio di privacy by design**. Qualsivoglia progetto o prodotto dovrà essere sviluppato tenendo in considerazione le problematiche in materia di protezione dei dati personali sin dalla progettazione in particolare a:
   a. Finalità del trattamento;
   b. Minimizzazione dei dati;
   c. Termini di conservazione;
   d. Cancellazione dei dati;
   e. Modalità del trattamento:
   f. Sviluppo software sicuro.

ii) Principio di privacy by default. Qualsivoglia progetto o prodotto dovrà garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento (questo con riferimento alla qualità dei dati raccolti, alla portata del trattamento, al periodo di conservazione e all'accessibilità).

A tal fine, il gestore del trattamento dovrà seguire quanto stabilito dalla procedura di gestione della privacy by design e privacy by default definita dalla società in linea con lo standard definito dal GRUPPO GASTALDI.

Non è possibile realizzare nuovi prodotti o servizi, *tool* o altra applicazione tecnica o funzionalità - rivolti sia ai clienti che ai dipendenti - che comportino il trattamento di dati personali, ivi compresi i relativi aggiornamenti, senza seguire le indicazioni di cui al presente paragrafo.

2.4.11. DATA PROTECTION IMPACT ASSESSMENT

Qualora il Referente Privacy della singola società, ritenga necessario che un trattamento sia eseguito solo dopo specifica Data Protection Impact Assessment (DPIA) ai sensi dell'articolo 35 del GDPR, il Referente Privacy darà mandato al responsabile del progetto relativo al prodotto/servizio dello sviluppo della DPIA. La DPIA dovrà vedere il coinvolgimento del Referente Privacy della singola società nelle modalità previste dalla normativa vigente.
La DPIA, vistata dal Referente Privacy della società, dovrà essere sottoposta al Consulente Privacy di gruppo per l'approvazione finale.

Occorre sempre ricordare che il Consulente Privacy:

i) valuterà se le misure adottate per minimizzare i rischi per i dati personali degli interessati sono adeguate, nel qual caso redigerà un verbale di corretta esecuzione della DPIA che sarà tenuto dal Consulente Privacy, mentre
ii) qualora valutasse che il trattamento presenta un rischio elevato in assenza di misure adottate per attenuare il rischio, procederà alla consultazione con l'Autorità di Controllo competente ai sensi dell'articolo 36 del GDPR.

I casi in cui una DPIA è necessaria comprendono, a mero titolo esemplificativo, e non esaustivo:

- lo svolgimento di attività di *scoring* e analisi dei comportamenti, inclusa la profilazione, in particolare con riferimento al rendimento professionale, alla situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti;
- l'adozione di decisioni basate su trattamenti automatizzati che producono effetti giuridici sull'Interessato o che possano incidere in modo significativo sullo stesso;
- il monitoraggio sistematico degli Interessati;
- il trattamento, su larga scala, di speciali categorie di dati personali di cui all'articolo 9 del GDPR e di dati relativi a condanne penali e reati ai sensi dell'articolo 10 del GDPR;
- più in generale, qualsivoglia trattamento su larga scala (determinato sulla base del numero degli interessati coinvolti, del volume di dati trattati, nonché della durata e dell'estensione geografica del trattamento);
- l'abbinamento o la combinazione di dati (ad esempio derivanti da differenti trattamenti effettuati per diverse finalità o da diverso titolare del trattamento);
- il trattamento di dati personali di persone fisiche vulnerabili, in particolare i minori;
- l'utilizzo innovativo o l'applicazione di nuove tecnologie (a mero titolo esemplificativo e non esaustivo l'utilizzo di sistemi che implichino il trattamento di impronte digitali o riconoscimento facciale);

- qualsivoglia altro trattamento che possa presentare, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, un rischio elevato per i diritti e le libertà delle persone fisiche.

È sufficiente che uno solo dei casi citati sia applicabile perché sia necessaria la DPIA.
In caso di dubbio, il Referente Privacy dovrà chiedere il parere del Consulente Privacy.

2.4.12. MONITORING E REPORTING

Il Consulente Privacy di gruppo effettua - con la collaborazione dei Referenti Privacy delle singole società - periodicamente e, comunque durante ogni anno solare, controlli sulle modalità del trattamento dei dati da parte delle singole Società del Gruppo, anche tramite la reportistica prevista dalla presente Data Protection Policy e, qualora considerato necessario, altre forme di controllo e/o di audit.

A seguito di tali controlli, il Consulente Privacy di Gruppo invierà, entro il 15 febbraio di ogni anno solare e in caso di emergenze (e.g. in caso di *data breach*), al Legale rappresentante di ciascuna Società del Gruppo per mezzo del Referente Privacy di gruppo, un report indicante, a titolo esemplificativo e non esaustivo:

- richieste o investigazioni dell'Autorità di Controllo competente;
- le eventuali inosservanze rilevate in materia di protezione dei dati personali ed i relativi correttivi, i rischi o problematiche rilevanti connesse al trattamento dei dati personali;
- i *Data Protection Impact Assessment* effettuati e quelli dallo stesso raccomandati tramite le proprie opinioni;
- nuovi progetti e la conformità degli stessi ai principi di *privacy by design* e *by default*.

