Finlombarda

REGOLAMENTO SULLA PROTEZIONE DEI DATI PERSONALI AI SENSI DEL REGOLAMENTO (UE) 2016/679

DATA DI APPROVAZIONE DA PARTE DEL CONSIGLIO DI AMMINISTRAZIONE

22 MAGGIO 2018

Finlombarda

Cronologia delle revisioni

REVISIONE N.	RIF. SCHEDA DI VERIFICA	MOTIVO REVISIONE	DATA APPROV.NE	DATA DIFFUSIONE
0	06/2018		22/05/2018	25/05/2018

Indice

1 PREMESSA

Finlombarda S.p.A. (nel seguito anche "**Finlombarda**" o la "**Società**"), nell'ambito delle attività che svolge per adempiere ai suoi obblighi istituzionali, tratta i dati personali di differenti categorie di soggetti.

La Società tratta i dati personali con due differenti ruoli:

- in qualità di **Titolare del trattamento** (nel seguito anche il "**Titolare**"), definendo autonomamente le finalità e i mezzi tecnologici e organizzativi affinché i dati personali dei soggetti interessati siano adeguatamente protetti da perdita, distruzione, alterazione, diffusione, furto, appropriazione, o ogni altro evento che possa, in maniera accidentale o meno, ledere i diritti e le libertà dei soggetti interessati;
- in qualità di **Responsabile del trattamento** (nel seguito anche il "**Responsabile**") per conto di soggetti terzi, tratta i dati personali per conto del Titolare terzo, seguendo le sue istruzioni e mettendo in atto misure tecniche e organizzative adeguate di modo che i trattamenti soddisfino i requisiti normativi e garantiscano la tutela dei diritti degli interessati.

In entrambi i casi sopra descritti, i trattamenti dei dati personali (nel seguito anche "**Trattamenti**") si svolgono nel pieno rispetto della normativa vigente.

La Società si impegna ad adeguare i contenuti del presente documento (nel seguito anche il "**Regolamento**") all'evoluzione normativa in materia di protezione dei dati personali.

Finlombarda considera la tutela dei diritti e delle libertà delle persone un elemento imprescindibile e reputa la protezione dei dati personali una condizione essenziale da garantire nello svolgimento dei propri compiti istituzionali. Promuove a questo scopo ogni tipo di azione e iniziativa affinché i trattamenti siano svolti nelle condizioni di maggiore sicurezza possibile e nel rispetto dei principi di liceità, necessità e proporzionalità.

1.1 Scopo

Obiettivo del presente Regolamento è definire i principi che Finlombarda pone in essere per garantire la conformità al «Regolamento (UE) del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)» (nel seguito anche il "**Regolamento 2016/679**" o il "**RGPD**").

Ogni trattamento è preventivamente valutato affinché siano verificati i presupposti normativi che garantiscono il rispetto dei diritti dei soggetti interessati e perché sia certo che i trattamenti siano limitati e pertinenti rispetto alle loro finalità.

La Società mette a disposizione tutte le risorse necessarie per assicurare la conformità al Regolamento 2016/679 e garantisce il continuo aggiornamento conseguente alle più recenti evoluzioni tecnologiche.

1.2 Ambito di applicazione

Il presente Regolamento si applica a tutti i Trattamenti svolti dalla Società per le proprie finalità o per le finalità di un altro titolare del trattamento (p.e. Regione Lombardia).

Sono ricompresi nell'ambito del Regolamento tutti i Trattamenti di Finlombarda, siano essi svolti direttamente da personale interno (incaricati del trattamento), oppure svolti all'esterno del suo perimetro organizzativo, ossia da fornitori o *partner* che a vario titolo trattano dati personali (c.d. responsabili "esterni" del trattamento).

I destinatari del presente documento sono:

- Consiglio di Amministrazione;
- Titolare del trattamento;
- Direttore Generale;
- Responsabile del trattamento (qualora individuato);
- Responsabile della Protezione dei Dati (nel seguito anche il "**RPD**");
- Responsabile Coordinamento Privacy;
- Referenti Privacy;
- Incaricati del trattamento;
- tutti gli altri dipendenti della Società;
- soggetti esterni:
  a) collaboratori;
  b) fornitori;
  c) Finlombarda Gestioni SGR S.p.A.

