POLICY PRIVACY

Data emissione: 18/12/2018

Versione: 01

INDICE

1 - PREMESSA

1.1 Oggetto e scopo

La presente Policy sulla Protezione dei Dati Personali (la "Policy") definisce le linee guida alle quali la Cooperativa (di seguito denominata "Titolare") deve attenersi nella pianificazione e nello svolgimento di qualsivoglia attività che implichi il trattamento di Dati personali per assicurare la tutela di tali Dati secondo i requisiti previsti dalla normativa in materia e in particolare al Regolamento (UE) 2016/679 in materia di protezione dei Dati personali (di seguito anche "GDPR").

Le disposizioni della presente Policy hanno il fine di garantire che il trattamento dei dati personali avvenga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità delle persone fisiche.

In particolare, la Policy individua:

- i destinatari della normativa interna ed esterna in materia di privacy;
- i principi generali a protezione dei Dati personali a cui è improntata l'attività aziendale;
- i principali ruoli previsti in ambito privacy.

1.2 Contesto normativo di riferimento

Il 14 aprile 2016 il Parlamento e il Consiglio Europeo hanno approvato il Regolamento UE n. 679/2016 in materia di protezione dei Dati personali (di seguito "GDPR" e "Regolamento"), entrato in vigore il 25 Maggio 2016 e direttamente applicabile in tutta l'Unione Europea dal 25 Maggio 2018 con conseguente abrogazione della Direttiva 95/46/CE del Parlamento e del Consiglio Europeo del 24 Ottobre 1995, recepita in Italia dal Decreto Legislativo n. 196 del 30 Giugno 2003 (Codice in materia di protezione dei Dati personali).

Il GDPR modifica in maniera profonda la normativa in materia di privacy e in particolare:

- armonizza la disciplina sulla protezione dei Dati personali all'interno di tutta l'Unione europea;
- attribuisce fondamentale importanza ai principi della accountability, della privacy by design e by default;
- coerentemente con il principio della accountability, introduce, tra gli altri, gli istituti del Registro dei trattamenti, della valutazione d'impatto sulla protezione dei dati e della data breach notification;
- rafforza e introduce nuovi diritti degli interessati, che tutti i Titolari sono tenuti a garantire al fine di assicurare che il trattamento dei Dati personali sia svolto in piena conformità alla normativa, anche per incrementare il livello dei servizi forniti ai clienti;
- introduce la figura del Data Protection Officer;
- 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 a livello di gruppo imprenditoriale.

Il contesto normativo di riferimento comprende inoltre l'ulteriore normativa primaria e secondaria in materia privacy e protezione dei Dati personali, compresi i provvedimenti emanati dal Garante, dalle Istituzioni europee e dal WP29, nonché le norme previste del codice civile e penale italiano.

1.3 Principi generali

Il Titolare svolge le proprie attività nel rispetto dei principi generali in materia di privacy previsti dalla normativa di riferimento e dalla presente Policy.

In particolare, nella pianificazione o espletamento di qualsiasi attività che comporti trattamento di Dati personali, il Titolare assicura che i Dati personali siano:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (**principio di liceità, correttezza e trasparenza**);
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in un modo non incompatibile con tali finalità (**principio di limitazione della finalità**);
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (**principio di minimizzazione dei Dati personali**);
- esatti e, se necessario, aggiornati tempestivamente rispetto alle finalità per le quali sono trattati (**principio di esattezza**);
- 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 (**principio di limitazione della conservazione**);
- 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 (**principi di integrità e riservatezza**).

