

POLICY SULLA PROTEZIONE DEI DATI PERSONALI

CON ALLEGATO N. 1

Approvata dal Consiglio di Amministrazione nella seduta del 27 giugno 2019

Aggiornamenti:

1° Aggiornamento del-----



INDICE

1. PREMESSA

- 1.1 Obiettivi del documento
- 1.2. Ambito di applicazione
- 1.3 Riferimenti normativi principali
- 1.4 Aggiornamento/revisione del documento

2 Principi e presidi generali sul trattamento di dati personali

- 2.1 Liceità del trattamento
 - 2.1.1 Richiesta del consenso
 - 2.1.2 Legittimo interesse
 - 2.1.3 Trasferimento dei dati all'estero

2.2 Diritti degli interessati

- 2.2.1 Informativa sul trattamento
- 2.2.2 Diritti d'accesso, rettifica, cancellazione, portabilità e opposizione
- 2.3 Registro dei trattamenti, analisi dei rischi, valutazione d'impatto e consultazione preventiva
- 2.4 Sicurezza del trattamento
- 2.5 Gestione degli eventi di data breach

3 Ruoli e Responsabilità

- 3.1 Consiglio di Amministrazione
- 3.2 Delegati interni al trattamento dei dati
- 3.3 Data Protection Officer
- 3.4 Responsabili/ Sub-Responsabili del trattamento dei dati
- 3.5 Incaricati del trattamento dei dati

4. Disciplina e modello di GRUPPO - Osservanza

5 Modelli di nomina

- 5.1 Incaricati del trattamento
- 5.2 Responsabili/ Sub responsabili del Trattamento

6. Interventi formativi per gli Incaricati del trattamento

Allegato 1

Principali definizioni



1. PREMESSA

1. BPP Service S.p.a., società facente parte del Gruppo Bancario Banca Popolare Pugliese, (nel prosieguo “Società”), in qualità di Titolare del trattamento nell’esecuzione delle proprie attività, effettua trattamenti di Dati comuni, particolari e giudiziari per dipendenti, mandatari, procuratori, clienti (anche minori) e fornitori ed è pertanto sottoposta alla normativa in materia di protezione dei dati personali.

La Società opera altresì quale Responsabile del trattamento dei dati forniti dalla Committente capogruppo Banca Popolare Pugliese Soc. Coop. Per Azioni, titolare del trattamento, per l’espletamento delle attività aziendali, consistenti in:

- recupero crediti, strettamente limitata al sollecito telefonico effettuato da suoi dipendenti autorizzati e al sollecito domiciliare per mezzo di mandatari esterni, munita di licenza di cui all’art. 115 TULPS (Testo Unico Leggi di Pubblica Sicurezza)
- acquisizione di immobili o diritti reali immobiliari, nell’ambito o al di fuori di procedure esecutive o concorsuali o giudiziarie in genere, dietro segnalazione delle Capogruppo e successiva vendita degli stessi.

Anche nell’ambito delle attività di cui sopra, la Società è Titolare:

- dei trattamenti di dati personali e particolari connessi all’adempimento di qualsiasi obbligo di legge;
- dei trattamenti di dati ulteriori, rispetto a quelli in relazione ai quali è Responsabile, acquisiti nel corso dello svolgimento delle attività da essa effettuate;
- dei trattamenti connessi alle attività di controllo o miglioramento della qualità del servizio.
-

1.1. Obiettivi del documento

La Società, nell’esecuzione delle proprie attività, effettua trattamenti di Dati comuni, particolari, e giudiziari per dipendenti, clienti (anche minori) e fornitori nonché, limitatamente ai dipendenti, di Dati relativi alla salute, ed è pertanto sottoposta alla normativa in materia di protezione dei dati personali.

La Società considera la salvaguardia dei Dati Personali di cui è Titolare/Responsabile, in conformità con la normativa e regolamentazione applicabile, come un obiettivo di primaria importanza e si impegna ad adottare le misure necessarie per ottemperare a quanto richiesto. Le operazioni di Trattamento dei Dati Personali devono pertanto avvenire nel rispetto dei principi di riservatezza e necessità richiesti dalla normativa e ispirandosi ai principi di correttezza e liceità di Trattamento.

La presente Policy sulla Protezione dei Dati Personali (di seguito anche “Policy”) definisce le linee guida alle quali la Società, in qualità di Titolare/Responsabile, del trattamento come specificato in premessa, deve attenersi per assicurare la tutela dei dati personali secondo i requisiti previsti dalla normativa vigente in materia e in particolare al Regolamento (UE) 2016/679 in materia di protezione dei dati personali (di seguito anche “GDPR”), che tra le principali novità:

- armonizza la disciplina sulla protezione dei dati personali all’interno dell’Unione europea;
- attribuisce fondamentale importanza ai principi della *accountability*, della *privacy by design* e *by default*;



- prevede la formalizzazione del registro dei trattamenti eseguiti, la valutazione d'impatto sulla protezione dei dati e la *data breachnotification*;
- tutela i diritti degli interessati;
- introduce la figura del *Data ProtectionOfficer*
- inasprisce le sanzioni amministrative pecuniarie che, nei casi delle violazioni ritenute più gravi, possono arrivare sino ad un massimo di 20.000.000€o al 4% del fatturato globale annuo.