1.3 Definizioni

Ove non diversamente specificato, i termini di seguito indicati hanno nel Regolamento il significato, al singolare o al plurale, loro attribuito nelle seguenti definizioni:

- **Archivio**: indica 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**: indica l'autorità pubblica indipendente istituita da uno Stato membro incaricata di sorvegliare l'applicazione del Regolamento 2016/679 al fine di tutelare i diritti e

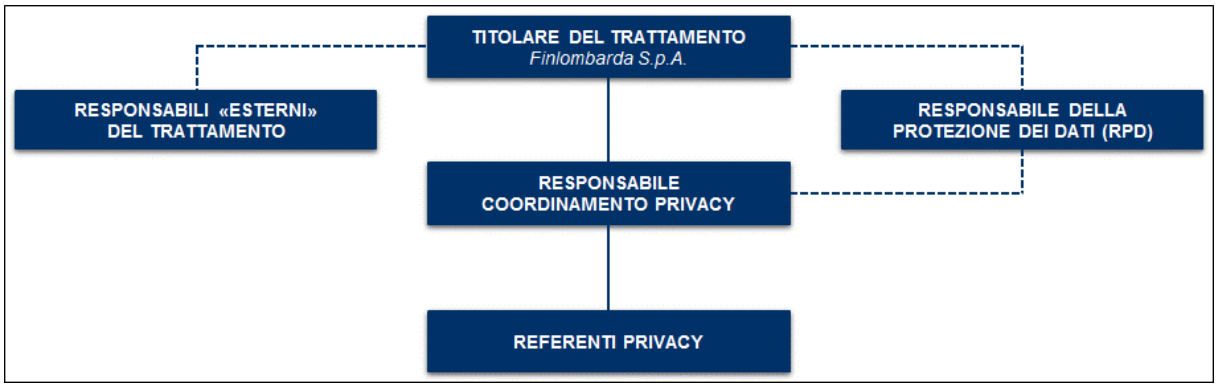
le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione. Per l'Italia si tratta del Garante per la protezione dei dati personali (www.garanteprivacy.it);

- **Consenso dell'interessato**: 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;
- **Dato personale**: indica qualsiasi informazione riguardante una persona fisica identificata o identificabile (cfr., di seguito, "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**: indica 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**: indica 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. Le autorità pubbliche che ricevono 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;
- **DPIA (*Data Protection Impact Assessment*)**: indica la valutazione d'impatto sulla protezione dei dati di cui all'art. 35 del Regolamento 2016/679, ossia la valutazione: (**a**) della necessità e proporzionalità dei trattamenti in relazione alle finalità, (**b**) dei rischi per i diritti e le libertà degli interessati e (**c**) delle misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento 2016/679, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione;
- **Fornitore**: indica qualsiasi soggetto, persona fisica o giuridica, che tratta dati personali per conto della Società in virtù di un contratto;

- **Incaricato del trattamento**: indica la persona fisica che, su specifica autorizzazione del Titolare o del Responsabile, effettua materialmente le operazioni di trattamento dei dati personali;
- **Interessato**: indica la persona fisica, identificata o identificabile, alla quale si riferiscono i dati personali trattati;
- **Pseudonimizzazione**: indica 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**: indica la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare;
- **RPD (Responsabile della Protezione dei Dati)**: indica la persona fisica o giuridica designata dal Titolare o dal Responsabile per assolvere alle funzioni di supporto e controllo, consultive, formative e informative relative all'applicazione del Regolamento 2016/679; coopera con l'Autorità di Controllo e costituisce il primo punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali;
- **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;
- **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;
- **Violazione dei dati personali**: 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.

1.4 Responsabilità

Finlombarda struttura la propria organizzazione in termini di risorse, processi e competenze per essere in grado di far fronte alle varie esigenze in tema di protezione dei dati personali, in particolare in relazione alle previsioni derivanti dal Regolamento 2016/679. L'organizzazione che la Società ha definito per raggiungere e mantenere la conformità al RGPD è la seguente:



Vengono di seguito riportate le principali responsabilità:

- **Consiglio di Amministrazione**
  a) approva, su proposta del Direttore Generale, la metodologia per la valutazione dei rischi privacy, la valutazione dei rischi privacy e i relativi presidi;
- **Titolare del trattamento** – è Finlombarda S.p.A., rappresentata dal Presidente del Consiglio di Amministrazione, in qualità di Legale Rappresentante. Nello specifico:
  a) è responsabile della conformità agli obblighi derivanti dal Regolamento 2016/679;
  b) decide in ordine alle finalità, alle modalità di trattamento dei dati personali e agli strumenti utilizzati, anche sotto il profilo della sicurezza del Trattamento;
  c) mette a disposizione mezzi, risorse e competenze per il raggiungimento degli obiettivi prefissati;
  d) coopera, su richiesta, con l'Autorità di Controllo nell'esecuzione dei suoi compiti;
  e) nomina il Responsabile della Protezione dei Dati, che può essere sia un soggetto interno che un soggetto esterno alla Società;
  f) nomina i responsabili del trattamento attraverso un contratto o altro atto giuridico a norma del diritto dell'Unione o degli Stati membri;
  g) nomina gli incaricati del trattamento;

h) dà indicazioni al Responsabile Coordinamento Privacy, ogniqualvolta vi siano variazioni in relazione ai Trattamenti effettuati dalla Società, di effettuare ulteriori valutazioni preliminari dei rischi privacy e la approva una volta che la stessa sia stata effettuata;
i) approva, previo parere del RPD, la valutazione di impatto sulla protezione dei dati (DPIA);
j) approva, previa verifica del RPD, i format documentali, compresi quelli di cui al successivo art. 2.1;
k) approva il registro delle attività di trattamento svolte dalla Società.

Le attività di cui alle precedenti lett. c), f), g) e j) possono essere delegate a dipendenti della Società.

- **Direttore Generale**
  a) nomina il Responsabile Coordinamento Privacy, che può essere sia un soggetto interno che un soggetto esterno alla Società;
  b) nomina i Referenti Privacy su richiesta del Responsabile Coordinamento Privacy e sentiti i responsabili delle relative unità organizzative aziendali;
  c) propone al Consiglio di Amministrazione l'approvazione della valutazione dei rischi privacy e dei relativi impatti;
  d) approva le procedure, comprese quelle di cui al successivo art. 2.1.
- **Responsabile della Protezione dei Dati** – esercita una funzione di indirizzo e controllo rispetto alla conformità delle procedure e degli atti societari al Regolamento 2016/679; nell'esecuzione dei propri compiti considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. Nello specifico:
  a) informa e fornisce consulenza al Titolare o al Responsabile, nonché ai dipendenti e collaboratori che eseguono il trattamento (c.d. "incaricati del trattamento"), in merito agli obblighi derivanti dal Regolamento 2016/679, nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
  b) sorveglia l'osservanza del Regolamento 2016/679, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare o del Responsabile in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
  c) fornisce un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e ne sorveglia lo svolgimento ai sensi dell'art. 35 del RGPD;

d) coopera e funge da punto di contatto per l'Autorità di Controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del RGPD, ed effettua, se del caso, consultazioni relativamente a qualunque altra questione.
e) supporta la corretta individuazione dei trattamenti dei dati personali;
f) verifica, preventivamente alla loro approvazione, i format documentali, compresi quelli di cui al successivo art. 2.1.

- **Responsabile Coordinamento Privacy** – è il soggetto al quale è affidata l'esecuzione delle attività per il raggiungimento degli obiettivi prefissati in materia di protezione dei dati personali e di conformità al Regolamento 2016/679. Nello specifico:
  a) coordina quanto necessario per la corretta esecuzione delle attività che la Società deve svolgere per la tutela dei diritti e delle libertà degli interessati;
  b) si interfaccia con il RPD sulle questioni interpretative della norma per garantire il corretto andamento delle attività previste in ordine al rispetto dei requisiti di conformità privacy;
  c) garantisce i flussi informativi verso il Titolare e le strutture coinvolte nel trattamento dei dati;
  d) aggiorna, con l'ausilio dei Referenti Privacy, il registro delle attività di trattamento;
  e) qualora necessario, svolge con il supporto della Direzione Amministrazione e Controllo, la valutazione di impatto sulla protezione dei dati (DPIA), confrontandosi con il RPD in merito agli aspetti metodologici, coinvolgendo le pertinenti unità organizzative aziendali per il tramite dei rispettivi Referenti Privacy ed, eventualmente, i fornitori;
  f) risponde, di concerto con il RPD, alle richieste degli interessati;
  g) supporta il RPD nella raccolta delle informazioni necessarie per gestire i rapporti con l'Autorità di controllo;
  h) si attiva, di concerto con il RPD, per garantire il monitoraggio dell'applicazione della norma nei confronti dei trattamenti svolti da Finlombarda o da soggetti terzi;
  i) richiede, qualora lo ritenga necessario, l'individuazione e la nomina dei Referenti Privacy al Direttore Generale;
  j) supporta la Funzione Risk Management e Antiriciclaggio nell'effettuare le ulteriori valutazioni preliminari dei rischi privacy anche avvalendosi dei Referenti Privacy;
  k) si raccorda con la Direzione Risorse e Organizzazione, Servizio Personale, nella definizione del fabbisogno formativo in relazione alle tematiche di cui al presente Regolamento.
- **Referenti Privacy** – sono le figure preposte al presidio della privacy all'interno delle unità organizzative aziendali di appartenenza. Nello specifico:

a) presidiano la tematica e gli adempimenti relativi alla privacy all'interno delle proprie unità organizzative, collaborando per quanto di competenza con il Responsabile Coordinamento Privacy nello svolgimento di tutte le attività a questo assegnate;
b) censiscono le attività gestite dalle proprie unità organizzative che implicano il trattamento di dati personali;
c) curano l'aggiornamento, in raccordo con il Responsabile Coordinamento Privacy, del registro delle attività di trattamento svolte dalla Società, per le parti di competenza delle proprie unità organizzative;
d) partecipano, se richiesti e con funzione consultiva, alla redazione delle *policy* e delle procedure aziendali relative alla privacy.

- **Incaricati del trattamento**
  a) effettuano materialmente il trattamento dei dati personali attenendosi alle istruzioni ricevute.
- **Fornitori (Responsabili "esterni" del trattamento)**
  a) in quanto responsabili del trattamento operano in conformità alle previsioni di cui all'art. 28 del RGPD.
- **Direzione Risorse e Organizzazione, Servizio Personale**
  a) definisce, in raccordo con il Responsabile Coordinamento Privacy, il fabbisogno formativo in relazione alle tematiche di cui al presente Regolamento, promuovendo azioni di sviluppo delle competenze.
- **Funzione Risk Management e Antiriciclaggio**
  a) identifica, misura e monitora il rischio operativo di privacy a cui è esposta la Società in collaborazione con le articolazioni societarie;
  b) effettua, su indicazione del Titolare e con il supporto del Responsabile Coordinamento Privacy, le ulteriori valutazioni dei rischi privacy;
  c) qualora svolta la DPIA ne inserisce i dati all'interno della mappatura dei rischi della Società.

1.4.1 Responsabilità in Finlombarda Gestioni SGR S.p.A.

Definisce autonomamente, tenendo in debita considerazione la propria complessità, l'organizzazione a presidio della corretta implementazione del Regolamento 2016/679, potendo altresì non procedere alla nomina del RPD laddove non vi sia espresso obbligo normativo ai sensi dell'art. 37, comma 1 del RGPD.

1.5 Riferimenti normativi

Il presente documento è redatto tenendo conto delle disposizioni contenute nelle seguenti fonti normative esterne ed interne:

- Statuto di Finlombarda;
- Sistema documentale aziendale di Finlombarda;
- Regolamento organizzativo di Finlombarda;
- Regole per la predisposizione dei documenti organizzativi di Finlombarda;
- Regolamento (UE) del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
- Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers ('DPOs')*, WP 243 rev.01, adopted on 13 December 2016, as last revised and adopted on 5 April 2017;
- Article 29 Data Protection Working Party, *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,* WP 248 rev.01, adopted on 4 April 2017, as last revised and adopted on 4 October 2017;
- Article 29 Data Protection Working Party, *Guidelines on Personal data breach notification under Regulation 2016/679,* WP 250 rev.01, adopted on 3 October 2017, as last revised and adopted on 6 February 2018.

2 LINEE GUIDA E CONTENUTO DEL REGOLAMENTO

2.1 Architettura documentale e processo di approvazione

Il presidio della normativa sulla privacy da parte della Società è garantito dal presente Regolamento e dalle seguenti tre procedure:

1. procedura di protezione dei dati fin dalla progettazione e di protezione per impostazione predefinita;
2. procedura di evasione richieste degli interessati;
3. procedura di notifica delle violazioni dei dati personali;

oltre a quelle che saranno emanate successivamente in applicazione della disciplina privacy tempo per tempo vigente.

