COMPASS

SINTESI DELLA POLITICA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Sintesi della Politica in materia di protezione dei dati personali

Edizione marzo 2026

COMPASS

Indice

1 Premessa

1.1. Obiettivo del documento e contesto di riferimento

La presente politica (di seguito "Politica") è redatta in ottemperanza all'art. 24, comma 2, del Regolamento (UE) 2016/679 ("GDPR" o "Regolamento") 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.

La Politica definisce:

(i) i principi generali applicabili a Compass Banca S.p.A. (di seguito, "Compass"), in qualità di titolare del trattamento dei dati personali, ovvero quando agisce in qualità di responsabile o contitolare del trattamento, nonché i presìdi generali adottati per ottemperare a tali principi;

(ii) la declinazione dei principi e dei presidi applicabili alle Società Controllate, italiane ed estere, in materia di trattamento di dati personali;

(iii) le responsabilità e i compiti degli organi sociali e delle strutture aziendali di Compass relativamente alla *data protection*.

La Politica è entrata in vigore il 25 maggio 2018, è pubblicata nella intranet aziendale e uno stralcio della stessa, afferente ai principi generali sul trattamento dei dati personali, nella sezione privacy del sito istituzionale www.compass.it.

1.2. Contesto normativo di riferimento

Di seguito è riportata la principale normativa di riferimento. Si precisa che in caso di successivi aggiornamenti o di nuove regolamentazioni in materia, in attesa del recepimento nella normativa interna, si dovrà far riferimento alla Normativa di più recente emanazione rispetto a quella riportata nel presente paragrafo.

1.2.1. Normativa esterna

- Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GDPR);
- Decreto Legislativo 30 giugno 2003, n.196, recante il "Codice in materia di protezione dei dati personali".

1.3. Ambito di applicazione e destinatari

L'applicazione della disciplina al Gruppo avviene sulla base del seguente modello:

- tutte le Società Controllate italiane del Gruppo che effettuano trattamenti dei dati personali (es. di clienti, dipendenti, visitatori, fornitori) nell'Unione europea applicano integralmente il GDPR, unitamente alla normativa italiana in materia (cluster 1);
- le Società Controllate estere stabilite nell'Unione europea che trattano dati personali, quelle non stabilite nell'Unione che trattano i dati personali per l'offerta di beni o servizi (anche solo in parte) a persone fisiche nell'Unione o monitorando i loro comportamenti nell'Unione, devono applicare il GDPR, unitamente alla normativa locale di riferimento (cluster 2);

- le Società Controllate estere non rientranti nelle fattispecie precedenti, ove procedano al trattamento dei dati personali, rientrano nel cluster 3.

La Politica trova quindi applicazione integrale per il cluster 1 e, previo adeguamento alla normativa locale di riferimento, per il cluster 2. Con riferimento al cluster 3, identifica i principi cardine cui si ispira il Gruppo Mediobanca nella protezione dei dati personali e deve essere applicata, anche in tale circostanza, previo adeguamento alla normativa locale, secondo un principio di proporzionalità, con particolare riferimento ai principi e presidi descritti nel paragrafo 2.

Il presidio del rischio correlato al trattamento dei dati personali è assicurato:

- per il cluster 1, attraverso:

  (i) l'adozione dei presìdi generali contenuti nella presente Politica e

  (ii) la nomina del medesimo Data Protection Officer (da parte di ciascuna Società), facoltà concessa dall'articolo 37 del GDPR[1];

- per i cluster 2 e 3, attraverso il coordinamento tra il Data Protection Officer di Gruppo e il referente locale di Compliance, ovvero il Data Protection Officer della Società, ove nominato.

Compass è inserita nel cluster 1 e applica dunque integralmente la presente Politica.

2 Principi applicabili al trattamento dei dati personali e presidi generali

La Politica identifica i principali presìdi individuati da Compass per assicurare il rispetto dei principi generali contenuti nel GDPR, con particolare riguardo a (i) liceità del trattamento, (ii) diritti degli interessati; (iii) registro dei trattamenti e valutazione d'impatto sulla protezione dei dati; (iv) sicurezza dei trattamenti e (v) gestione delle violazioni dei dati personali (data breach).