Il presente documento definisce, altresì, le linee guida per il governo del processo di gestione dei Dati Personali in conformità alle norme, ai regolamenti, ai requisiti e agli standard aziendali in materia; esso ha valore globale, cioè si applica a tutti i Trattamenti di Dati, con riguardo sia ai dati dei Dipendenti, sia ai dati relativi ad altri soggetti in forza dell'operatività aziendale.

La Politica definisce:

- (i) i principi generali applicabili a BPP Service Spa, in qualità di Titolare/Responsabile del trattamento di dati personali e i presidi generali adottati per ottemperare a tali principi;
- (ii) le responsabilità e i compiti degli organi sociali e delle strutture aziendali di BPP SERVICE SpA

1.2. Ambito di Applicazione

La presente Policy si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in archivi o destinati a figurarvi.

Ciascun soggetto deve assicurare il rispetto delle regole stabilite da BPP Service Spa nella presente Policy, onde garantire che i dati personali su cui opera non siano soggetti, anche solo accidentalmente, a distruzione, perdita, accesso non autorizzato o trattamento non consentito o non conforme alle finalità o ai motivi della raccolta.

1.3. Riferimenti normativi principali

I seguenti documenti costituiscono la normativa di riferimento in relazione alla tematica privacy:

- ❖ Regolamento (UE) 2016/679 in materia di protezione dei dati personali (di seguito anche "GDPR");
- ❖ Decreto Legislativo 30 Giugno 2003, N.196 (Codice in materia di protezione dei dati personali) come modificato dal D. Lgs. 10/8/2018, recante Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679
- ❖ Altri provvedimenti normativi o regolamentari nazionali per l'attuazione del GDPR;
- ❖ Provvedimenti, decisioni e linee-guida adottate da parte dell'Autorità Garante per la protezione dei dati personali, tra i quali, in particolare:
 - Provvedimento 27 novembre 2008, "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" e successive modifiche ed integrazioni, di seguito anche "Provvedimento Amministratori di Sistema";
 - Rifiuti di apparecchiature elettriche ed elettroniche (RAEE) e misure di sicurezza dei Dati Personali, del 13 ottobre 2008, di seguito anche "Provvedimento RAEE";
 - Provvedimento in materia di videosorveglianza, dell'8 aprile 2010, di seguito anche "Provvedimento Videosorveglianza";
 - Linee Guida sul trattamento di dati personali dei lavoratori privati, 23 novembre 2006.

- ❖ Linee guida sui responsabili della protezione dei dati (DPO), adottate il 13/12/2016 (e modificate il 5/4/2017) dal Gruppo di lavoro istituito dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, in base agli artt. 29 e 30 della stessa (WP243); nonché in materia di valutazione di impatto sulla protezione dei dati (WP248)

1.4 Aggiornamento/revisione del documento

La Società, con la consulenza del Data Protection Officer, provvede a rivedere la Politica e a valutare eventuali modifiche da apportare a seguito di :

- (i) mutamenti organizzativi di BPP Service Spa;
- (ii) modifiche della normativa europea o nazionale;
- (iii) emanazione o modifica della normativa di secondo livello (es .Provvedimenti del Garante Privacy).

La necessità di revisione del documento viene portata a conoscenza del Consiglio di Amministrazione e del Collegio Sindacale della Società nell'ambito delle relazioni periodiche e dei flussi informativi verso gli organismi di vertice.

La Politica entra in vigore il 1° luglio 2019, sarà pubblicata sulla intranet aziendale e uno stralcio della stessa afferente ai principi generali sul trattamento dei dati personali sarà pubblicato sul sito internet di BPP Service SpA.

2. PRINCIPI E PRESIDI GENERALI SUL TRATTAMENTO DI DATI PERSONALI

La Politica identifica i principali presidi individuati da BPP Service SpA per assicurare il rispetto dei principi generali contenuti nel GDPR, con particolare riguardo a:

- (i) liceità del trattamenti,
- (ii) diritti degli interessati;
- (iii) registro dei trattamenti e valutazione d'impatto sulla protezione dei dati;
- (iv) sicurezza dei trattamenti
- (v) gestione degli eventi di data breach.

Al riguardo BPP Service spa :

- (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;
- (iii) assicura 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 o, all'esterno, da parte di mandatarî o procuratori sotto l'autorità del Titolare/Responsabile.

I trattamenti di dati personali delle diverse categorie di soggetti interessati (es. clienti, dipendenti, mandatarî, procuratori, visitatori, fornitori o altri soggetti terzi che espletano incarichi per conto della Società) svolti da BPP SERVICE SpA si fondano sui seguenti principi:



- **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 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 in materia di protezione dei dati personali devono essere considerati fin dalle fasi di progettazione, implementazione e configurazione di tutte le tecnologie utilizzate per le operazioni di trattamento. BPP Service SpA deve trattare, di default, solamente quei dati che siano necessari al perseguimento delle 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.

2.1 Liceità del trattamento

I trattamenti di dati personali all'interno di BPP Service SpA possono essere condotti esclusivamente in presenza di una o più delle seguenti circostanze e/o sulla base di una o più delle seguenti condizioni:

- esistenza di un contratto di cui l'interessato è parte;
- obbligo legale cui è soggetta BPP Service SpA ;
- salvaguardia di interessi vitali del soggetto interessato;
- esplicito consenso dell'interessato;
- perseguimento di un legittimo interesse di BPP Service SpA.

