Città di Lecce

Procedura di Gestione delle Violazioni dei dati personali (“*Data Breach Procedure Management*”)

COMUNE DI LECCE

Via Rubichi 16 - 73100 Lecce (LE)

Telefono: 0832.682111 - Codice Fiscale: 80008510754

Indirizzo PEC: protocollo@pec.comune.lecce.it

Città di Lecce

COMUNE DI LECCE	
TIPOLOGIA	Procedura
ARGOMENTO	Procedura di Gestione delle Violazioni dei dati personali (Data Breach)
OBIETTIVO	Assicurare una corretta gestione delle violazioni previste dalle normative sulla protezione dei dati
DESTINATARI	Tutto il personale dipendente, collaboratori e Responsabili del trattamento
REDATTO DA	Titolare del trattamento – Responsabile Protezione Dati (RPD/DPO)
COLLABORAZIONE	Responsabile Protezione Dati (RPD/DPO)

STORIA DELLE MODIFICHE			
NOME DEL FILE/CODIFICA	**DATA**	**VERS. - REV.**	**RIFERIMENTO**
Istituzione Procedura	25/05/2018	01.00	GDPR

Città di Lecce

SOMMARIO

PROCEDURA DI GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI ("*DATA BREACH PROCEDURE MANAGEMENT*") 1

INTRODUZIONE 4

SCOPO 5

AMBITO APPLICATIVO 6

DEFINIZIONI, TERMINI E ACRONIMI 6

DOCUMENTI E NORMATIVE DI RIFERIMENTO 9

GESTIONE DEL *DATA BREACH* DA PARTE DEI SOGGETTI AUTORIZZATI AL TRATTAMENTO E NOTIFICA AL GARANTE DELLA PROTEZIONE DEI DATI PERSONALI. 13

Gestione *Data Breach* da parte dei Responsabili (ex art. 28) e notifica al Garante 14

INDIVIDUAZIONE E DESCRIZIONE DELLA VIOLAZIONE DEI DATI PERSONALI 15

Tipi di Violazioni (Data Breach) 15

Violazione di dati 18

VALUTAZIONE DEL RISCHIO CONNESSO ALLA VIOLAZIONE 19

NOTIFICA DELLA VIOLAZIONE DEI DATI PERSONALI ALL'AUTORITÀ DI CONTROLLO 22

COMUNICAZIONE DELLA VIOLAZIONE DEI DATI PERSONALI A INTERESSATO/I 23

REGISTRO DELLE VIOLAZIONI E DOCUMENTAZIONE DELLA VIOLAZIONE 25

CONTROLLI 26

ALLEGATI AL PRESENTE DOCUMENTO: 27

Città di Lecce

INTRODUZIONE

Il Regolamento Generale sulla protezione dei dati UE 679/2016 (di seguito GDPR), prescrive per il Titolari del trattamento un nuovo adempimento generalizzato che consiste nella violazione dei dati personali (*c.d. Data Breach*), in precedenza e in base alla normativa italiana tale adempimento era infatti limitato solo ad alcuni specifici settori e contesti.

In tale contesto il COMUNE DI LECCE, in qualità di Titolare del trattamento dei dati personali, ritiene necessario dotarsi di una procedura interna per la corretta gestione delle violazioni dei dati personali.

In base al Considerando 85 del GDPR, una violazione dei dati personali (*c.d. Data Breach*) potrebbe, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali e immateriali alle persone fisiche.

A seguito di un violazione di dati personali possono derivare pregiudizi di varia natura dalla perdita di controllo dei dati personali alla limitazione diritti degli interessati compreso il furto o usurpazione di identità, pregiudizio alla propria reputazione e perdita di riservatezza, ma più in generale qualsiasi danno economico o sociale anche significativo agli interessati.

Al fine prevenire o mitigare tali pregiudizi, il Titolare del trattamento ho l'obbligo, senza ingiustificato ritardo e ove possibile entro le 72 ore da quando ne è venuta a conoscenza, di notificare la violazione occorsa all'Autorità di Controllo competente. Il Titolare viene ritenuto esente da tale obbligo qualora ritenga sotto la propria responsabilità che la violazione dei dati personali presenti un rischio improbabile in termini di pregiudizio per i diritti e le libertà delle persone fisiche.

