MARSH RISK CONSULTING

RISK. DISPUTES. STRATEGY.

Regolamento Europeo UE 2016/679 in materia di protezione dei dati personali

28 Settembre 2018

MARSH

AGENDA

Sezione #1 Obiettivi

Sezione #2 Contesto di riferimento Privacy

Sezione #3 Concetti base della Privacy

Sezione #4 Linee Guida

Sezione #1 | Obiettivi

Obiettivi del documento

Obiettivi

Lo scopo del presente documento è quello di fornire indicazioni in merito al trattamento dei dati personali eseguito dalle Misericordie della Toscana (di seguito “Misericordie”), in modo che i trattamenti siano svolti in conformità con quanto predisposto dal GDPR e che i dati siano trattati nel rispetto dei principi di Sicurezza delle Informazioni.

In particolare le slide successive hanno come obiettivo quello di indirizzare le attività svolte dalle Misericordie che prevedono un trattamento di dati personali in modo da garantire:

- la conformità a quanto previsto dalla nuova normativa sulla protezione dei dati personali dei trattamenti effettuati internamente alle Misericordie come Titolari del Trattamento dei dati e come Responsabili Esterni del Trattamento e dei trattamenti effettuati da terze parti (ad es. fornitori delle Misericordie) che, nell’ambito delle proprie attività, eseguono un trattamento dei dati personali di cui le Misericordie sono Titolari;
- la definizione di strategie di controllo e monitoraggio costante del rispetto della normativa sulla protezione dei dati personali e sul rispetto dei principi inerenti la Sicurezza delle Informazioni.

Sezione #2 | Contesto di riferimento Privacy

Il contesto

In data 4 maggio 2016 è stato pubblicato sulla Gazzetta ufficiale dell'Unione europea il Nuovo Regolamento per la protezione dei dati personali (*General Data Protection Regulation*, di seguito anche GDPR)

Innumerevoli e di carattere sostanziale sono le novità introdotte in materia di protezione dei dati personali dal Nuovo Regolamento che, oltre a determinare impatti in termini organizzativi, operativi e tecnologici, introducono un approccio alla *Data Privacy* indirizzata secondo il principio del Rischio associato alla valutazione delle misure applicate ai Dati trattati

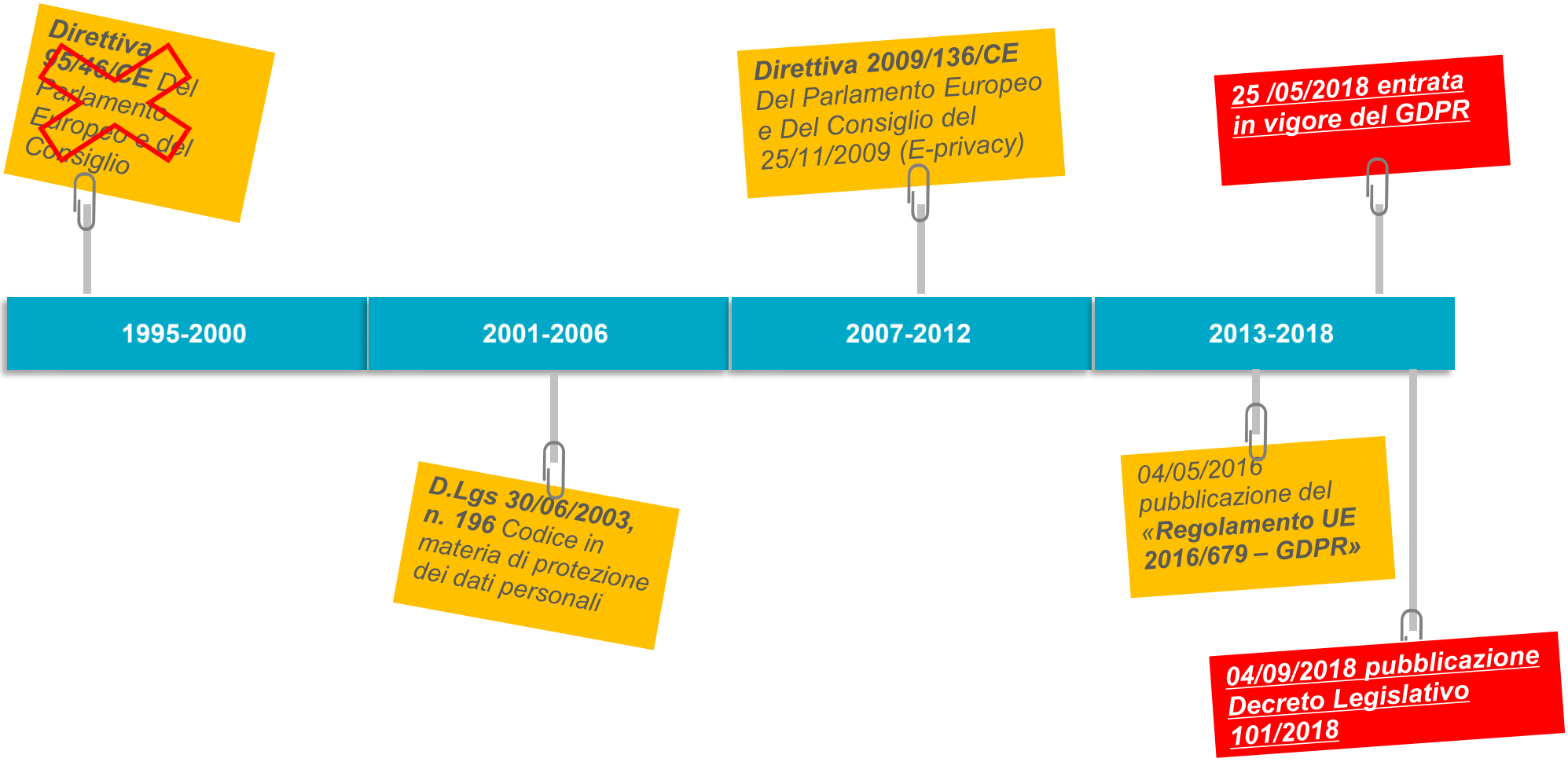
Evoluzioni della normativa in ambito Privacy - Overview