2.1.1 Richiesta del consenso

Laddove il trattamento di dati personali si fonda 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 e risulti 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, le procedure di BPP Service SpA devono prevedere che il trattamento di dati personali possa essere effettuato al fine di perseguire un legittimo interesse di BPP Service SpA connesso ad esempio, all'esercizio e difesa dei diritti in sede giudiziaria ed al controllo e miglioramento della qualità del servizio. In ottemperanza al principio di *accountability*, in tali casi, le procedure devono



prevedere che la valutazione circa il corretto bilanciamento tra gli interessi di BPP Service SpA e i diritti dell'interessato sia adeguatamente documentata.

2.1.3 Trasferimento dei dati all'estero

Qualora la Società intenda trasferire i dati personali trattati all'esterno dell'Unione europea, il DPO verifica il rispetto di almeno una delle condizioni previste dal GDPR per il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali.

In particolare, il trasferimento di dati personali all'esterno dell'Unione europea potrà avvenire in presenza di:

- una decisione della Commissione in merito al livello di protezione dei dati personali garantito dal Paese Terzo(art. 45 GDPR);
- clausole tipo di protezione dei dati adottate dalla Commissione (art. 46 GDPR, § 2 lett. c));
- clausole contrattuali tra il Titolare/Responsabile del trattamento e il Titolare/responsabile destinatario dei dati nel paese terzo approvate dall'autorità di controllo (art. 46 GDPR, § 3, lett. a);
- un codice di condotta o un meccanismo di certificazione e il contestuale impegno del Titolare/responsabile destinatario dei dati di applicare le garanzie adeguate(art. 46 GDPR, § 2, lett e), f).
- Inoltre, il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale sarà anche possibile nel caso in cui:
- l'interessato abbia prestato esplicitamente il consenso dopo essere stato informato dei possibili rischi;
- il trasferimento sia necessario per l'esecuzione di un contratto concluso tra l'interessato e il Titolare/Responsabile ovvero di misure precontrattuali adottate su istanza dell'interessato;
- il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il Titolare/Responsabile e un terzo a favore dell'interessato;
- il trasferimento sia necessario per importanti motivi di interesse pubblico.

2.2 Diritti degli interessati

2.2.1 Informativa sul trattamento

In conformità ai principi di trasparenza, correttezza, limitazione delle finalità e data retention, le procedure devono prevedere che ai soggetti interessati, all'atto della raccolta dei dati personali, vengano fornite chiare informazioni (Informativa) circa:

- (i) l'identità di BPP Service SpA e del Responsabile della Protezione dei Dati ("DPO –Data ProtectionOfficer");
- (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.

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

Le procedure devono assicurare il rispetto del principio di esattezza e di data retention, prevedendo che ogni interessato abbia il diritto di ottenerla 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);

Il Titolare/Responsabile del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni e le comunicazioni (articoli da 13 a 22 e articolo 34 del GDPR) relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

Il Titolare/Responsabile del trattamento agevola l'esercizio dei diritti dell'interessato e non può rifiutare di soddisfare la richiesta dell'interessato finalizzata ad esercitare i suoi diritti, salvo che dimostri che non è in grado di identificare l'interessato.

Gli interessati contattano direttamente il DPO per l'esercizio dei propri diritti.

Egli si avvale della collaborazione e del supporto di Delegati Interni, designati dalla Società con delibera del Consiglio di Amministrazione, per fornire all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste.

Il DPO informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta. Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato.

Se non ottempera alla richiesta ricevuta, il DPO informa l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale.

I diritti garantiti all'interessato sono:

- 1. Diritto di Accesso:** l'interessato ha il diritto di ottenere la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali che comprendono i dati personali conferiti dall'interessato, i dati personali osservabili generati in esecuzione del contratto, i termini del trattamento compreso il periodo di conservazione previsto;
- 2. Diritto all'informativa:** l'interessato ha diritto a ricevere un'informativa contenente tutti gli elementi indicati negli articoli 13 e 14 GDPR sia nel caso i dati siano forniti direttamente dall'interessato stesso, che nel caso in cui questi siano ottenuti da terzi;
- 3. Diritto di Rettifica:** l'interessato ha il diritto di ottenere la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa;
- 4. Diritto di Cancellazione:** l'interessato ha il diritto di ottenere, se sussistono i motivi indicati dall'art. 17 GDPR, la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e la Società ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali;
- 5. Diritto di limitazione di trattamento:** l'interessato ha il diritto di ottenere la limitazione del trattamento quando si verificano le ipotesi previste dall'Art. 18 del GDPR;
- 6. Diritto di Opposizione / Revoca:** l'interessato ha il diritto di opporsi, o revocare il consenso, in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'art. 6, paragrafo 1, lett.e) o f) del GDPR, compresa la profilazione. La Società si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi



legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

7. Diritto alla Portabilità: l'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti dalla Società e ha il diritto di trasmettere tali dati a un altro Titolare/Responsabile del trattamento senza impedimenti da parte della Società cui li ha forniti qualora il trattamento è effettuato con mezzi automatizzati.