Città di Lecce

SCOPO

La presente procedura ha lo scopo di indicare le corretta modalità operative adottate da parte del Titolare del trattamento dei dati personali, nel rispetto dei principi previsti dalle disposizioni del Regolamento UE 679/2016, per la gestione delle violazione de dati personali ed in particolare:

- Assicurare la migliore tutela per i diritti e libertà degli interessati;
- Garantire una effettiva conformità rispetto al quadro normativo applicabile in materia di protezione dei dati;
- Salvaguardare il proprio patrimonio informativo.

Garantendo altresì:

- La notifica di una violazione dei dati personali all'Autorità di controllo e la comunicazione di una violazione dei dati personali all'interessato, qualora il Titolare ritenga probabile che dalla violazione derivino rischi per i diritti e le libertà degli interessati;
- L'identificazione della violazione;
- L'analisi delle cause della violazione;
- La definizione delle misure da adottare per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi;
- La registrazione delle informazioni relative alla violazione, delle misure identificate e dell'efficacia delle stesse.

AMBITO APPLICATIVO

Le politiche descritte nel presente documento si applicano a tutti i dipendenti e collaboratori dell'Ente (con particolare riferimento alla gestione di tutti gli archivi/documenti cartacei e di tutti i sistemi informatici), i quali durante lo svolgimento delle loro attività possono venire a conoscenza di una violazione dei dati personali. Le presenti politiche si applicano anche ai fornitori nella misura in cui sono da considerarsi Responsabili del trattamento, ai sensi dell'articolo 28 del GDPR e compatibilmente con procedure adottate e applicate dagli stessi.

In tal contesto è fatto obbligo loro di segnalare la violazione secondo le modalità indicate nelle presente procedura.

DEFINIZIONI, TERMINI E ACRONIMI

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 (art. 4, punto 1).

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 (art. 4, punto 2).

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia digitalizzato o meno, centralizzato, decentralizzato o ripartito in modo funzionale o geografico (art. 4, punto 6).

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 (art. 4, punto 7).

Data Protection Officer **(DPO):** la persona fisica individuata come Responsabile della protezione dei dati personali ai sensi del GDPR (in particolare artt. 37, 38, 39).

GDPR: Regolamento Generale per la protezione dei dati personali.

Designati al trattamento (Art. 2-quaterdecies del D.Lgs. 196/2003 come novellato dal D.Lgs. 101/2018): la persona fisica che, secondo l'organizzazione aziendale, ricopre un ruolo gestionale e di responsabilità all'interno, che determina specifiche modalità organizzative rispetto ad uno o più trattamenti.

Autorizzato al trattamento: la persona fisica, espressamente designata, che opera sotto l'autorità del Titolare del trattamento, con specifici compiti e funzioni connessi al trattamento dei dati personali (artt. 29 e 4, punto 10).

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 (artt. 28 e 4, punto 8).

Device Fissi: si intendono gli strumenti informatici non facilmente removibili dal perimetro "aziendale" quali personal computer, server locali, stampanti affidati alle Persone Autorizzate;

Device Mobili: in generale si intendono quegli strumenti informatici che per loro natura sono facilmente asportabili dal perimetro "aziendale" quali chiavette USB, SD Cards, Hard Disk esterni, Tablet e Smartphone utilizzati dalla Persone Autorizzate;

Rete: rappresenta il perimetro digitale "aziendale" contenente Dati Personali e/o informazioni riservate comprensivo della rete interna (*Intranet*) e della rete esterna (*Internet*) a cui ci si può collegare via rete LAN, Wi-Fi o VPN.

Violazione dei dati personali (*c.d. 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 (art. 4, punto 12);

«Autorità di controllo/Autorità»: l'Autorità pubblica indipendente istituita da uno Stato membro; in Italia è il Garante per la protezione dei dati personali.

RAID: Responsabile Area informatica/digitale

DESIGNATI: Responsabili della tutela dei dati personali e della sicurezza dei dati designati per la gestione della violazione dei dati che coordinano e supervisionano la corretta applicazione della procedura di gestione delle violazioni dei dati personali.