Per le attività di controllo interno il Consulente Privacy di gruppo potrà procedere anche a controlli intersecati (cioè il Referente Privacy di una società potrà controllare le attività privacy effettuate da un'altra società del gruppo).
Ad ogni audit di controllo dovrà essere redatta un apposito rapporto che dovrà essere consegnato alla società auditata ed al Consulente Privacy di Gruppo.

Le raccomandazioni del Consulente Privacy inviate al Legale rappresentante di ciascuna Società del Gruppo a seguito della propria attività di controllo devono essere valutate dal Consiglio di Amministrazione della Società del Gruppo interessata e, se la Società decide di non conformarsi alle stesse, la decisione deve essere adeguatamente motivata e conservata nel verbale del relativo Consiglio di Amministrazione.

2.4.13. REGISTRO DEI TRATTAMENTI[9]

È necessario provvedere all'aggiornamento costante del registro delle attività di trattamento contenente almeno le seguenti informazioni:

a) il nome e i dati di contatto del Titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del Referente Privacy;
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali;

[9] Art. 30 del GDPR.

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e) i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, con indicazione del paese terzo o dell'organizzazione internazionale, e la documentazione delle garanzie adeguate;
f) i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.

Il registro dei trattamenti dovrà essere conservato sotto la responsabilità del Referente Privacy della singola società, che provvederà all'aggiornamento dello stesso non appena questo rilevi un cambiamento nelle informazioni ivi contenute o venga a conoscenza di un nuovo prodotto o servizio che implichi il trattamento di dati personali. Ogni aggiornamento del Registro deve essere comunicato al Consulente Privacy di Gruppo che manterrà l'elenco delle versioni valide.

A tal proposito, ove le singole Funzioni aziendali delle Società del Gruppo rilevino un cambiamento nel trattamento dei dati di loro competenza o introducano un nuovo prodotto o servizio, dovranno darne immediata comunicazione al Referente Privacy e, per iscritto, al Consulente Privacy affinché questi effettuino le opportune verifiche.

2.5. VALUTAZIONE DEI RISCHI

Ogni Società del Gruppo deve predisporre, sulla base della propria organizzazione, una valutazione dei rischi, opportunamente documentata, all'interno dei propri trattamenti/processo aziendale/sistema informatico.
La valutazione dei rischi dovrà essere portata all'analisi del Comitato Privacy e del Consulente Privacy di Gruppo per il tramite dei Referenti Privacy per essere annotata e per definire il rischio residuo con le caratteristiche di accettabilità.
Il rischio residuo dovrà sempre essere accettato formalmente dal singolo titolare con apposito documento di accountability.
Le attività sul rischio derivante da trattamenti svolti con l'IT dovranno essere effettuate dalla eventuale unica società che gestisce tutti i sistemi informativi.

2.6. MONITORAGGIO E CONTROLLO

Per ragioni organizzative e produttive e per la tutela del patrimonio aziendale, le Società del gruppo possono avere la necessità di controllare l'utilizzo dei propri sistemi IT.
Tale attività, definita ai sensi del legittimo interesse del titolare, non è tuttavia da considerarsi quale attività di monitoraggio del dipendente ed è condotta in conformità alla legge italiana in materia di diritti dei lavoratori e protezione dei dati personali.
Le ragioni per cui le Società del Gruppo potrebbero effettuare una attività di controllo includono:
a) identificare e prevenire qualsiasi accesso o comunicazione di informazioni non autorizzati,
b) assicurare conformità alle leggi e ai regolamenti anche interni,
c) prevenire e identificare attività criminale,

d) controllare i virus e altre minacce di codice malevolo,
e) assicurare la continuità del business,
f) ove vi sia un sospetto, investigare o identificare usi inappropriati,
g) ove vi sia un sospetto, investigare violazioni della presente o di altre policy specifiche della Società,
h) rispondere a un reclamo,
i) effettuare un'investigazione disciplinare o legale,
j) assistere nell'investigazione di presunto illecito.

Particolare rilevanza occorre porre alle attività di gestione dei sistemi informativi. Tale attività è concentrata in una società del Gruppo che la svolge per tutti gli altri. Tale attività va regolamentata con accordo specifico sul trattamento dati personali.

Il monitoraggio viene effettuato nei limiti di quanto permesso o richiesto dalla legge e in quanto necessario e giustificabile per gli scopi delle Società del Gruppo.

Le informazioni identificate durante il monitoraggio (comprese le informazioni personali) possono essere utilizzate e conservate per la durata di ogni procedimento investigativo, disciplinare, regolamentare o criminale e possono essere divulgate a terze parti quando necessario. Eventuali procedimenti disciplinari dovranno rispettare l'iter previsto dal Contratto Collettivo applicato.