Al riguardo Compass:

(i) adotta processi, strumenti e controlli idonei, che consentano il pieno rispetto dei principi generali sul trattamento dei dati personali;

(ii) garantisce adeguati flussi informativi da e verso gli organi sociali, le strutture di controllo e operative nonché verso l'Unità Group Data Protection della Capogruppo;

(iii) assicura, d'intesa con Group Human Capital, Organization and Change, lo svolgimento delle attività di formazione del personale in materia di protezione dei dati personali, al fine di garantire il rispetto della normativa applicabile da parte di chiunque ponga in essere attività di trattamento dei dati personali all'interno della struttura aziendale sotto l'autorità del titolare.

I trattamenti dei dati personali delle diverse categorie di interessati (es. clienti e dipendenti, visitatori, fornitori) svolti da Compass si fondano sui seguenti principi:

[1] Resta ferma la possibilità da parte di ciascuna Società, al ricorrere di determinate circostanze e d'intesa con la Capogruppo nel caso delle Controllate, di nominare un proprio Data Protection Officer.

- **liceità, correttezza e trasparenza**: i dati personali sono raccolti e trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- **limitazione della finalità**: i dati personali sono raccolti e trattati per finalità determinate, esplicite e legittime;
- **minimizzazione dei dati**: i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- **esattezza**: i dati personali sono mantenuti esatti ed aggiornati e sono adottate misure ragionevoli per cancellare o rettificare, tempestivamente, i dati inesatti o superati;
- **limitazione della conservazione (c.d. data retention)**: i dati personali sono conservati per un arco temporale non superiore al conseguimento delle finalità per cui sono stati raccolti;
- **integrità, disponibilità e riservatezza**: i dati personali sono trattati in modo da garantirne un'adeguata sicurezza, attraverso l'adozione di misure tecniche ed organizzative adeguate;
- **privacy by design e privacy by default**: gli aspetti relativi alla protezione dei dati personali sono considerati sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, al fine di mettere in atto misure tecniche e organizzative adeguate. Compass, per impostazione predefinita, tratta solo i dati personali necessari per ogni specifica finalità del trattamento;
- **responsabilizzazione (c.d. accountability)**: i trattamenti dei dati personali sono svolti secondo i principi che precedono e il loro rispetto è adeguatamente documentato.

L'adozione dei presidi di seguito riportati segue, con riferimento alle Società del Gruppo italiane ed estere, le logiche di applicazione descritte al paragrafo 3.

2.1. Liceità del trattamento

I trattamenti di dati personali all'interno di Compass sono condotti esclusivamente sulla base di una o più delle seguenti condizioni di liceità:

- esecuzione di un contratto di cui l'interessato è parte o esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- adempimento di un obbligo legale al quale è soggetta Compass;
- espressione del consenso da parte dell'interessato;
- perseguimento di un legittimo interesse di Compass 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.

2.1.1. Richiesta del consenso

Laddove il trattamento di dati personali si fondi sul consenso dell'interessato, la raccolta del consenso è effettuata tramite dichiarazione scritta ovvero, in casi particolari caratterizzati da minore rischiosità, in forma orale e documentata per iscritto. Qualora nel modulo utilizzato per la raccolta del consenso si trattino altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile, in forma comprensibile e facilmente accessibile, utilizzando un

linguaggio chiaro e semplice, in modo tale che la volontà dell'interessato sia liberamente espressa. Il consenso è revocabile in qualsiasi momento e la sua revoca non pregiudica la liceità del trattamento effettuato fino a quel momento.

2.1.2. Legittimo interesse

In alcuni casi, ad esempio per la difesa in giudizio di Compass, le procedure di Compass prevedono che il trattamento dei dati personali possa essere effettuato al fine di perseguire un suo legittimo interesse. In ottemperanza al principio di accountability, in tali casi, la normativa interna prevede che la valutazione circa il corretto bilanciamento tra gli interessi di Compass e i diritti e le libertà fondamentali dell'interessato sia adeguatamente documentata.