DOCUMENTI E NORMATIVE DI RIFERIMENTO

Articolo 33

Notifica di una violazione dei dati personali all'Autorità di controllo:

1. In caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'Autorità di controllo competente a norma dell'articolo 55 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. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

2. Il Responsabile del trattamento informa il Titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

3. La notifica di cui al paragrafo 1 deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le probabili conseguenze della violazione dei dati personali;

d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

5. Il Titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'Autorità di controllo di verificare il rispetto del presente articolo.

Articolo 34

Comunicazione di una violazione dei dati personali all'Interessato:

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento comunica la violazione all'Interessato senza ingiustificato ritardo.

2. La comunicazione all'Interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).

3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:

a) il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

4. Nel caso in cui il Titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

Linee Guida e Provvedimenti

- Guida all'applicazione del Regolamento Europeo in materia di protezione dei dati personali, Garante per la protezione dei dati personali (edizione aggiornata – Febbraio 2018);

- REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 "GDPR" relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) - ***Considerando n. 85, 86, 87, 88 artt. 33 e 34;***

- Decreto Legislativo 30 giugno 2003 n. 196, come modificato e armonizzato dal Decreto Legislativo del 10 agosto 2018, n. 101;

- Decreto Legislativo 10 agosto 2018, n. 101 - Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati).

- Linee guida sulla notifica delle violazioni di dati personali ai sensi del Regolamento UE 679/2016 ("*on Personal Data Breach Notification under Regulation 2016/679*), adottate dal Gruppo di lavoro Articolo 29 ("*WP 29*") - adottate il 3 Ottobre 2017 – Revisionate in via definitiva il 6 Febbraio 2018;

- Guida all'applicazione del Regolamento Europeo in materia di protezione dei dati personali, Garante per la protezione dei dati personali (edizione aggiornata – Febbraio 2018)

- Linee guida concernenti la Valutazione di Impatto sulla Protezione dei Dati nonché i criteri per stabilire se un trattamento "*possa presentare un rischio elevato*" ai sensi del Regolamento 2016/679, adottate dal *WP29* - in via definitiva il 4 ottobre 2017;

- Linee guida sui Responsabili della Protezione dei Dati (WP243), adottate dal *WP29*;

- Dichiarazione relativa al ruolo di un approccio basato sul rischio nel quadro normativo in materia di protezione dati (WP218), adottata dal *WP29* il 30 maggio 2014.

Città di Lecce

GESTIONE DEL "DATA BREACH" DA PARTE DEI SOGGETTI DESIGNATI/AUTORIZZATI AL TRATTAMENTO E NOTIFICA AL GARANTE DELLA PROTEZIONE DEI DATI.

Ogni Soggetto Designato/Autorizzato al trattamento dei dati personali, ai sensi dell'articolo 29 del GDPR e dell'art. 2 quaterdecies del D.Lgs. 196/2003 (come modificato dal D.Lgs. 10 agosto 2018, n. 101), qualora venga a conoscenza di un potenziale caso di una violazione dei dati personali, è tenuto ad avvisare tempestivamente il Titolare del trattamento e/o i soggetti da esso delegati per la gestione della violazione dei dati che coordinano e supervisionano la corretta applicazione della procedura di gestione delle violazioni dei dati personali (in seguito indicati anche con l'acronimo **RTDP/DESIGNATI**), tali figure coordinano le attività di comunicazione al Garante e al DPO.

I soggetti indicati con l'acronimo **RTDP/DESIGNATI**, che ricevono una segnalazione su una potenziale violazione dei dati personali sono tenuti:

A) La segnalazione viene inoltrata al **TITOLARE** e viene immediatamente informato il **DPO**;

B) Si avviano gli accertamenti dovuti per comprendere il contesto del trattamento, la natura dei dati personali coinvolti e qualunque informazione utile per una completa valutazione dell'episodio;

C) Conclusi gli accertamenti e comunque non appena vengano individuati elementi chiari per la valutazione dell'episodio, si procederà a seconda dei casi a:

C.1) Chiudere l'accertamento senza annotazione nel "*Registro delle violazioni",* qualora sia esclusa in modo chiaro una violazione dei dati personali;

C.2) Annotare la violazione dei dati personali nel Registro, senza effettuare alcuna notificazione qualora vi sia un rischio improbabile per i diritti e le libertà degli interessati (a seguito della valutazione di tale rischio);

C.3) Annotare la violazione dei dati personali nel Registro ed effettuare la notificazione all'Autorità di Controllo e/o la comunicazioni agli Interessati.