Le suddette procedure sono approvate dal Direttore Generale.

La corretta valutazione dei rischi privacy è garantita, innanzitutto, da una valutazione in grado di censire tutti i Trattamenti effettuati da Finlombarda suscettibili, a norma dell'art. 35 del Regolamento 2016/679, di presentare un rischio elevato e dalla conseguente eventuale esigenza di svolgere una valutazione d'impatto sulla protezione dei dati (DPIA).

La valutazione dei rischi privacy e dei relativi impatti è svolta dalla Funzione Risk Management e Antiriciclaggio con il supporto del Responsabile Coordinamento Privacy ed è approvata dal Consiglio di Amministrazione.

Laddove la suddetta analisi evidenzi la presenza di un rischio elevato, si rende necessario procedere alla conseguente DPIA, a cura del Responsabile Coordinamento Privacy con il supporto della Direzione Amministrazione e Controllo, confrontandosi con il RPD in merito agli aspetti metodologici, coinvolgendo le pertinenti unità organizzative aziendali per il tramite dei rispettivi Referenti Privacy ed, eventualmente, i fornitori.

La DPIA è approvata dal Titolare, previo parere del RPD.

Completa il corredo documentale aziendale il registro delle attività di trattamento svolte dalla Società, predisposte dal Responsabile Coordinamento Privacy ed approvate dal Titolare.

Il Titolare, previa verifica del RPD, approva i seguenti format:

a) nomina a Responsabile "esterno" del trattamento dei dati;
b) clausola di riservatezza e protezione dei dati personali;
c) informativa relativa al trattamento dei dati personali del personale aziendale;
d) informativa relativa al trattamento dei dati personali relativi a gare di appalto;
e) nomina degli Incaricati del trattamento;

oltre a quelli che saranno predisposti successivamente in applicazione della disciplina privacy tempo per tempo vigente.

2.1.1 Indirizzi per Finlombarda Gestioni SGR S.p.A.

Finlombarda Gestioni SGR S.p.A. adotta il medesimo set documentale, ferma restando la sua piena autonomia nel definire il proprio processo deliberativo in coerenza allo specifico assetto di *governance*.

2.2 Principi applicativi

2.2.1 Titolare e responsabilizzazione

Al fine di soddisfare i requisiti previsti dal Regolamento 2016/679, Finlombarda definisce ed implementa una serie di processi sistemici per la protezione dei dati personali.

La Società, in qualità di Titolare, si impegna a far proprio un comportamento proattivo, attraverso il quale si venga a determinare e documentare, nella cornice dei criteri definiti all'interno del Regolamento, un sistema di controlli ed evidenze che dimostrino di aver posto in essere tutte le scelte idonee a garantire, nel pieno rispetto della vigente normativa, i diritti e le libertà personali dei soggetti interessati.

In funzione del livello di rischio rilevato, Finlombarda decide autonomamente il giusto livello di protezione e quindi le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel Regolamento stesso.

Nei casi in cui la Società agisce in veste di Responsabile del trattamento, esegue le attività sotto la direzione del Titolare del soggetto terzo e, comunque, nel rispetto di quanto previsto dall'art. 28 del Regolamento 2016/679.

2.2.2 Documentazione dei trattamenti

Finlombarda, ai sensi dell'art. 30 e del Considerando 82 del RGPD, redige e mantiene aggiornato un registro di tutte le attività di trattamento svolte sotto la propria responsabilità.

Tale registro, affidato al Responsabile Coordinamento Privacy, viene aggiornato ogni qualvolta intervengano modifiche alle modalità di trattamento, o qualora venga introdotta una nuova attività di trattamento di dati personali, ed è sempre disponibile per le attività ispettive che dovessero essere svolte dall'Autorità di Controllo o per fornire informazioni ai soggetti interessati in relazione all'esercizio dei loro diritti.

Il registro dei trattamenti contiene tutte le informazioni fondamentali di ogni trattamento, per poter valutare le condizioni entro le quali il trattamento stesso si svolge. Tali informazioni comprendono:

- 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 responsabile della protezione dei dati;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di Paesi terzi od organizzazioni internazionali;
- ove applicabile, i trasferimenti di dati personali verso un Paese terzo o un'organizzazione internazionale, compresa l'identificazione del Paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui all'art. 49, comma 2 del Regolamento 2016/679, la documentazione delle garanzie adeguate;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'art. 32, comma 1 del RGPD.