1.4 Definizioni

Ai fini della presente Policy si intende per:

- **"Dato personale"**: 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 – articolo 4, punto 1), GDPR;
- **"Dati particolari":** Dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona – articolo 9 GDPR;
- **«Dati rischiosi»** Il trattamento dei dati diversi da quelli particolari e giudiziari che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti.
- **"Titolare del trattamento**" la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le

finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

- **"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 – articolo 4, punto 8), GDPR;
- **Data Protection Officer o DPO":** indica il soggetto designato dal Titolare o dal Responsabile del trattamento per assolvere funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del GDPR;
- **«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.
- **"Incaricato"**: la persona fisica autorizzata a compiere operazioni di trattamento dal Titolare o dal Responsabile;
- **"Garante"**: l'Autorità garante italiana per la protezione dei Dati personali;
- **«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.
- **"Registro dei trattamenti"**: i titolari e i Responsabili del trattamento devono tenere il registro delle attività di trattamento svolte sotto la propria responsabilità, contenenti le informazioni di cui all'articolo 30 GDPR;
- **"Valutazione di impatto sulla protezione dei dati"** o **"Data Protection Impact Assessment (DPIA)"**: valutazione di impatto sulla protezione dei dati effettuata dal titolare quando un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

1.5 Ambito di applicazione

Tutto il personale (compresi stagisti o tirocinanti), i collaboratori ed eventuali terze parti che a diverso titolo operano per il Titolare, sono tenuti a rispettare la presente Policy nell'ambito delle rispettive competenze e attività.

2 - DPO

Il DPO e la relativa struttura organizzativa, ove presente, rappresentano la principale funzione di consultazione, consulenza, sorveglianza e controllo in materia di protezione dei Dati personali.
Nell'espletamento delle proprie attribuzioni, il DPO si avvale inoltre della collaborazione del Referente Privacy.

2.1 Posizione

Il DPO:

- è interessato quando vengono prese decisioni con implicazioni sulle misure di protezione dei Dati personali;
- è coinvolto nel processo di definizione di nuovi prodotti, servizi, progetti di business e relaziona periodicamente in merito alla conformità dei trattamenti e all'andamento degli indicatori interni sulla protezione dei Dati personali;

- è facilmente raggiungibile, tramite mezzi sicuri di comunicazione, dagli interessati e all'interno dell'organizzazione aziendale, per tutte le questioni relative al trattamento dei loro Dati personali e ai loro diritti previsti dal GDPR;
- funge da punto di contatto per il Garante per questioni connesse al trattamento, tra cui la consultazione preventiva e consultazioni relative a qualunque altra questione.

2.2 Mansioni del DPO

Il GDPR attribuisce al DPO compiti di consulenza, informazione e sorveglianza, nonché un ruolo di contatto con il Garante e gli interessati, ammettendo la possibilità che gli siano attribuite mansioni ulteriori, purché non diano adito a conflitti di interesse.

3 - RUOLI PRIVACY

3.1 Referente privacy

Il Referente Privacy è nominato dal Consiglio di Amministrazione in funzione dell'esperienza professionale e della conoscenza della realtà aziendale.
Il Referente privacy svolge un ruolo di collegamento tra il DPO, gli Incaricati e gli Organi Aziendali del Titolare.

3.2 Incaricati al Trattamento

Il Titolare garantisce un'adeguata formazione degli Incaricati tramite corsi e la fornitura di istruzioni precise su come effettuare i trattamenti. A tal fine, il Titolare organizza eventi di formazione in materia di protezione dei Dati personali, sulla normativa applicabile e sull'impianto privacy adottato. Questi eventi formativi sono organizzati periodicamente e, in ogni caso, qualora dovessero intervenire novità normative o organizzative rilevanti.

3.3 Responsabili Esterni del Trattamento (Artt. 27 e 28 GDPR)

Il Titolare può esternalizzare alcuni trattamenti a soggetti individuati quali Responsabili del trattamento, selezionati tenendo in considerazione la capacità di offrire garanzie sufficienti a mettere in atto misure tecniche e organizzative adeguate al rispetto dei requisiti del GDPR.
Ogni qualvolta un trattamento è esternalizzato ad una persona fisica o giuridica, il Titolare assicura che tale soggetto terzo sia nominato Responsabile esterno del trattamento nel rispetto delle disposizioni del GDPR.
Una volta selezionato il Responsabile esterno, si provvede alla sottoscrizione di un contratto o diverso atto giuridico di nomina che presenti tutti gli elementi richiesti dal GDPR, tra cui precise istruzioni cui il Responsabile esterno dovrà attenersi e il diritto del Titolare di risolvere il contratto in caso di inadempimento della controparte.
Nel corso di tutta la relazione contrattuale, è assicurato un continuo monitoraggio, tramite verifiche periodiche sull'operato dei Responsabili esterni al fine di appurare il rispetto della normativa in materia di privacy e delle istruzioni impartite dal Titolare.