L'articolo 12 GDPR prevede che tutte le informazioni ed i riscontri debbano essere forniti all'interessato con le seguenti modalità:

- in una **forma concisa, trasparente, intelligibile** e con un **linguaggio semplice e chiaro**;
- **per iscritto**, o con mezzi elettronici se la richiesta è stata effettuata con mezzi elettronici. Una risposta orale è consentita solo su domanda espressa dall'interessato;
- **senza ingiustificato ritardo** e, al più tardi, **entro un mese** dal ricevimento della richiesta, salva la possibilità di prorogare tale termine di due mesi nei particolari casi previsti e fermo restando l'obbligo di informare comunque l'interessato del ritardo e dei motivi entro un mese dal ricevimento della richiesta. In ogni caso, se non è possibile soddisfare la richiesta entro un mese dal suo ricevimento, è necessario informare l'interessato (i) che non sarà possibile soddisfare la sua richiesta entro tale termine, (ii) sui motivi della proroga e (iii) sulla possibilità di proporre reclamo ad un'autorità di controllo e ricorso giurisdizionale;
- **gratuitamente**. Può essere addebitato un contributo ragionevole, o negata la soddisfazione della richiesta, solo nel caso di richieste manifestamente infondate o eccessive, anche per la loro ripetitività;
- **dopo aver verificato l'identità dell'interessato**, eventualmente anche domandando informazioni aggiuntive.

2.3 Registro dei trattamenti, analisi dei rischi, valutazione d'impatto e consultazione preventiva

BPP Service SpA è tenuta a predisporre e aggiornare periodicamente un "registro delle attività di trattamento" che identifichi le attività svolte in qualità di Titolare o di Responsabile del trattamento e contenga le informazioni di cui all'art. 30 GDPR. Il registro costituisce la mappatura di tutti i trattamenti effettuati e viene aggiornato periodicamente. Il registro deve essere reso disponibile su richiesta all'Autorità di Controllo. Il registro rappresenta la base per assicurare il rispetto dei principi generali sanciti dal GDPR.

Al fine di assicurare l'integrità e la riservatezza dei dati personali, per ciascuna attività di trattamento identificata nel registro, viene effettuata un'analisi del rischio. Ove da tale analisi emerga che il trattamento possa comportare un livello di rischio elevato per i diritti e le libertà degli interessati, le procedure devono prevedere lo svolgimento di una valutazione di impatto sulla protezione dei dati (Data Protection Impact Assessment, di seguito "DPIA"), previo consulto con il DPO.

Le procedure devono prevedere che, nel valutare la necessità di effettuare una DPIA su un determinato trattamento, si tenga conto, in particolare:

- (i) del livello di rischio per i diritti e le libertà degli interessati,
- (ii) dell'esistenza di un trattamento automatizzato
- (iii) del fatto che il trattamento sia effettuato su larga scala o
- (iv) possa comportare la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

2.4 Sicurezza del trattamento



La Società adotta misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio, valutato in termini di probabilità e gravità per i diritti e le libertà delle persone fisiche.

Tali misure devono essere altresì idonee a prevenire ogni violazione di dati personali, ivi incluse la distruzione, perdita, modifica, divulgazione non autorizzata o l'accesso, in modo accidentale o illegale, a dati personali trattati, nonché a ripristinare tempestivamente la disponibilità e l'accesso ai dati. Qualora si verifichi una violazione di dati personali, le misure tecniche e organizzative adottate devono comunque essere in grado di riconoscere e contrastare l'avvenuta violazione.

Per garantire un livello di sicurezza del trattamento dei dati adeguato al rischio, le procedure devono tener conto anche della natura dei dati personali, e basarsi sui principi di "privacy by design" e "privacy by default". Queste misure possono comprendere, tra l'altro:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di 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, le procedure devono definire le misure di sicurezza 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 Gestione degli eventi di data breach

Sempre al fine di assicurare il rispetto dei principi di integrità e riservatezza dei dati personali, laddove sia identificati un incidente o una violazione di sicurezza, accidentale o illecita, che comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata dei dati compromettendone la riservatezza, la disponibilità o l'integrità, le procedure devono assicurare, previo coinvolgimento del DPO, che la notifica all'Autorità di Controllo avvenga entro 72 ore dal momento in cui sia stata ravvisata la violazione. Tale notifica contiene:

- a) la descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati;
- b) i dati di contatto del DPO;
- c) l'indicazione delle probabili conseguenze della violazione;
- d) la descrizione delle 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, devono essere indicati i motivi del ritardo.

Nei casi in cui la violazione possa comportare elevati rischi per i diritti e le libertà dei soggetti interessati, le procedure devono prevedere che -previo consulto con il DPO -sia fornita agli interessati informativa sulla violazione senza ingiustificato ritardo. L'informativa deve contenere almeno le informazioni di cui alle lettere b), c), d) sopra riportate. Tale comunicazione non è necessaria se comporterebbe uno sforzo sproporzionato oppure se sono state adottate misure tecniche ed organizzative adeguate alla tutela dei dati (es. cifratura).