La Società ha sviluppato un modello di registro dei trattamenti esaustivo dal punto di vista delle informazioni e dei dettagli che lo compongono, convinta in questo modo di dare massima trasparenza alle sue attività di trattamento, agevolare le valutazioni di rischio e legittimare la conformità alla normativa vigente.

2.2.3 Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

Per attestare la conformità al Regolamento 2016/679, Finlombarda si impegna a configurare il trattamento dei dati personali definendo fin dall'inizio le garanzie indispensabili per tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

La Società assicura pertanto l'impegno al rafforzamento del presidio relativo alla valutazione dei rischi costituiti dal trattamento, in ottica di preventiva adozione di idonee soluzioni per la protezione dei dati personali, inclusa la valutazione che i dati trattati siano necessari, limitati e pertinenti rispetto alle finalità, adeguando in tal senso anche i processi di sviluppo delle soluzioni informatiche e individuando responsabilità organizzative relativamente a questi aspetti.

A tal fine, per il tramite del Responsabile Coordinamento Privacy, in stretto raccordo con il RPD, orienta le analisi sui trattamenti all'individuazione di soluzioni per la minimizzazione degli stessi, riducendo il più possibile i dati personali trattati, i tempi della loro conservazione negli archivi ed evitando gli accessi non strettamente necessari in relazione alle finalità.
Un'apposita procedura definisce le modalità con cui vengono applicati gli aspetti sopra citati.

2.2.4 Valutazione dei rischi privacy e dei relativi impatti

Finlombarda, nella piena consapevolezza che il principio di responsabilizzazione si esprime anche attraverso l'applicazione di una corretta metodologia per la valutazione dei rischi che i trattamenti svolti possono comportare nei confronti dei soggetti interessati, esegue, per il tramite del Responsabile Coordinamento Privacy, una DPIA in tutti i casi richiesti. Detta valutazione viene assicurata per tutti i nuovi trattamenti con rischio elevato per i diritti e le libertà delle persone fisiche e ha la finalità di determinare se procedere al trattamento o avviare, per il tramite del RPD, la consultazione preventiva dell'Autorità di Controllo per individuare le misure di protezione idonee per il livello di rischio.
Più in generale, la Società si attiene a quanto previsto dall'art. 32 del Regolamento 2016/679, ossia all'adozione per i trattamenti di misure tecniche o organizzative adeguate tenuto conto del rischio di varia probabilità e gravità per i diritti e le libertà dei soggetti interessati; il modello di miglioramento continuo prevede che tutti i trattamenti siano sottoposti a valutazioni di rischio per adeguare le misure di protezione applicate ai rischi valutati, anche tenuto conto dell'evoluzione tecnologica e del mutevole contesto delle minacce che possono impattare i trattamenti.
I risultati riscontrati durante la DPIA vengono forniti alla Funzione Risk Management e Antiriciclaggio che provvede a inserirli nella mappatura dei rischi della Società.

2.2.5 Liceità, consenso e informativa

Finlombarda assicura la conformità al RGPD attraverso il rispetto dei principii di liceità e trasparenza.
La Società garantisce che nessun trattamento possa avere inizio se non dopo la verifica del rispetto delle condizioni di liceità dello stesso.
I trattamenti di dati personali dei dipendenti prevedono sempre, come condizione di liceità, la raccolta di un consenso.
Per i trattamenti di dati personali di soggetti esterni a Finlombarda, la necessità di raccolta del consenso come condizione di liceità viene valutata di volta in volta, anche in considerazione delle previsioni di cui all'art. 6, comma 1, lett. e) del Regolamento 2016/679, secondo il quale

condizione sufficiente per la liceità del trattamento, anche in assenza di consenso, è l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare.

Il consenso può ritenersi validamente espresso quando è:

- verificabile l'identità dell'interessato;
- richiesta l'autorizzazione del genitore in caso l'interessato abbia età inferiore ad anni 16;
- fornita l'informativa prima della raccolta del consenso;
- registrato il consenso ottenuto in forma verbale o scritta;
- prestato in forma libera, comprensibile, chiara ed inequivocabile.

Affinché sia possibile conservarne opportuna traccia, il consenso è raccolto in forma scritta, quando possibile e opportuno, e collocato in archivi dedicati.