In caso di nomina di un nuovo Responsabile esterno o di modifica di Responsabili esterni esistenti, deve essere aggiornato conseguentemente anche il Registro dei trattamenti.

4 - GESTIONE DEI TRATTAMENTI

4.1 Condizioni di liceità del trattamento (Artt. 5 e 6 GDPR)

Il Titolare garantisce che i Dati personali siano trattati esclusivamente in presenza di una delle condizioni di liceità del trattamento previste dal GDPR, tenendo in considerazione la natura del dato personale oggetto di trattamento (i.e. dati comuni, categorie particolari di Dati personali, dati giudiziari e dati di minori).

In particolare, il Titolare adotta i presidi necessari ad assicurare che il trattamento di Dati personali sia effettuato solo ove ricorra almeno una delle seguenti condizioni:

- l'interessato ha espresso il proprio consenso;
- il trattamento è necessario per eseguire un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- il trattamento è necessario per adempiere ad un obbligo di legge;
- il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- il trattamento è necessario per perseguire un legittimo interesse del titolare o di terzi, salvo che prevalgano gli interessi o i diritti e le libertà dell'interessato.

Nel dare avvio a una nuova tipologia di trattamento, il Titolare verifica con il coinvolgimento del DPO, che esso sia fondato su una delle fonti di liceità del trattamento di cui sopra.

Il Titolare fornisce agli Incaricati che interagiscono con gli interessati le istruzioni necessarie a garantire il rispetto della normativa e della presente Policy.

Qualora il fondamento di liceità del trattamento sia il consenso, gli Incaricati devono rilasciare un'informativa agli interessati e richiedere il consenso, nel rispetto delle procedure interne e delle istruzioni ricevute, prima che il trattamento abbia inizio. Il consenso deve essere libero, specifico e informato, manifestato tramite un'azione positiva inequivocabile e richiesto separatamente per ogni finalità del trattamento.

La normativa interna stabilisce l'obbligo di registrare l'ottenuto consenso mediante procedure che assicurino un agevole recupero di data, modalità e contenuto del consenso.

I termini del trattamento, indicati sulle informative, contengono e descrivono in modo puntuale il periodo di conservazione dei Dati personali oppure, se non possibile, i criteri utilizzati per determinare tale periodo.

4.2 Trattamento di dati di minori e di categorie particolari di dati personali (Artt. 8 e 9 GDPR)

Nel caso in cui il trattamento sia basato sul consenso e abbia ad oggetto Dati personali di minori, il Titolare assicura che il trattamento abbia luogo esclusivamente se tale consenso è prestato o autorizzato dal titolare della potestà genitoriale.
Il consenso o l'autorizzazione del titolare della responsabilità genitoriale sono registrati tramite processi che ne assicurino un agevole recupero.
Qualora il trattamento riguardi Categorie particolari di Dati personali e il trattamento si basi sul consenso, il Titolare assicura che sia rilasciata un'informativa agli interessati e richiesto un consenso esplicito, nel rispetto delle Procedure interne, prima che il trattamento abbia inizio.

4.3 Gestione del Registro dei trattamenti (Art. 30 GDPR)

Il Titolare gestisce la tenuta, l'aggiornamento e la conservazione del Registro dei trattamenti nel rispetto della normativa e della presente Policy.
Vi sono attività che potrebbero comportare una modifica o l'inizio di un nuovo trattamento con la conseguente necessità di aggiornare il Registro dei trattamenti; fra queste rientrano a titolo esemplificativo:

- la progettazione di una nuova iniziativa che preveda il trattamento di Dati personali;
- l'estensione di un trattamento già previsto a nuove categorie di interessati o Dati personali;
- qualsiasi modifica della struttura organizzativa della società;
- la sottoscrizione di contratti di fornitura che comportino la nomina a Responsabile esterno della controparte;
- le categorie di destinatari cui i Dati personali oggetto del trattamento sono comunicati;
- la necessità di trasferire i Dati personali trattati all'esterno dell'Unione europea;
- qualsiasi modifica dei sistemi informativi adottati;
- l'adozione di nuove misure tecniche e/o organizzative.