Nei casi indicati ai punti C.2 e C.3 è fatto obbligo a tutti i soggetti coinvolgere immediatamente i vertici organizzativi del Titolare del trattamento anche al fine di valutare il coinvolgimento delle altre professionalità necessarie per l'analisi dell'accaduto.

Inoltre sono tenuti ad effettuare la valutazione del rischio della violazione di dati personali, per decidere, sulla scorta delle determinazioni raggiunte, se effettuare l'eventuale comunicazione all'Autorità Garante.

Gestione "Data Breach" da parte dei Responsabili (ex art. 28) e notifica al Garante

Qualora il trattamento di dati è affidato da parte del Titolare del trattamento ad un soggetto terzo, denominato Responsabile, così come disciplinato dall'articolo 28 del Regolamento sulla protezione dei dati personali (UE) 2016/679:

1) Ogni Responsabile del trattamento, qualora venga a conoscenza di un potenziale "*Data Breach"* che riguardi dati di cui il Comune di Lecce è Titolare, ne dà avviso senza ingiustificato ritardo; **Per "ingiustificato ritardo" si considera la notizia pervenuta al più tardi entro 72 ore dalla presa di conoscenza iniziale da parte del Responsabile.*

2) Il Responsabile del trattamento deve garantire il reperimento delle informazioni affinchè il Titolare stesso possa gestire il "*Data Breach";*

3) Ad ogni Responsabile del trattamento deve essere comunicato il soggetto/referente al quale effettuare la predetta segnalazione (indirizzo mail);

4) Il soggetto effettua una valutazione dell'evento avvalendosi, se necessario, di eventuali altre professionalità necessarie per la corretta analisi della situazione. Il soggetto può avvalersi del DPO per eventuali funzioni consulenziali.

INDIVIDUAZIONE E DESCRIZIONE DELLA VIOLAZIONE DEI DATI PERSONALI

Le violazioni dei dati personali sono una tipologia di incidente per la sicurezza delle informazioni nel quale sia coinvolto qualsiasi genere di dato di natura personale (anagrafici, numeri di carte personali, codici identificativi, dati sanitari, dati biometrici, dati relativi a conti correnti, ecc.). Per facilitare l'individuazione della violazione dei dati evidenzia di seguito le diverse tipologie, come indicate dalle Linee Guida W29. Il Presente paragrafo descrive le possibili violazioni dei dati personali.

Tipi di Violazioni (Data Breach)

a) Violazione della disponibilità, in caso di perdita o distruzione dei dati personali a seguito di accesso non autorizzato ai dati personali;

b) Violazione dell'integrità, in caso di alterazione non autorizzata o accidentale dei dati personali;

c) Violazione della riservatezza, in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali.