Le procedure devono stabilire che:

- la scelta della modalità di comunicazione dovrà tenere in considerazione l'accessibilità dei soggetti interessati a formati diversi, e, ove necessario, le diversità linguistiche dei destinatari;



- ciascuna violazione dei dati personali, sospetta o accertata, deve essere adeguatamente censita e documentata nel registro delle violazioni al fine di garantire il rispetto del principio di accountability.

3. RUOLI E LE RESPONSABILITÀ

3.1 Consiglio di Amministrazione del Titolare

- Approva la Policy sulla Protezione dei dati Personali.
- E' responsabile delle decisioni in ordine alle finalità e alle modalità del Trattamento;
- Definisce le misure di sicurezza, delegandone la corretta applicazione ai Responsabili di Settore.
- Nomina i Delegati Interni del Trattamento dei dati.
- Nomina i Responsabili e gli eventuali Sub-Responsabili dei trattamenti come previsto ai successivi punti 3.4 e 3.5 nonché i soggetti autorizzati ai trattamenti (incaricati) di cui al punto 3.6-
- Nomina le Persone Autorizzate al Trattamento.
- Dispone la conservazione presso la Sede sociale di tutte le lettere di nomina, debitamente sottoscritte, per accettazione, da parte dei nominati.
- Prende atto della nomina del DPO di Gruppo, dei compiti e delle responsabilità attribuiti e delle modalità di coordinamento e collaborazione con gli Organi e le Unità Organizzative aziendali.
- Definisce i flussi informativi da/verso le Unità Organizzative aziendali di Controllo e verso gli Organi aziendali.

per il tramite del DPO:

- Adotta misure appropriate per fornire all'interessato tutte le informazioni e le comunicazioni (articoli da 13 a 22 e articolo 34 del GDPR) relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.
 - Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici.
 - Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.
- Informa l'interessato in caso di proroga per l'invio di un riscontro richiesto, illustrando le motivazioni.
- Riceve dal DPO immediata informativa su eventuali fattori critici, relativi alla protezione dei dati, che possono comportare rischi elevati per le libertà e i diritti degli interessati compresi i casi in cui non è stato possibile adottare presidi idonei a mitigare rischi contingenti.
- Notifica eventuali incidenti o violazioni riguardanti i dati personali all'Autorità Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.
- Approva la relazione annuale presentata dal DPO e contenente l'informativa sullo stato dei controlli e del complessivo livello di protezione dei dati personali, informandone i Delegati Interni per le eventuali esigenze di aggiornamento e integrazione della Normativa interna di II livello.



3.2 Delegati Interni del Trattamento dei Dati

Sono nominati dal Consiglio di Amministrazione della Società:

I Delegati Interni:

- Avvalendosi della Struttura Organizzativa, assicurano la corretta applicazione della presente Policy e della normativa interna. Ove necessario od opportuno, propongono l'emanazione di normativa di II livello o, nei limiti della propria autonomia, la emanano direttamente verificandone, poi, la corretta attuazione.
- Dispongono le istruzioni operative per le Persone Autorizzate.
- Supportano il DPO, in particolare al fine di fornire riscontro alle richieste degli interessati per l'esercizio dei diritti di questi ultimi, rispettando i tempi previsti dalla normativa.
- Coadiuvano il DPO nei processi di privacy by design e by default.
- Verificano annualmente i trattamenti di tipo cartaceo ed elettronico, per i conseguenti interventi sul registro dei trattamenti, comunicando al DPO eventuali variazioni intervenute;
- Individuano e adottano idonee misure per evitare lo smarrimento, il danneggiamento, la corruzione, l'utilizzo da parte di soggetti non autorizzati, anche involontari dei dati su cui effettuano un Trattamento.
- Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, mettono in atto misure adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR.
- Ricevono informativa da parte del DPO in caso di rilievo di incidenti o violazioni (data breach), per eventualmente intraprendere le necessarie azioni correttive di competenza.

3.3 Data Protection Officer – DPO di Gruppo

- E' designato dal Consiglio di Amministrazione della Capogruppo in funzione delle sue qualifiche e competenze professionali, della conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati e della capacità di adempiere ai compiti di cui è responsabile;
- Agisce in maniera indipendente nell'ambito delle sue competenze.
- Ha accesso alle risorse umane e finanziarie necessarie ad adempiere ai propri compiti.
- Informa il Titolare/Responsabile del Trattamento sugli adempimenti richiesti dalla normativa e sugli aggiornamenti emanati.
- E' contattato dagli interessati per l'esercizio dei propri diritti, nonché per ricevere qualsiasi informazione relativa agli stessi e/o all' Informativa;
- Di concerto con il Titolare/Responsabile e con il supporto dei Delegati Interni , provvede a prendere in carico le richieste degli interessati e a fornire, senza ingiustificato ritardo e comunque, al più tardi, entro un mese dal ricevimento della stessa, le informazioni; tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste.