Il Registro dei trattamenti aggiornato deve essere reso disponibile a tutti gli Incaricati del Titolare secondo modalità atte ad assicurarne l'agevole consultazione.

5 - PRINCIPI DI PROTEZIONE DEI DATI PERSONALI

5.1 Accountability (Art. 5 GDPR)

Per trattare i Dati personali in conformità con la normativa vigente e la presente Policy, il Titolare adotta misure tecniche, organizzative e di sicurezza adeguate, nonché adeguati meccanismi di controllo della costante conformità ti tali misure nel tempo e ne dispone il costante aggiornamento.
Il Titolare documenta le attività svolte per garantire che i trattamenti siano effettuati in conformità alla normativa applicabile e tiene tale documentazione a disposizione per eventuali accessi del Garante.

5.2 Privacy by design (Art. 25 GDPR)

Il Titolare assicura che tutte le applicazioni, servizi, prodotti ed attività che prevedono il trattamento di Dati personali siano progettati e successivamente effettuati tenendo in considerazione gli effetti che potrebbero avere sulla protezione

dei Dati personali e sui diritti degli interessati. A tal fine, sin dal momento della determinazione di modalità e mezzi del trattamento dei Dati personali, sono adottate misure tecniche e organizzative adeguate, volte ad attuare in modo efficace i principi di protezione dei Dati e ad integrare nel trattamento le garanzie necessarie a soddisfare i requisiti della normativa applicabile e a tutelare i diritti degli interessati.

5.3 Privacy by default (Art. 25 GDPR)

Il Titolare assicura che siano trattati, per impostazione predefinita, esclusivamente i Dati personali necessari per ogni specifica finalità del trattamento.
A tal fine, in fase di delineazione del trattamento, sono adottate le idonee misure tecniche e organizzative e sono valutati, in particolare, i seguenti elementi allo scopo di ridurre al minimo necessario l'impatto sul diritto alla protezione dei Dati personali rispetto alle finalità perseguite:

- quantità dei Dati personali da raccogliere;
- portata del trattamento;
- periodo di conservazione;
- numero di soggetti che ha accesso ai Dati personali.

6 - TRASFERIMENTO DI DATI PERSONALI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI (Artt. 44, 45, e 46 GDPR)

Il trasferimento di Dati personali all'esterno dell'Unione Europea può avvenire, in presenza di almeno una delle seguenti condizioni:

- una decisione di adeguatezza della Commissione Europea;
- clausole tipo di protezione ("Model Contract Clauses") dei dati adottate dalla Commissione Europea;
- clausole contrattuali tra il Titolare del trattamento e il Titolare/Responsabile destinatario dei Dati personali nel paese terzo approvate dall'autorità di controllo;
- adozione di un codice di condotta o meccanismo di certificazione e contestuale impegno del Titolare/Responsabile destinatario dei Dati personali di applicare le garanzie adeguate.

Il trasferimento di Dati personali verso un paese terzo o un'organizzazione internazionale sarà inoltre 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 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 e un terzo a favore dell'interessato;
- il trasferimento sia necessario per importanti motivi di interesse pubblico.

7 - DIRITTI DEGLI INTERESSATI

I diritti attribuiti dal GDPR agli interessati si dividono in due categorie: (i) i diritti che necessitano di una richiesta espressa dell'interessato; (ii) i diritti ai quali la normativa collega un obbligo del titolare in modo autonomo dalla ricezione di una previa richiesta dell'interessato.

7.1 I diritti subordinati a una richiesta espressa dell'interessato (Artt. 15-21 GDPR)

Il processo per la gestione dei diritti esercitati dagli interessati mediante espressa richiesta è riconducibile alle seguenti fasi principali:

- ricezione della richiesta;
- gestione della richiesta;
- riscontro all'interessato e archiviazione.