Città di Lecce

TIPO DI VIOLAZIONE (DATA-BREACH)	DEFINIZIONE	ESEMPI
PERDITA DI DISPONIBILITÀ	Tale violazione comporta che non si può accedere ai dati personali, quando un incidente di sicurezza rende non accessibili i dati personali, anche solo per un certo periodo. Tale ipotesi è da considerare un *Data Breach*, in quanto la mancanza di accesso ai dati può avere un impatto significativo sui diritti e libertà degli Interessati.	**1-** Furto o smarrimento di un dispositivo (Hard Disk) contenente dati. **2-** Copia unica di dati personali crittografata da *Ransomware*, o comunque crittografata utilizzando una chiave di cifratura non più disponibile. **3-** Cancellazione volontaria o accidentale di dati di cui se ne deve assicurare la conservazione. **4-** Impossibilità di ripristinare l'accesso ai dati, ad esempio da un backup. **5-** Interruzione significativa del normale servizio anche in caso di interruzione di corrente o attacco *Denial of Service*, tale da rendere i dati personali non disponibili. **6-** Annullamento di attività che presuppongono un trattamento di dati personali a causa di un disservizio tecnico, per cui le persone potrebbero subire un serio danneggiamento. **7-** Perdita, anche solo temporanea, di disponibilità (ad esempio nel caso in cui i dati possono essere successivamente ripristinati dal backup) causata da un'infezione dei sistemi informatici, *Ransomware*. In tal caso, comunque, si è verificata un'intrusione nella rete del Titolare, con possibile DB. **8-** Pirata informatico contatta l'azienda dopo aver Hackerato del sistema informatico per chiedere un riscatto. **9-** Distruzione o perdita di una copia o un backup di dati detenuti dai soggetti autorizzati, ma i dati sono ancora detenuti dal Titolare. **10-** Perdita di documenti contenenti categorie particolari di dati

Città di Lecce

VIOLAZIONE DELL'INTEGRITÀ	Tale violazione comporta alterazione non autorizzata o accidentale dei dati personali	**1.** Il Titolare rileva che c'è stata una possibile intrusione nella sua rete, che potrebbe aver compromesso l'integrità dei dati. **2.** Modifica di dati personali o categoria di dati personali contenuti in documenti.
VIOLAZIONE DELLA RISERVATEZZA	Tale violazione riguarda la divulgazione o accesso non autorizzato o accidentale di dati personali	**1.** Perdita di una chiave USB con dati personali non crittografati, di cui terzi potrebbero essere venuti in possesso. **2.** Segnalazione, anche da parte di un terzo, di un episodio nel quale un soggetto non autorizzato accidentalmente ricevuto dati personali relativi a soggetti interessati per trattamenti riferibili dal Titolare. **3.** Situazioni in cui un terzo contatti l'Ente dopo aver *hackerato* il suo sistema per chiedere un riscatto. **4.** Situazioni in cui un terzo o un soggetto autorizzato a trattare i dati informa l'Ente di aver ricevuto dai suoi indirizzi mail una comunicazione non destinata a lui, contenente dati personali. **5.** Violazione della riservatezza e/o accesso non autorizzato a documenti contenenti categorie particolari di dati personali

Violazione di dati

Nel caso la violazione interessi dati archiviati in formato digitale su basi dati o supporti di memorizzazione o in formato cartaceo, devono essere osservate le seguenti modalità per la segnalazione.

1. Chi rileva la violazione lo comunica ai **RTDP/ DESIGNATI** e/o al **RAID,** fornendo i dati in suo possesso.

2. Il **RAID** e i **RTDP/DESIGNATI** accertano la reale esistenza della violazione e, in caso sia confermata la violazione stessa, confermano al **TITOLARE** e al **DPO** l'avvenuta violazione.

3. Il **DPO**, acquisito un ragionevole grado di certezza del fatto che sia avvenuta un incidente per la sicurezza delle informazioni che abbia compromesso dati personali, inserisce una voce per la descrizione del *Data Breach* nel "*Registro delle violazioni*", ed avvia il trattamento della violazione.

Città di Lecce

Tabelle per accertamenti e ispezioni preliminari

VALUTAZIONE DEL RISCHIO CONNESSO ALLA VIOLAZIONE

Per identificare le modalità di gestione di una violazione e gli eventuali obblighi di notifica e/o di comunicazione, i **RAID** (con il supporto del **DPO**), effettuano la valutazione del rischio, come di seguito indicato.

Il livello di rischio è definito sulla base di due parametri, gravità e probabilità:

- **Gravità**: rilevanza degli effetti pregiudizievoli che la violazione è in grado di produrre sui diritti e le libertà delle persone coinvolte (es. impedendo il controllo da parte dell'interessato sulla diffusione dei propri dati);
- **Probabilità**: grado di possibilità che si verifichino uno o più eventi temuti (es. la perdita di ogni traccia dei dati).

