Politica aziendale per la protezione dei dati personali, al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche

Scopo del presente documento è quello di descrivere i principi generali di sicurezza ed obblighi di riservatezza delle informazioni e dei dati personali definiti dal Titolare del trattamento, o del Responsabile che '**Prime Servizi s.r.l.'** garantisce ed assicura a tutti i soggetti coinvolti nell'ambito del trattamento dei dati, al fine di sviluppare un efficiente e sicuro sistema di gestione delle procedure e dei processi per la sicurezza dei dati personali nel rispetto dei diritti e le libertà fondamentali delle persone, in ottemperanza al Regolamento Europeo 2016/679, d'ora in avanti GDPR.

---

1. Definizioni

Come stabilito dall'articolo n. 4 del Regolamento Europeo n. 2016/679, ai fini di questo disciplinare aziendale si intende per:

a) «**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può esser 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;

b) «**trattamento**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

c) «**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

d) «**profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

e) «**pseudonimizzazione**»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

f) «**archivio**»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

g) «**destinatario**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

h) «**terzo**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

i) «**consenso dell'interessato**»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

l) «**violazione dei dati personali**»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

m) «**dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

n) «**dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

o) «**dati relativi alla salute**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

A proposito delle tipologie di "dati" sopra indicate, si fa presente che il Regolamento europeo non utilizza la definizione "dati sensibili" per la quale, quanto meno sino all'emanazione della legge italiana di revisione del D.lgs. 196/20013, si fa espresso rinvio all'articolo n. 4 del vigente Codice della privacy (D.lgs. 196/2003): definizione che, quindi, al momento rimane nell'utilizzo e nel linguaggio corrente per la materia di cui si tratta. U.L.SS. n. 8 Berica UOC Affari Generali 11

p) «**autorità di controllo**»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del Regolamento UE;

Quelle sopra riportate, di cui si è data evidenza, rappresentano le "definizioni" su cui ha inciso maggiormente il nuovo Regolamento europeo: per le altre "definizioni" si fa espresso rinvio al testo dell'articolo n. 4 del Regolamento Europeo n. 2016/679.

---

2. Titolare e Responsabile del Trattamento, DPO

Il **Titolare del Trattamento** è '**Prime Servizi s.r.l.'** P.IVA / CF: 03499970402 con sede in Via Flaminia, 233/A - 47924 Rimini (Rimini) , Italia

---

3. PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI

Come stabilito dall'articolo n. 5 del Regolamento Europeo n. 2016/679, i dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («**liceità, correttezza e trasparenza**»);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1 del Regolamento UE, considerato incompatibile con le finalità iniziali («**limitazione della finalità**»);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («**minimizzazione dei dati**»). A tale proposito, il Regolamento UE ricalca i principi sostanziali di "**necessità, pertinenza, indispensabilità e non eccedenza**" (rispetto alle finalità del trattamento) contenuti negli articoli 4 e 11 del D.lgs. 196/2003.

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («**esattezza**»);

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del Regolamento UE, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («**limitazione della conservazione**»);

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

Come stabilito dal Regolamento UE, il Titolare del trattamento (**Prime Servizi s.r.l.**) è competente per il rispetto di quanto sin qui esposto ed è in grado di comprovarlo verso l'esterno (principio europeo dell'«**accountability**» o «r**esponsabilizzazione**»).

---

4. INFORMATIVA SUL TRATTAMENTO DEI DATI:

Come stabilito dall'articolo n. 13 del Regolamento Europeo n. 2016/679, in caso di raccolta presso l'interessato di dati che lo riguardano, il Titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:

a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;

b) i dati di contatto del Responsabile della protezione dei dati (D.P.O.);

c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;

d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f) del Regolamento UE, i legittimi interessi perseguiti dal titolare del trattamento o da terzi;

e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;

f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione, nei termini previsti dal Regolamento UE.