- Trasmette alla Società la normativa interna emanata dalla Capogruppo in materia di protezione dei dati personali, nonché i relativi aggiornamenti.
- Verifica la conformità del trattamento con le disposizioni previste dalla normativa di etero ed auto-regolamentazione, fornendo pareri e osservazioni alla Società.
- Fornisce consulenza alla Società sulla predisposizione e la tenuta del Registro dei Trattamenti, verificandone l'aggiornamento in caso di variazioni connesse ai singoli trattamenti o in caso di istituzione di nuovi trattamenti.
- Verifica, almeno annualmente, i trattamenti eseguiti dalla Società.
- Comunica alla Società eventuali variazioni connesse ai singoli trattamenti o i nuovi trattamenti eseguiti da apportare sul registro.
- Richiede, quando lo ritenga, il supporto dei Delegati interni.
- Può richiedere il supporto di Referenti Interni del Trattamento qualora ritenga di avvalersi della collaborazione di esperti e/o specialisti di specifiche materie ("Subject Matter Expert").
- Fornisce consulenza alla Società sulla normativa interna di I e II livello in materia di trattamento dati personali.
- Fornisce consulenza Società per la valutazione della necessità di effettuare una valutazione dell'impatto che un trattamento potrebbe presentare in relazione alla protezione dei dati (Data Protection Impact Assessment - DPIA) nei casi in cui sia previsto un nuovo trattamento, sia modificato un trattamento esistente, o muti il rischio presentato da un trattamento in essere.
- Fornisce consulenza alla Società durante lo svolgimento di una DPIA partecipando attivamente al gruppo di lavoro.
- Verifica la congruità dei piani di formazione posti in essere, richiedendone eventualmente l'erogazione di ulteriori e fornendo consulenza per predisporre l'attività di formazione e addestramento del personale.
- Riceve informativa dalla Società relativamente ad episodi significativi ai fini privacy, intervenuti nello svolgimento dell'attività della Società.
- Informa immediatamente il Titolare/Responsabile del Trattamento ed i Delegati Interni in caso di rilievo di incidenti o violazioni (data breach) per i quali è necessario effettuare la comunicazione al Garante, nonché la notifica agli interessati.
- Con periodicità annuale, predisponde un'informativa per il Consiglio di Amministrazione della Capogruppo sullo stato dei controlli e del complessivo livello di protezione dei dati personali, nonché di eventuali esigenze di aggiornamento e integrazione della normativa interna.
- Coopera con l'Autorità Garante.

3.4 Responsabili del Trattamento dei Dati

Per uno o più trattamenti di dati, la Società, quando riveste la qualità di Titolare può, anche esternalizzando tali trattamenti, nominare soggetti terzi quali Responsabili; può, altresì nominare soggetti terzi quali Sub-Responsabili quando essa riveste la qualità di Responsabile.

I Responsabili e/o i Sub-Responsabili sono selezionati sulla base della sua capacità di offrire garanzie sufficienti a mettere in atto misure tecniche e organizzative adeguate al rispetto dei requisiti del GDPR e per la tutela dei diritti degli interessati, come previsto dall'art. 28 GDPR.

I Responsabili e/o i Sub-Responsabili così nominati:

--

- a) Eseguono trattamenti per conto del Titolare/Responsabile, a seguito sottoscrizione di un contratto in cui sono definite la materia e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali destinati ad essere trattati e le categorie di interessati, gli obblighi e i diritti del Titolare/Responsabile del trattamento e le garanzie e le misure di sicurezza di cui al successivo punto d).
- b) Trattano i dati personali solo su istruzione documentata del Titolare/Responsabile
- c) Garantiscono che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.
- d) Adottano le misure tecniche e organizzative adeguate per garantire un livello di sicurezza commisurato al rischio ai sensi dell'articolo 32 del GDPR.
- e) Rispettano le condizioni di cui ai paragrafi 2 e 4 dell'articolo 28 del GDPR.
- f) Su scelta del Titolare/Responsabile del trattamento, cancellano o restituiscono i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellano le copie esistenti, salvo che sia previsto, per provvedimento normativo o per ordine vincolante di un'Autorità che ne abbia il potere, un obbligo di conservazione dei dati.
- g) Mettono a disposizione del Titolare/Responsabile del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi normativi previsti dal GDPR.
- h) Predispongono e aggiornano un registro dei trattamenti.
- i) Informano immediatamente il DPO in caso di verifica di violazione della protezione dei dati.

3.5 Procedura per il conferimento dell'incarico

Una volta selezionato il Responsabile /Sub-Responsabile si formalizza la designazione tramite la conclusione di un contratto che presenti tutti gli elementi richiesti dal GDPR, tra cui precise istruzioni cui il Responsabile dovrà attenersi e il diritto della Società di risolvere il contratto in caso di inadempimento della controparte.

Nel corso di tutta la relazione contrattuale, dovrà essere assicurato un monitoraggio, prevedendo verifiche periodiche al fine di appurare il rispetto della normativa e delle istruzioni impartite.

A tal fine, sarà contrattualmente previsto il diritto della Società di richiedere l'invio di rendiconti, la compilazione di questionari e/o di effettuare delle visite ispettive.

Nel caso in cui dovessero emergere alcune criticità, il DPO – messo al corrente - verifica e valuta i necessari interventi per la loro mitigazione. Qualora le criticità dovessero perdurare o fossero di un'entità tale da giustificare la cessazione del rapporto contrattuale, il DPO sottopone la proposta di interruzione della relazione contrattuale con il Responsabile/Sub-Responsabile all'approvazione del Consiglio di Amministrazione.