Finlombarda richiede un consenso aggiuntivo ed esplicito per il trattamento di particolari categorie di dati personali, quali le informazioni relative all'origine etnica, alle opinioni politiche, alle credenze religiose, allo stato genetico, allo stato di salute o all'orientamento sessuale.

Tutti gli interessati al trattamento possono in qualsiasi momento, in conformità con quanto previsto dalla normativa vigente, revocare il consenso al trattamento rilasciato.

La Società garantisce inoltre un'esaustiva informativa per ciascun trattamento di dati, consegnata o messa a disposizione degli interessati, nella quale sono descritte – ad esempio – le finalità del trattamento, la base giuridica che giustifica il trattamento, le categorie di destinatari, i diritti dei soggetti interessati (diritto di accesso, diritto di rettifica, diritto all'oblio, diritto di limitazione del trattamento, diritto di opposizione, diritto alla portabilità dei dati), il tempo di conservazione dei dati, i dati di contatto del Titolare e del RPD.

Ogni aggiornamento di tutta o di una parte dell'informativa rilasciata agli interessati viene comunicato o messo a disposizione degli stessi nella maniera più opportuna e quanto prima possibile.

2.2.6 Diritti degli interessati

Finlombarda, in qualità di Titolare, agevola l'esercizio dei diritti da parte degli interessati, adottando ogni misura tecnica e organizzativa a ciò idonea.

In qualità di Responsabile si impegna a collaborare con il Titolare ai fini dell'esercizio dei diritti degli interessati ai sensi dell'art. 28, comma 3, lett. e) del Regolamento 2016/679.

In particolare l'esercizio dei diritti può concernere:

- diritto di accesso;
- diritto di rettifica;

- diritto di cancellazione (“diritto all’oblio”);
- diritto di limitazione di trattamento;
- diritto alla portabilità dei dati;
- diritto di opposizione.

Un’apposita procedura definisce modalità e tempi per l’evasione delle richieste effettuate dagli interessati.

2.2.7 Sicurezza dei dati personali

La Società, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, 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, mette in atto misure tecniche e organizzative per garantire un adeguato livello di sicurezza dei dati personali trattati. Nel definire l’adeguato livello di sicurezza Finlombarda tiene conto in special modo dei rischi presentati dal trattamento che 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.

Le misure tecniche e organizzative comprendono, tra le altre e se del caso:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

2.2.8 Notifica delle violazioni

Finlombarda, in qualità di Titolare, si impegna, come richiesto dal Regolamento 2016/679 e con le modalità precisate all’interno di un’apposita procedura, a notificare all’interessato e all’Autorità di Controllo l’eventuale violazione di sicurezza. In particolare, il Titolare:

- si impegna a notificare all’Autorità di Controllo l’avvenuta violazione di dati personali, che possa determinare un rischio per i diritti e le libertà degli interessati, nei tempi previsti dal RGPD (72 ore), motivando un eventuale ritardo nella comunicazione;
- assicura la notifica agli interessati a cui si riferiscono i dati personali, qualora detta violazione costituisca un rischio particolarmente elevato per i diritti e le libertà delle persone fisiche

interessate, comunicandola non appena ragionevolmente possibile e senza ingiustificato ritardo.

Finlombarda si impegna inoltre a documentare qualsiasi violazione dei dati personali, comprese le circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Quando la Società agisce in veste di responsabile del trattamento è tenuta ad informare tempestivamente il titolare del trattamento delle violazioni occorse.

2.2.9 Cooperazione con le autorità competenti

Finlombarda assicura la conformità Regolamento 2016/679 anche attraverso la cooperazione con l'Autorità di Controllo.

Essa promuove in tutte le forme ad essa consentite la necessaria collaborazione, per il tramite del RPD, con la finalità di raggiungere i migliori livelli di conformità.

La Società garantisce all'Autorità di Controllo la disponibilità di tutta la documentazione relativa al proprio sistema di protezione dei dati personali, nonché l'accesso al registro dei trattamenti, agli *asset* informatici e cartacei nei quali risiedono i dati personali degli interessati, al registro degli incidenti. Quest'ultimo contiene le informazioni relative agli incidenti come, ad esempio, il tipo di evento occorso, la data in cui si è verificato, il suo impatto, le azioni intraprese per la sua risoluzione, etc.