Ai fini della identificazione dei valori da attribuire ai due parametri per la valutazione del rischio, è possibile considerare i seguenti fattori:

- tipo di violazione;
- natura, sensibilità e volume dei dati personali;
- facilità nella identificazione degli interessati;
- gravità delle conseguenze per gli interessati;
- particolarità degli interessati (es. minori);
- numero degli interessati.

Città di Lecce

GRAVITÀ	<u>Impatto della violazione sui diritti e le libertà delle persone coinvolte:</u> • ***Basso***: nessun impatto • ***Medio***: impatto poco significativo, reversibile • ***Alto***: impatto significativo, irreversibile
PROBABILITÀ	<u>Possibilità che si verifichino uno o più eventi temuti:</u> • ***Basso***: l'evento temuto non si manifesta • ***Medio***: l'evento temuto potrebbe manifestarsi • ***Alto***: l'evento temuto si è manifestato

		GRAVITÀ		
		A	**M**	**B**
PROBABILITÀ	**A**			
	M			
	B			

	DESCRIZIONE	**Notifica all'Autorità Garante**	**Comunicazione agli interessati**
RISCHIO	Basso: nessun pregiudizio sui diritti e sulle libertà degli interessati né sulla sicurezza dei dati personali coinvolti	**NO**	**NO**
	Medio: possibile pregiudizio sui diritti e sulle libertà degli interessati e sulla sicurezza dei dati personali coinvolti	**SI/NO**	**NO**
	Alto: pregiudizio certo sui diritti e sulle libertà degli interessati e sulla sicurezza dei dati personali coinvolti	**SI**	**SI**

Sulla base degli elementi di cui sopra:

I. I **RTDP/ DESIGNATI** coadiuvati dal **DPO**, stimano la gravità e la probabilità della violazione e classifica il rischio;

II. Il **DPO**, previa condivisione della valutazione con il Titolare e i **RTDP/ DESIGNATI**, documenta la decisione presa a seguito della valutazione del rischio nel "*Registro delle violazioni*";

i. Nel caso in cui il rischio sia considerato non elevato e non si ritenga necessario procedere con la comunicazione, il **DPO** specifica la giustificazione per tale scelta, riservando la possibilità di comunicare la violazione in seguito.

ii. Nel caso il rischio lo richieda, il **DPO** su indicazione del **TITOLARE** procede alla notifica della violazione all'Autorità garante, e ove necessario agli Interessati.

III. Gli elementi a supporto del procedimento e degli esiti della valutazione del rischio sono documentati dal **DPO** su indicazione del **TITOLARE** e dei **RTDP/ DESIGNATI**.

Città di Lecce

NOTIFICA DELLA VIOLAZIONE DEI DATI PERSONALI ALL'AUTORITÀ DI CONTROLLO

La normativa prevede che, non appena si viene a conoscenza di una violazione dei dati personali che presenti un rischio di qualsiasi livello superiore al livello "Medio" per i diritti e le libertà delle persone coinvolte, è obbligatorio effettuare la notifica all'Autorità.

Per le violazioni così identificate, i **RTDP/ DESIGNATI** con il supporti del **DPO**, redige il documento di notifica della violazione, compilando l'apposito modello presente sul sito dell'Autorità, e la invia all'Autorità di controllo tramite posta elettronica certificata (PEC). **N.B.:** Da Dicembre 2020 è divenuto operativo il nuovo servizio del Garante (https://servizi.gpdp.it/databreach/s/) per gli adempimenti previsti in caso di Data Breach.

Qualora la notifica all'Autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Il documento di notifica contiene almeno i seguenti elementi:

- La natura della violazione dei dati personali, compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- Il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- Le probabili conseguenze della violazione dei dati personali;

- Le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione;
- I motivi del ritardo, qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore;
- Eventualmente, una dichiarazione sulla mancanza di alcune delle informazioni necessarie e un impegno a fornire, il prima possibile, le informazioni aggiuntive, in una o più fasi successive.

COMUNICAZIONE DELLA VIOLAZIONE DEI DATI PERSONALI A INTERESSATO/I

Nel caso di accertamento di una violazione dei dati personali che sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare comunica la violazione all'interessato/i.