In aggiunta alle informazioni di cui sopra, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:

a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a) del Regolamento UE, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

d) il diritto di proporre reclamo a un'autorità di controllo;

e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;

f) l'eventuale esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4 del Regolamento UE, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

---

5. Diritti dell'interessato:

Gli interessati, come previsto dal Regolamento Europeo 679/2016, potranno esercitare i diritti sanciti dagli articoli da 15 al 21 ed, in particolare:

- **diritto di accesso** – articolo 15 GDPR: diritto di ottenere conferma che sia o meno in corso un trattamento di dati personali che La riguardano e, in tal caso, ottenere l'accesso ai Suoi dati personali, compresa una copia degli stessi.
- **diritto di rettifica** – articolo 16 GDPR: diritto di ottenere, senza ingiustificato ritardo, la rettifica dei dati personali inesatti che La riguardano e/o l'integrazione dei dati personali incompleti;
- **diritto alla cancellazione** (diritto all'oblio) – articolo 17 GDPR: diritto di ottenere, senza ingiustificato ritardo, la cancellazione dei dati personali che La riguardano.
- **diritto di limitazione di trattamento** – articolo 18 GDPR: diritto di ottenere la limitazione del trattamento, quando:

1. l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare per verificare l'esattezza di tali dati;
2. il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
3. i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
4. l'interessato si è opposto al trattamento ai sensi dell'art. 21 GDPR, nel periodo di attesa della verifica in merito all'eventuale prevalenza di motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

- **diritto alla portabilità dei dati** – articolo 20 GDPR: diritto di ricevere, in un formato strutturato, di uso comune e leggibile da un dispositivo automatico, i dati personali che La riguardano forniti al Titolare e il diritto di trasmetterli a un altro titolare senza impedimenti, qualora il trattamento si basi sul consenso e sia effettuato con mezzi automatizzati. Inoltre, il diritto di ottenere che i Suoi dati personali siano trasmessi direttamente dalla Banca ad altro titolare qualora ciò sia tecnicamente fattibile;
- **diritto di opposizione** – articolo 21 GDPR: diritto di opporsi, in qualsiasi momento per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che La riguardano basati sulla condizione di liceità del legittimo interesse o dell'esecuzione di un compito di interesse pubblico o dell'esercizio di pubblici poteri, compresa la profilazione, salvo che sussistano motivi legittimi per il Titolare di continuare il 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; potrà opporsi in qualsiasi momento al trattamento qualora i dati personali siano trattati per finalità di marketing diretto, compresa la profilazione, nella misura in cui sia connessa a tale marketing diretto;

I diritti di cui sopra potranno essere esercitati, nei confronti del Titolare, contattando i riferimenti sopra indicati.

L'esercizio dei Suoi diritti in qualità di interessato è gratuito ai sensi dell'articolo 12 GDPR. Tuttavia, nel caso di richieste manifestamente infondate o eccessive, anche per la loro ripetitività, il Titolare potrebbe addebitarle un contributo spese ragionevole, alla luce dei costi amministrativi sostenuti per gestire la Sua richiesta, o negare la soddisfazione della sua richiesta.

- **DIRITTO DI REVOCA:**

  revocare il consenso - in qualsiasi momento, con la stessa facilità con cui è stato fornito, senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca.

- **DIRITTO DI RECLAMO:**

  L'interessato ha il diritto di proporre reclamo all'Autorità Garante per la protezione dei dati personali, Piazza di Montecitorio n. 121, 00186, Roma (RM).

---

6. POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

Adempimenti e procedure applicate alle aziende clienti:

• La verifica dei dati che saranno oggetto di trattamento con identificazione delle varie tipologie di dati e delle categorie di appartenenza. La verifica della finalità di ogni trattamento e della base giuridica sul quale ciascuno di essi si fonda, anche al fine di rendere adeguata informativa ai soggetti interessati, come previsto dagli artt. 13 e 14 del GDPR;

• La predisposizione della/delle informative (o il suo aggiornamento) che deve essere fornita agli interessati nel rispetto di tutti gli elementi indicati agli artt. 13 e 14 del GDPR. In particolare gli interessati dovranno essere messi a conoscenza dei diritti che il Regolamento riconosce loro (diritto di accesso, diritto all'oblio, diritto di rettifica, diritto di limitazione e di opposizione al trattamento, diritto alla portabilità dei dati); le informative per i soggetti interessati ai trattamenti dati di cui il cliente è titolare del trattamento sono fornite dal cliente se nei software o servizi sviluppati o configurati è prevista la raccolta di dati;

• La predisposizione del registro delle attività di trattamento dei dati personali, qualora esso risulti necessario in base al disposto dell'art. 30 del GDPR, ossia nel caso in cui l'impresa o l'organizzazione che effettua il trattamento dei dati abbia più di 250 dipendenti. Tale registro dovrà essere redatto anche nel caso in cui l'impresa od organizzazione abbia meno di 250 dipendenti, ma ponga in essere un trattamento dei dati che presenta un potenziale rischio per i diritti e libertà degli interessati il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