Qualora venga nominato un nuovo Responsabile /Sub-responsabile o vengano modificati i Responsabili/ Sub-responsabili esistenti, la Società informa il DPO e aggiorna il registro,.

L'elenco dei nominativi dei Responsabili è riportato nella sezione "Privacy" del sito www.BPPSERVICE.it.

Gli atti formali di nomina dei Responsabile/ Sub-responsabilidel Trattamento vengono conservati presso la Sede della Società unitamente ai verbali delle delibere del Consiglio di Amministrazione".

3.6 Nomina dei soggetti autorizzati all'esecuzione dei trattamenti - Incaricati

La Società disciplina il processo per la nomina di tutti i dipendenti che trattano dati personali e particolari, nel rispetto delle disposizioni della normativa vigente.



Le lettere di nomina, debitamente controfirmate dai nominati, vengono conservate presso la Sede sociale.

Sono soggetti autorizzati i dipendenti della Società che effettuano operazioni di Trattamento di dati personali dei clienti, dipendenti, mandatari, procuratori e fornitori.

Essi operano sotto la diretta autorità del Titolare o Responsabile, attenendosi alle istruzioni da questi impartite a seguito della nomina ad Incaricato del Trattamento dei Dati Personali e riportate di seguito:

- trattare i dati personali in modo lecito, secondo correttezza e per scopi determinati, espliciti e legittimi, utilizzandoli in altre operazioni di trattamento esclusivamente in termini compatibili con tali scopi;
- verificare che i dati siano esatti, pertinenti, completi e non eccedenti rispetto alle finalità per cui sono stati raccolti e successivamente trattati e, se necessario, aggiornarli;
- conservare i dati in una forma che consenta l'identificazione dell'interessato solo per il tempo strettamente necessario agli scopi per cui i dati sono stati raccolti e successivamente trattati ed in base alla normativa applicabile;
- comunicare, mettere in qualsiasi modo a disposizione, trasferire all'estero i dati personali solo ai soggetti (dipendenti/collaboratori del Titolare/Responsabile meno) autorizzati a riceverli legittimamente per le finalità per cui i dati sono stati raccolti, nel rispetto delle istruzioni ricevute e del GDPR;
- restituire integralmente al Titolare-Responsabile/soggetto indicato dal Titolare/Responsabile i dati personali che per cessazione/modifica delle mansioni lavorative non si ha più ragione di trattare, con espresso divieto di conservarli in copia (in qualsiasi formato), duplicarli, comunicarli o diffonderli. Eventuali copie dovranno essere restituite al Titolare-Responsabile/soggetto indicato dal Titolare/Responsabile o, su richiesta del Titolare/Responsabile, dovranno essere integralmente distrutte, fatti salvi eventuali dati personali la cui conservazione sia imposta dalla normativa vigente;
- informare prontamente il DPO di ogni circostanza idonea a determinare pericolo alla sicurezza dei dati o trattamenti illeciti;
- informare prontamente il DPO : 1) qualora si verifichi la necessità di realizzare operazioni di trattamento di dati personali per finalità o con modalità diverse da quelle risultanti dalle istruzioni ricevute; 2) qualora sia presentata un'istanza da parte degli interessati, o una richiesta del Garante o di altre autorità; 3) qualora ricorra qualsiasi circostanza che esuli dalle istruzioni ricevute;
- accedere e trattare solo le banche dati e i dati (gestiti dal Titolare/Responsabile a cui lo stesso ha accesso per la propria attività) strettamente necessari all'esercizio delle proprie funzioni e mansioni lavorative;
- non fornire telefonicamente o a mezzo fax dati e informazioni:
 - relativi a terzi, senza una specifica autorizzazione del Titolare o del Responsabile;
 - ai diretti interessati, senza avere la certezza della loro identità;
- rispettare le misure di sicurezza fisiche, tecniche e procedurali adottate dal Titolare/Responsabile per la protezione dei dati, facendo quanto necessario per garantirne l'attuazione;
- impiegare maggiore cautela per i dati particolari, giudiziari e relativi a trattamenti che presentano rischi specifici secondo il GDPR o che per qualsiasi ragione sono indicati dal Titolare/Responsabile come meritevoli di particolare attenzione;
- partecipare alle attività di formazione;
- garantire l'esecuzione di quanto altro richiesto dal GDPR e dalle istruzioni ricevute e non espressamente richiamato nel presente documento.



3.6 Amministratori di Sistema

Sono le figure professionali dedicate alla gestione e alla manutenzione di impianti di elaborazione con cui vengono effettuati Trattamenti di Dati Personali, compresi i sistemi di gestione delle basi di Dati, i sistemi *software* complessi quali i sistemi ERP (i.e. *Enterprise Resource Planning*), le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui Dati Personali.

La Società si avvale degli Amministratori di sistema della Capogruppo da quest'ultima nominati previa verifica di tutti i requisiti di legge.

4 DISCIPLINA E MODELLO DI GRUPPO- OSSERVANZA

La Società quale componente del Gruppo Banca Popolare Pugliese si attiene all'applicazione della disciplina del Gruppo Banca Popolare Pugliese; il presidio del rischio correlato al trattamento dei dati personali è assicurato attraverso:

- (i) l'adozione dei presidi generali contenuti nella presente Politica
- (ii) la nomina del medesimo DPO, di cui all'art. 37 del GDPR
- (iii) il coordinamento tra il DPO e il Referente interno di Compliance della Società, nominato dal Consiglio di Amministrazione e identificato nel Responsabile del Settore Recupero Credito.