La comunicazione non è richiesta se è soddisfatta una delle seguenti condizioni:

- ✓ Il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- ✓ Il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

- ✓ Detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

La comunicazione contiene almeno i seguenti elementi:

- La natura della violazione dei dati personali, descritta con linguaggio semplice e chiaro;
- Il nome e i dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- Le probabili conseguenze della violazione dei dati personali;
- Le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione.

Per la comunicazione, è possibile identificare uno o più canali di comunicazione, a seconda delle circostanze, quali email, SMS, posta, comunicati pubblicitari, banner o notifiche su siti web, scegliendo il canale che massimizza la probabilità che tutti gli interessati siano raggiunti dal messaggio.

Città di Lecce

REGISTRO DELLE VIOLAZIONI E DOCUMENTAZIONE DELLA VIOLAZIONE

Il **TITOLARE** avvalendosi dei **RTDP/ DESIGNATI** coadiuvati dal **DPO**, coordinano e supervisionano l'aggiornamento del *Registro delle violazioni*, ai sensi dell'art. 33, comma 5 del GDPR, verificando che siano state annotate tutte le informazioni utili e necessarie per la gestione della possibile violazione dei dati personali.

Per ogni violazione di cui sia accertata l'esistenza, il **TITOLARE** avvalendosi dei **RTDP/ DESIGNATI** coadiuvati dal **DPO** coordinano e supervisionano l'aggiornamento del "*Registro delle violazioni*", ai sensi dell'art. 33, comma 5 del GDPR, verificando unitamente al **DPO** che siano state annotate tutte le informazioni utili e necessarie per la gestione della possibile violazione dei dati personali, ovvero:

- ✓ Data rilevazione della violazione;
- ✓ Natura della violazione e categorie di dati personali coinvolti;
- ✓ Servizio/Area coinvolti;
- ✓ Categorie (numero ove possibile) degli interessati coinvolti;
- ✓ Cause della violazione;
- ✓ Probabili conseguenze della violazione;
- ✓ Rischio (derivante dalla stima della gravità e della probabilità);

- ✓ Misure adottate o di cui si propone l'adozione per mitigare i rischi e possibili effetti negativi;
- ✓ Notifica Autorità Garante per la Protezione dei dati (data e ora, rifermento per reperire la notifica);
- ✓ Comunicazione agli interessati (data e ora, modalità di comunicazione);
- ✓ Verifica attuazione ed efficacia delle misure adottate e data di verifica.

Ad integrazione di quanto riportato nel Registro, il **DPO** raccoglie e conserva tutti i documenti relativi ad ogni violazione, compresi quelli inerenti le circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione è resa disponibile all'Autorità di controllo per le verifiche di competenza.

CONTROLLI

Qualora siano identificati più Titolari del trattamento (caso di Responsabili esterni del trattamento o di Titolari autonomi), ruoli e responsabilità tra le parti sono stati definiti preliminarmente con la "Nomina di Responsabile esterno del trattamento" ovvero con la "*clausola privacy*" sottoscritte dal soggetto esterno, per la gestione degli obblighi di notifica e di comunicazione in caso di violazione dei dati personali. In questi casi, il Titolare del trattamento con il supporto del **DPO,** concorda con i Responsabili esterni del trattamento o Titolari autonomi, le modalità per la gestione degli obblighi di notifica e di comunicazione in caso di violazione dei dati personali, al fine di garantire il rispetto dei termini di notifica e di comunicazione, di cui il Titolare del trattamento resta legalmente responsabile.

ALLEGATI AL PRESENTE DOCUMENTO:

- ***Allegato DB.1***_Modello segnalazione *Data Breach*;
- ***Allegato DB.2***_Disposizioni operative di prevenzione del *Data Breach;*
- ***Allegato DB.3***_Modello di comunicazione all'Interessato della violazione dei dati personali;
- ***Allegato DB.4.1***_Tabella accertamenti e ispezioni preliminari in caso di Violazione dei dati personali;
- ***Allegato DB.4.2***_Check list valutazione del rischio inerente la Violazione;
- ***Allegato DB.4.3***_Possibili scenari di *Data Breach;*
- ***Allegato DB.5***_Registro delle Violazioni dei dati personali - *Data Breach.*