2.1.3. Trasferimento di dati al di fuori dello Spazio Economico Europeo

Il trasferimento di dati personali verso un paese terzo (non appartenente allo Spazio Economico Europeo) o un'organizzazione internazionale può aver luogo senza autorizzazioni specifiche solo se la Commissione europea ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale garantiscono un livello di protezione adeguato, sulla base di una serie di elementi (tra cui il rispetto dei diritti umani e delle libertà fondamentali, l'esistenza e l'effettivo funzionamento delle Autorità di controllo, gli impegni internazionali assunti in relazione alla protezione dei dati personali).

In mancanza di una decisione di adeguatezza[2], la Banca trasferisce i dati personali solo in presenza di una delle garanzie previste dal Titolo V del GDPR[3].

2.2. Diritti degli interessati

2.2.1. Informativa sul trattamento

In conformità ai principi applicabili al trattamento, la normativa interna prevede che ai soggetti interessati, all'atto della raccolta dei dati personali, vengano fornite chiare informazioni circa:

(i) l'identità e i dati di contatto di Compass e del Data Protection Officer[4];

(ii) le caratteristiche del trattamento (es. le finalità e la base giuridica dello stesso, il periodo di conservazione dei dati);

(iii) i diritti del soggetto interessato.

Qualora i dati non siano stati ottenuti presso l'interessato, l'informativa indica anche la fonte da cui hanno origine i dati personali e se si tratta di dati provenienti da fonti accessibili al pubblico.

[2] Le decisioni sinora adottate ai sensi della Direttiva 95/46/CE in materia di adeguatezza sono consultabili tramite questa link.
[3] Ad esempio, le clausole tipo per il trasferimento di dati personali verso paesi terzi adottate dalla Commissione europea (c.d. "*Standard Contractual Clauses*").
[4] Il Data Protection Officer – o Responsabile della protezione dei dati – costituisce un elemento chiave all'interno del sistema di governance dei dati e ad esso sono attribuiti dal GDPR compiti generali di facilitare e favorire l'osservanza della normativa attraverso strumenti di *accountability* e fungere da interfaccia tra i vari soggetti coinvolti (autorità di controllo, interessati e divisioni operative all'interno della struttura aziendale).

2.2.2. Diritti d'accesso, rettifica, cancellazione, portabilità e opposizione

La normativa interna assicura il rispetto dei principi applicabili al trattamento, prevedendo che ogni interessato abbia il diritto di ottenere:

(i) la conferma che siano o meno in corso attività di trattamento di suoi dati personali e informazioni sulle caratteristiche del trattamento (es. finalità, categorie di dati personali, destinatari della comunicazione dei dati, diritti dell'interessato);

(ii) la rettifica di dati personali inesatti che lo riguardano, nonché la loro integrazione qualora siano incompleti;

(iii) la cancellazione, se sussistono alcune fattispecie, ad esempio se i dati non sono più necessari rispetto alle finalità per le quali sono stati raccolti, se l'interessato ha revocato il consenso o ha esercitato il diritto di opposizione al trattamento, oppure se i dati personali sono stati trattati illecitamente;

(iv) la limitazione del trattamento, qualora si configurino alcune ipotesi, ad esempio in caso di contestazione dell'esattezza dei dati personali o quando il trattamento è illecito e l'interessato si oppone alla cancellazione chiedendo che ne sia limitato l'utilizzo;

(v) la portabilità dei dati oggetto del trattamento, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, qualora il trattamento si basi su un consenso legittimo e sia effettuato con mezzi automatizzati;

(vi) l'opposizione, quando, ad esempio il trattamento dei dati si fonda sul legittimo interesse, o con riferimento al trattamento dei dati per finalità di marketing diretto;

(vii) la revoca del consenso, con conseguente cessazione del trattamento dei dati fondato su tale condizione di liceità.

La normativa interna prevede che, a seguito di ciascuna richiesta, si debbano fornire agli interessati le informazioni necessarie in forma concisa, accessibile e usando un linguaggio semplice e chiaro, entro un mese (estendibile fino a due mesi, in casi di particolare complessità), anche in caso di eventuale diniego che viene motivato.

2.3. Registro dei trattamenti, rischi per i diritti e le libertà degli interessati e valutazione d'impatto

Compass ha predisposto e aggiorna periodicamente un "registro delle attività di trattamento" che tiene traccia dei trattamenti svolti in qualità di titolare, di responsabile o di contitolare del trattamento. Il registro, reso disponibile su richiesta all'Autorità di controllo, è tenuto in forma scritta tramite uno specifico applicativo gestionale.