I principali diritti che il GDPR garantisce all'interessato e che lo stesso può esercitare mediante richiesta sono i seguenti:

1. **Diritto di Accesso**. L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di Dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai Dati personali 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 di Rettifica.** L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei Dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei Dati personali incompleti, anche fornendo una dichiarazione integrativa;
3. **Diritto di Cancellazione**. L'interessato ha il diritto di ottenere dal titolare del trattamento, se sussistono i motivi indicati dal GDPR, la cancellazione dei Dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i Dati personali;
4. **Diritto di limitazione di trattamento**. L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando si verificano le ipotesi previste dall'art. 18 del GDPR;
5. **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'articolo 6, paragrafo 1, lettere e) o f) del GDPR, compresa la profilazione. Il titolare del trattamento si astiene dal trattare ulteriormente i Dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
6. **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 a un titolare del trattamento e ha il diritto di trasmettere tali Dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora il trattamento è effettuato con mezzi automatizzati.

Infine, nel caso di esercizio dei diritti di rettifica, cancellazione e/o limitazione del trattamento da parte dell'interessato, il Titolare provvede anche a effettuare la comunicazione ai destinatari interessati prevista dall'articolo 19 GDPR.

7.2 I diritti non subordinati a una richiesta dell'interessato

Pur in assenza di richiesta da parte dell'interessato, il Titolare garantisce che allo stesso sia fornita idonea informativa al momento della raccolta dei suoi Dati personali presso lo stesso o, se i Dati non sono raccolti direttamente presso l'interessato, entro i seguenti termini:

- entro un termine ragionevole dall'ottenimento dei Dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i Dati personali sono trattati;
- nel caso in cui i Dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato;
- nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei Dati personali.

8 - MISURE DI SICUREZZA (Art. 32 GDPR)

Il Titolare adotta le misure tecniche e organizzative opportune 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, nonché del rischio di varia 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 o l'accesso non autorizzato a Dati personali, effettuati in modo accidentale o illegale. 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.

9 - LA VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI - DPIA (Art. 32 GDPR)

Nel caso in cui un determinato tipo di trattamento presenti un rischio elevato per i diritti e le libertà delle persone fisiche (ad esempio perché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento), è necessario effettuare una valutazione dell'impatto prima di procedere al trattamento stesso.
Qualora la valutazione di impatto sulla protezione dei Dati personali evidenzi un rischio elevato per gli interessati, con l'eventuale supporto del DPO, deve essere valutata l'adozione di ulteriori misure per attenuare il rischio e/o la necessità di

effettuare una consultazione preventiva con il Garante. Eventuali successivi suggerimenti del Garante sono immediatamente recepiti prima di procedere al trattamento oggetto della DPIA.
Per i trattamenti già sottoposti a DPIA è prevista una revisione di tali valutazioni almeno ogni 3 anni.

10 - DATA BREACH (Artt. 33 e 34 GDPR)

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.
Nel caso in cui si verifichi una violazione dei Dati personali che presenti un rischio per le libertà e i diritti degli interessati, il Titolare prevede una modalità immediata di reazione che permetta:

- la notifica dell'avvenuta violazione al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza e, se ricorrono i presupposti, all'interessato;
- l'adozione delle misure necessarie ad attenuare gli effetti negativi della violazione.

Il Titolare tiene un registro delle violazioni e stabilisce procedure interne che disciplinano il suo aggiornamento al sussistere di ogni violazione, indipendentemente dal rischio presentato per i diritti e le libertà degli interessati e meccanismi di conservazione di tutte le comunicazioni riguardanti la violazione. In tale registro sono indicati tutti gli elementi richiesti dalla normativa applicabile, tra cui:

- le circostanze relative alla violazione;
- le conseguenze;
- le misure adottate per contrastarla e limitarne gli effetti;
- i Dati personali coinvolti; informazioni adeguate per permettere al Titolare di determinare le motivazioni per non aver effettuato la notifica, o averla effettuata in ritardo.