• L'instaurazione di una procedura da adottare in caso di eventuali violazioni dei dati (c.d. Data Breach di cui agli articoli 33 e 34 del GDPR), ad esempio al verificarsi di una divulgazione (intenzionale o meno), della distruzione, della perdita, della modifica o dell'accesso non autorizzato ai dati personali oggetto di trattamento. Il GDPR prevede infatti degli specifici adempimenti nel caso in cui si verifichi una violazione di tal genere, a causa di un attacco informatico, di un accesso abusivo o di un incidente. In questi casi il GDPR impone, come previsto dall'art. 33, in capo al Titolare del trattamento l'obbligo di comunicare all'autorità di controllo l'avvenuta violazione entro 72 ore (o comunque senza ritardo). Nel caso in cui la violazione verificatasi faccia presumere che vi sia anche un elevato e attuale pericolo per i diritti e le libertà degli interessati, anche questi ultimi dovranno essere direttamente informati senza ritardo di quanto successo;

• All'art. 35 del GDPR, si configura, in capo al Titolare del trattamento (e con la possibilità di consultare il Responsabile della protezione dei dati se nominato), l'obbligo di procedere ad una valutazione d'impatto sulla protezione dei dati nel caso in cui un tipo di trattamento, anche in considerazione della natura, dell'oggetto, del contesto e delle finalità del trattamento stesso, presenti un rischio elevato per i diritti e le libertà delle persone fisiche. Si precisa che il GDPR non sancisce un vero e proprio obbligo di svolgimento della valutazione d'impatto, ma si ricorda che il Regolamento prevede un generale obbligo, in capo al Titolare del trattamento, di attuare le misure idonee al fine di gestire adeguatamente i rischi per i diritti e le libertà degli interessati che possono derivare dal trattamento dei loro dati. Sarà quindi opportuno procedere all'effettuazione della valutazione d'impatto anche quando sul Titolare non incombe l'obbligo normativo in tale senso.

• Agli articoli 37 – 38 e 39 viene introdotto un altro adempimento richiesto al Titolare del trattamento che consiste nella designazione del Responsabile della protezione dei dati definito altresì Data Protection Officer. Tale nomina, come previsto dall'art. 37 del GDPR, è obbligatoria soltanto in una serie di ipotesi, in particolare, nel caso in cui il trattamento dei dati sia effettuato da un'autorità pubblica o da un organismo pubblico (ad eccezione per le autorità giurisdizionali quando esercitano le loro funzioni); quando le attività principali svolte del titolare o del responsabile del trattamento consistono in operazioni che, per la loro natura, l'ambito di applicazione o le finalità, richiedono un monitoraggio regolare e sistematico degli interessati su larga scala;

e infine nel caso in cui le attività principali effettuate consistano nel trattamento, su larga scala, di dati sensibili o di dati relativi a condanne penali e a reati consistenti nell'illecito trattamento dei dati personali. Come suggerito anche dal Gruppo dei 29, l'organismo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato

membro che ha predisposto le Linee guida dettando regolare sulla nomina del Responsabile per la protezione dei dati personali, quando il Regolamento non impone specificamente la nomina di un DPO, questa figura potrà comunque essere designata dal titolare o dal responsabile del trattamento su base volontaria.

---

7. RESPONSABILITÀ DELLA POLITICA DI SICUREZZA DELLE INFORMAZIONI

Il "titolare del trattamento" e il "responsabile" sono responsabili del sistema di gestione sicura delle informazioni, in coerenza con l'evoluzione del contesto aziendale e di mercato, valutando eventuali azioni da intraprendere a fronte di eventi come:

· Evoluzioni significative del business;

· Nuove minacce rispetto a quelle considerate nell'attività di analisi del rischio;

· Significativi incidenti di sicurezza;

· Evoluzione del contesto normativo o legislativo in materia di trattamento sicuro delle informazioni;

Periodicamente o all'occorrenza dovrà essere svolto un riesame per la verifica dell'efficienza e dell'efficacia, nonché dell'adeguatezza delle misure tecniche/organizzative applicate, nel rispetto ed al fine ultimo della protezione dei dati, diritti e libertà fondamentali delle persone.

Data: 08/11/2018

FIRMA

Giulio D'Angelo
Amministratore della 'Peime Servizi s.r.l.'