Al fine di assicurare l'integrità, la disponibilità e la riservatezza dei dati personali, per ciascuna attività di trattamento identificata nel registro, vengono valutati i rischi per i diritti e le libertà degli interessati. Ove da tale valutazione emerga che il trattamento comporta un rischio elevato, la normativa interna deve prevedere lo svolgimento di una valutazione di impatto sulla protezione dei dati (Data Protection Impact Assessment "DPIA"), previa consultazione con il Data Protection Officer.

In particolare, la normativa interna prevede che, nel valutare la necessità di effettuare un DPIA su un determinato trattamento, si tenga conto dei criteri definiti nelle linee guida del Comitato

europeo per la protezione dei dati e nel documento del Garante per la protezione dei dati personali con l'elenco delle tipologie di trattamenti soggetti al requisito di un DPIA.

2.4. Sicurezza del trattamento

Per garantire un livello di sicurezza del trattamento dei dati adeguato al rischio, la normativa interna definisce le misure tecniche e organizzative, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi del trattamento e alla natura dei dati personali trattati, in accordo ai principi di privacy by design e privacy by default.

Queste misure possono comprendere:

- la pseudonimizzazione e la cifratura dei dati personali;
- quelle idonee ad assicurare la riservatezza e l'integrità dei sistemi e dei servizi di trattamento su base permanente;
- meccanismi di verifica e valutazione della loro efficacia.

Tenendo conto dei rischi presentati dal trattamento che derivano, in particolare, dalla distruzione, dalla perdita o dalla modifica non autorizzata di dati personali, la normativa interna definisce le misure tecniche e organizzative che possono garantire un adeguato livello di protezione dei dati personali di default e in via preventiva rispetto allo stesso trattamento dei dati personali.

2.5. Presidio dei responsabili del trattamento

Alla luce delle disposizioni in materia di protezione dei dati personali in merito alle garanzie che devono prestare i responsabili del trattamento, nonché del costante incremento degli attacchi informatici evidenziato ogni anno nelle relazioni annuali del Garante Privacy, Compass e, in generale, il Gruppo pone particolare attenzione alla protezione dei dati personali trattati dai propri fornitori.

La normativa interna prevede pertanto l'impiego esclusivo di fornitori responsabili del trattamento dei dati che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato.

A tal fine, è previsto che venga effettuata una verifica accurata di tali fornitori prima della sottoscrizione del contratto, con un processo che vede il coinvolgimento di più strutture della Banca con competenze specialistiche. Questa verifica non è un evento isolato, ma un processo continuo che viene ripetuto annualmente durante la durata del contratto. Inoltre, in circostanze particolari, vengono effettuate verifiche di conformità specifiche, anche tramite l'accesso alle strutture dei responsabili del trattamento.

Questo approccio proattivo e rigoroso alla protezione dei dati personali riduce i rischi, garantendone una gestione responsabile.

2.6. Gestione degli eventi di data breach

Laddove sia identificata una violazione di sicurezza, accidentale o illecita, che comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata dei dati personali compromettendone la riservatezza, la disponibilità o l'integrità, la normativa interna assicura,

previo coinvolgimento del Data Protection Officer, che la notifica all'Autorità di controllo avvenga entro 72 ore dal momento in cui sia stata ravvisata la violazione, qualora la violazione comporti un rischio per i diritti e le libertà delle persone fisiche coinvolte.

Tale notifica contiene:

- la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati;
- i dati di contatto del Data Protection Officer;
- le probabili conseguenze della violazione;
- le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e attenuarne i possibili effetti negativi.

Qualora la notifica non sia effettuata entro 72 ore, la normativa interna prevede di indicare i motivi del ritardo.

Nei casi in cui la violazione possa comportare elevati rischi per i diritti e le libertà dei soggetti interessati, la normativa interna prevede che – previa consultazione con il Data Protection Officer – sia fornita agli interessati informativa sulla violazione senza ingiustificato ritardo. Tale comunicazione non è necessaria qualora dovesse comportare uno sforzo sproporzionato oppure in presenza di misure tecniche e organizzative adeguate di protezione dei dati (es. la cifratura).