5. INTERVENTI FORMATIVI PER LE PERSONE AUTORIZZATE AL TRATTAMENTO DI DATI PARTICOLARI RELATIVI AL RAPPORTO DI LAVORO

La Società ha messo a disposizione di tutti gli incaricati per i trattamenti di dati particolari relativi al rapporto di lavoro specifici corsi di autoformazione, in linea con le disposizioni normative.

Tali interventi formativi, basati sugli standard "WBT" (Web Based Training) sono fruibili dalla Intranet aziendale e si propongono di fornire le nozioni fondamentali relative ai principali rischi che incombono sui dati, alle misure per prevenire eventi dannosi e alle responsabilità che ne derivano, nonché i profili principali della disciplina sulla protezione dei dati personali.

La Funzione Personale della Capogruppo con cadenza annuale definisce un programma di formazione specificatamente rivolto alle persone autorizzate al Trattamento dei dati avente ad oggetto:

- l'aggiornamento sugli obblighi normativi in materia di protezione dei dati personali;
- adeguate istruzioni circa i ruoli e responsabilità ad essi facenti capo.

Gli eventi formativi sono organizzati con periodicità annuale. Le modalità di erogazione possono essere definite sulla base delle specifiche necessità dei soggetti interessati ed in base a competenze già acquisite in tale ambito (e.g., e-learning, corso in aula, approccio misto).



Allegato 1 – Definizioni

L'entrata in vigore del Regolamento UE 2016/679 ("GDPR"), pubblicato in Gazzetta Ufficiale UE il 4 maggio 2016, abroga la precedente Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 comporta il superamento del Decreto Legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali (il "Codice Privacy"). Il Codice Privacy resta in vigore per le disposizioni non incompatibili con il Regolamento e per le misure che offrono una tutela maggiore dei diritti e delle libertà dei soggetti interessati dal trattamento.

Si riportano di seguito le definizioni dei termini maggiormente utilizzati nella presente Policy.

Principali definizioni

Dati personali

Tutte le informazioni relative a persone fisiche che consentano l'identificazione, diretta o indiretta, degli individui a cui i dati si riferiscono. Ad esempio, sono dati personali oggetto di tutela, oltre ai dati anagrafici ed economici, anche le immagini ed i codici identificativi riconducibili ad un individuo

Categorie particolari di dati personali

Dati capaci di rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale

Dati relativi alla salute

Dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute

Dati relativi a condanne penali e a reati

Dati relativi a condanne penali e reati o a connesse misure di sicurezza. Il loro trattamento è ammesso solo sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'UE o degli Stati membri, in presenza di garanzie appropriate per i diritti e le libertà degli interessati

Dati biometrici

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 datidattiloscopici

Dati genetici

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

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

Archivio

Qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentrato o ripartito in modo funzionale o geografico

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. I contitolari definiscono i rispettivi ambiti di responsabilità e compiti in un accordo scritto

Data Protection officer (DPO).

La persona fisica responsabile della protezione dei dati trattati dalla Società; ha tra i compiti principali: vigilanza sulla normativa, rendere pareri sulla valutazione di impatto privacy, consultare il Garante della protezione dei dati personali e cooperare con essi.

Delegato interno del trattamento.

Dipendenti della Società, chiamati a fornire collaborazione al DPO, ai fini del rispetto delle vigenti disposizioni in materia di 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. E' nominato dal titolare, qualora un trattamento debba essere effettuato per suo conto

Sub-responsabile del trattamento

La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del responsabile del trattamento, previo ottenimento della richiesta di autorizzazione scritta, specifica o generale, del Titolare del trattamento

Persona autorizzata

Il soggetto che tratta dati personali sotto l'autorità del Titolare del trattamento o del responsabile del trattamento su loro specifiche istruzioni

Amministratore di sistema

Le persone incaricate di gestire e mantenere gli impianti di elaborazione di dati personali o sue componenti. L'attribuzione delle funzioni di amministratore di sistema avviene previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle disposizioni in materia di trattamento di dati personali. La designazione ad amministratore è individuale e reca l'elencazione analitica degli ambiti di operatività in base al profilo di autorizzazione assegnato

Rappresentante

La persona fisica o giuridica stabilita nell'Unione Europea che, designata per iscritto dal Titolare del trattamento/responsabile del trattamento non stabilito nell'EU, li rappresenta per quanto riguarda gli obblighi di cui al GDPR

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 caratteristiche riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica

Pseudonimizzazione

Il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative

Cifratura



Modalità di conversione del testo originale in una sequenza apparentemente casuale di lettere, numeri e segni speciali che solo la persona in possesso della corretta chiave di decifratura potrà riconvertire nel file di testo originale

Violazione dei dati personali (data breach)

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

Autorità di controllo

L'autorità pubblica indipendente istituita da uno Stato membro con lo scopo di sorvegliare l'applicazione della normativa sulla protezione dei dati personali, 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

Dipendenti e/o personale assimilato

Ogni dipendente, collaboratore e/o stagista di BPP Service SpA.