2.2.10 Rapporti con i fornitori

Finlombarda, nella veste di titolare del trattamento può avvalersi di fornitori per il trattamento dei dati personali. In questo caso il Titolare nomina tali fornitori responsabili "esterni" del trattamento dei dati personali mediante un 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.

Ove il fornitore si avvalga di subfornitori per il trattamento dei dati personali, Finlombarda può decidere di nominare direttamente detti subfornitori quali responsabili "esterni" del trattamento, oppure di delegare il fornitore affinché questo proceda in proprio alla nomina dei suoi fornitori quali responsabili "esterni" del trattamento. In quest'ultimo caso la Società deve essere preventivamente informata per rilasciare la necessaria autorizzazione e il responsabile "esterno" del trattamento deve impegnarsi a:

- trasmettere alla società in subappalto le disposizioni di sicurezza predisposte da Finlombarda;

- comunicare a Finlombarda il Paese nel quale la società in subappalto svolge le sue mansioni.

In entrambe le circostanze, i fornitori devono ricevere puntuali istruzioni all'interno dell'atto di designazione a responsabili "esterni" del trattamento per lo svolgimento delle attività loro affidate che implicano il trattamento di dati personali.

Fra le clausole che impegnano i fornitori deve essere indicata quella di accettazione delle attività di controllo che potranno essere svolte da parte della Società per verificare il rispetto dei requisiti di conformità in materia di protezione dei dati personali.

Nel caso in cui Finlombarda tratti dati personali in qualità di responsabile "esterno" del trattamento, lo farà sulla base delle modalità e delle istruzioni ricevute dal titolare del trattamento. In questo caso è la Società ad essere nominata responsabile "esterno" del trattamento dal titolare del trattamento e da esso potrà quindi ricevere o meno la delega alla nomina degli eventuali subfornitori. Per tutto quanto consegue i rapporti con detti subfornitori quando Finlombarda agisce in veste di responsabile "esterno" del trattamento, valgono tutte le regole applicabili al caso in cui la Società agisca in veste di titolare del trattamento.

2.2.11 Formazione

Finlombarda è costantemente impegnata per assicurare che i principi del presente Regolamento siano applicati, costantemente verificati e che tutto il personale addetto che ha regolare o occasionale accesso ai dati personali, o che ha la responsabilità di sviluppare gli strumenti per trattare tali dati, sia adeguatamente istruito per rendere efficaci tali principi.

Al tal fine, la Direzione Risorse e Organizzazione, Servizio Personale, definisce il necessario fabbisogno formativo, promuovendo azioni di sviluppo delle competenze in raccordo con il Responsabile Coordinamento Privacy.

Lo sviluppo delle competenze può inoltre essere attuato anche attraverso strumenti di comunicazione e informazione al personale a cura del RPD.

2.2.12 Trasferimento di dati verso Paesi terzi e organismi internazionali

Finlombarda, in qualità di Titolare o Responsabile, monitora l'eventuale trasferimento dei dati personali al di fuori dall'Unione europea, effettuato direttamente o per il tramite di un proprio fornitore. In questi casi, ove applicabile, effettua tutti gli opportuni controlli per verificare che il Paese terzo in questione garantisca un livello di protezione dei dati adeguato.

Qualora il livello di protezione fornito dal Paese terzo non risulti sufficiente, la Società si impegna a considerare la presenza di garanzie e condizioni adeguate da parte dei soggetti a cui i dati sono trasferiti.
In tutti i casi in cui non è verificata l'affidabilità del Paese terzo o del soggetto al quale i dati sono trasferiti, il RPD richiederà all'Autorità di Controllo competente un'autorizzazione specifica al trasferimento.

2.2.13 Miglioramento continuo

Finlombarda implementa i processi citati in un'ottica di miglioramento continuo, monitorando costantemente la conformità al Regolamento 2016/679 e prevedendo, ove necessario, le azioni correttive necessarie per assicurare l'evoluzione del proprio sistema di gestione della protezione dei diritti personali e l'efficacia dei sistemi di controllo su di esso.

3 DISPOSIZIONI FINALI

Il presente documento è sottoposto all'approvazione del Consiglio di Amministrazione di Finlombarda.

Per quanto riguarda le modalità di stesura, approvazione e modifica del presente Regolamento si rimanda a quanto previsto dal documento organizzativo "*Regole per la predisposizione dei documenti aziendali*" di Finlombarda.