La normativa interna prevede che: (i) la comunicazione descriva in modo chiaro e comprensibile la violazione dei dati personali, le sue possibili conseguenze e le misure adottate o previste per mitigarne gli effetti negativi, includendo i dati di contatto del Data Protection Officer; (ii) ogni violazione, sospetta o accertata, sia adeguatamente registrata e documentata nel registro delle violazioni, in conformità al principio di accountability.

3 Modello organizzativo – ruoli e responsabilità

In coerenza con quanto previsto dalla normativa, di seguito sono riportati i ruoli e le responsabilità definite nell'ambito del modello di gestione dei dati personali di Compass, caratterizzato dalla presenza di un unico Data Protection Officer di Gruppo.

Il **Consiglio di Amministrazione** adotta la presente Politica e nomina il Data Protection Officer.

Il **Data Protection Officer**[5], comune a tutte le Società italiane del Gruppo, è designato da ciascuna di esse e rappresenta una figura chiave per favorire l'osservanza della normativa in materia di protezione dati.

Il Data Protection Officer viene preventivamente e adeguatamente coinvolto da Compass in tutte le questioni riguardanti la protezione dei dati personali, anche con riferimento ad attività di interlocuzione con Autorità e interessati, al fine di supportare la Società in tutti gli adempimenti privacy.

Svolgendo il ruolo di interfaccia esterna, fra tutti i soggetti coinvolti dal trattamento (interessati e Autorità di controllo) e interna (vertici aziendali, diverse aree operative della Banca e addetti autorizzati al trattamento dei dati), il Data Protection Officer svolge le seguenti attività per Compass e per le Società Controllate italiane del Gruppo, assicurando il coordinamento delle omologhe strutture per le Società estere del Gruppo:

- analizza, gestisce e cura, le attività a presidio della normativa in materia di protezione dei dati personali, attraverso gli strumenti di accountability, supportando le valutazioni in materia di privacy;
- fornisce consulenza ai vertici e alle altre funzioni aziendali in merito agli obblighi derivanti dalla normativa in materia di protezione dei dati personali;
- sorveglia l'osservanza delle norme in materia di protezione dei dati personali;
- redige pareri in merito alla valutazione di impatto sulla protezione dei dati personali e supervisiona il corretto svolgimento della stessa;
- coopera con l'Autorità di controllo e le altre parti interessate;
- svolge centralmente le attività di formazione nei confronti dei dipendenti delle Società italiane del Gruppo;
- predispone gli strumenti informativi, quali una newsletter periodica con gli aggiornamenti in materia di protezione dei dati personali;
- viene coinvolto nella gestione dei reclami più critici, per definire il riscontro da fornire;
- predispone i template e gli standard relativi alla normativa interna, ai contratti e agli altri documenti di riferimento, che vengono inviati alle Società italiane del Gruppo, che li recepiscono e adottano;

[5] Il Gruppo Mediobanca, coerentemente con quanto previsto dal GDPR, ha identificato la necessità, per le Società Controllate italiane, di dotarsi della figura di Data Protection Officer in quanto le attività di trattamento svolte possono comportare il monitoraggio regolare e sistematico degli interessati su larga scala. Le valutazioni condotte da Mediobanca circa la necessità di dotarsi di un Responsabile della protezione dei dati sono riportate nell'Allegato 1.

- definisce il piano dei controlli, che viene messo a disposizione delle Controllate italiane del Gruppo per essere adottato tenendo conto delle rispettive specificità, previa condivisione con il Data Protection Officer;

- conduce i controlli e supporta le Controllate italiane del Gruppo nello svolgimento degli stessi, verificando, in concreto, che il trattamento dei dati avvenga sempre nel pieno rispetto della disciplina e delle istruzioni fornite a tutti i soggetti coinvolti;

- esamina le schede dei controlli svolti dalle Controllate italiane del Gruppo per un confronto sulle eventuali criticità riscontrate;

- predispone le relazioni annuali delle attività svolte per ogni Società Controllata italiana del Gruppo.

In un'ottica di gestione strutturata, sono previsti flussi informativi periodici e ad evento tra le Controllate italiane e il Data Protection Officer, e viceversa.

Il Data Protection Officer, secondo quanto previsto dalla vigente disciplina:

(i) possiede un'approfondita conoscenza della normativa e delle prassi in materia di protezione dei dati personali, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento;

(ii) agisce in piena indipendenza, in conformità al considerando 97 del GDPR, e autonomia, senza ricevere istruzioni e riferendo direttamente ai vertici aziendali e

(iii) dispone di risorse (personale, locali, attrezzature, ecc.) necessarie per l'espletamento dei propri compiti.

I dati di contatto del Data Protection Officer sono pubblicati nella sezione privacy del sito istituzionale www.compass.it. Al momento della designazione, il suo nominativo e i suoi dati di contatto sono comunicati al Garante per la protezione dei dati personali attraverso la procedura online. Eventuali revoche o variazioni sono comunicate seguendo le medesime modalità.

L'unità **Group Data Protection** è la struttura che, a diretto riporto del Data Protection Officer, lo supporta nello svolgimento delle attività sopra descritte.

L'unità **Group Human Capital, Organization and Change** è responsabile, di concerto con l'unità Group Data Protection, della predisposizione e della verifica dei piani di formazione per garantire il costante aggiornamento del personale.

L'unità **Cyber Security, Resilience & IT Regulation** di Capogruppo supporta il Data Protection Officer nell'individuazione delle misure di sicurezza più idonee e opportune al fine di assicurare la conformità alla normativa vigente da adottare.

La Funzione Compliance di Compass è responsabile della predisposizione e della diffusione della normativa interna in materia di protezione dei dati personali, tra cui quelle indicate nella sezione privacy del sito istituzionale www.compass.it.

Tutti i **dipendenti** sono nominati addetti autorizzati al trattamento dei dati personali ai sensi dell'articolo 29 del GDPR e sono responsabili della corretta gestione dei dati personali trattati e del rispetto delle disposizioni della Politica e della normativa interna in materia.

Da ultimo si segnala che, in conformità all'articolo 28 del GDPR, Compass può avvalersi di soggetti terzi che possono svolgere trattamenti per suo conto, designati responsabili del trattamento. Tali soggetti sottoscrivono un contratto specifico con Compass (nomina a responsabile del trattamento) e presentano garanzie adeguate circa il rispetto degli obblighi normativi e la protezione dei dati personali trattati, garanzie che vengono verificate alla stipula e periodicamente nel corso del rapporto da Compass. I responsabili del trattamento possono poi avvalersi di sub-responsabili del trattamento, previo ottenimento di specifica autorizzazione da parte di Compass. Qualora Compass, invece, determini congiuntamente con uno o più titolari le finalità e i mezzi del trattamento, le parti sono da considerarsi contitolari del trattamento. In tali casi, mediante uno specifico accordo tra le parti, redatto in conformità all'articolo 26 del GDPR, sono definiti i rispettivi ambiti di responsabilità, con particolare riguardo all'adozione di adeguate misure tecniche ed organizzative a protezione dei dati personali ed all'esercizio dei diritti degli interessati.

Allegato 1 – Principali definizioni

Addetti autorizzati al trattamento dei dati personali	Chiunque agisca sotto l'autorità e le istruzioni del titolare o del responsabile del trattamento, che abbia accesso ai dati personali.
Dati personali	Qualsiasi informazione riguardante una persona fisica identificata o identificabile ("**interessato**"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. A titolo esemplificativo e non esaustivo: Dati anagrafici (es. nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale); Dati di contatto (es. indirizzo postale o di posta elettronica, numero di telefono fisso o mobile); Dati di identificazione (es. NDG, username, customer ID); Dati di profilazione (es. abitudini di acquisto di prodotti o servizi); Dati relativi a documenti di identificazione/riconoscimento (es. carta di identità, passaporto, patente, CNS); Dati relativi alle immagini (es. fotografie, registrazioni, videoregistrazioni).
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.
Titolare del trattamento	La persona fisica o giuridica, l'autorità pubblica o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento.
Contitolare del trattamento	La persona fisica o giuridica che determina congiuntamente ad uno o più titolari le finalità e i mezzi del trattamento.
Responsabile del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Sub-responsabile del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto di un responsabile del trattamento.