Di seguito si riporta la *time line* temporale indicativa delle evoluzioni normative in ambito *privacy* dal 1995, data di pubblicazione della Direttiva 95/46/CE, fino al 25 Maggio del 2018, termine per l'adeguamento al GDPR.

CONTESTO DI RIFERIMENTO PRIVACY

Evoluzioni della normativa in ambito Privacy - Overview

Di seguito si riporta la *time line* temporale indicativa delle evoluzioni normative in ambito *privacy* dal 1995, data di pubblicazione della Direttiva 95/46/CE, fino al 25 Maggio del 2018, termine per l'adeguamento al GDPR.



Sezione #3 | Concetti base della Privacy

Le parole chiave della Privacy (1/2)

PRIVACY

1. **Ambito di applicazione:**
   Il GDPR si applica alle persone fisiche /giuridiche coinvolte nel Trattamento dei Dati Personali riguardanti persone fisiche dell'Unione Europea. In casi specifici si applica anche se il titolare del trattamento non è un membro dell'Unione Europea

2. **Dato personale:**
   Qualsiasi informazione che riguardi persone fisiche identificate o che possono essere identificate anche attraverso altre informazioni

3. **Categoria particolare di dati:**
   dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare 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

4. **Dato relativo a condanne o reati:**
   dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza

5. **Trattamento:**
   Un'operazione o un complesso di operazioni che hanno per oggetto dati personali

6. **Ruoli e responsabilità:**
   in conformità con il GDPR dovranno essere definite le seguenti figure previste dal regolamento:
   - Titolare del trattamento
   - *Data Protection Officer*
   - Responsabile del trattamento

Le parole chiave della Privacy (2/2)

7. Interessato:
Persona fisica o giuridica, a cui si riferiscono i dati personali, ovvero il proprietario dei suoi dati

8. Titolare del trattamento:
Persona fisica o giuridica, autorità giuridica, servizio od organismo che determina le finalità ed i mezzi del trattamento di dati personali

9. Responsabile del trattamento:
Persona fisica o giuridica, autorità giuridica, servizio od organismo che tratta dati personali per conto del titolare del trattamento

PRIVACY

10. Autorizzato:
Persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile ai sensi dell'art. 29 GDPR

11. Violazione dei dati personali:
La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati trasmessi, conservati o comunque trattati (data breach)

Sezione #4 | Linee Guida

Misure da implementare (1/2)

Di seguito si riportano le principali misure da implementare:

1. Registro delle attività di Trattamento – art. 30

Deve essere garantita la piena conoscenza e tracciabilità dei dati personali trattati dalle Misericordie e la valutazione della loro criticità, al fine di agevolare l'implementazione degli adeguati livelli di protezione e sicurezza.
In questo contesto, il Titolare del trattamento dovrà predisporre un Registro dei trattamenti ed aggiornarlo periodicamente, si consiglia almeno ogni quattro mesi, o ogni qualvolta ci sia una modifica dei trattamenti contenuti al suo interno.

2. Informative sul Trattamento dei Dati Personali – art. 13

L'Interessato deve essere informato in merito alle modalità e alle finalità con cui si eseguono i trattamenti dei propri dati personali prima di effettuarne la raccolta e, laddove necessario, fornire il proprio consenso al trattamento dei dati.
Tali informazioni dovranno essere erogate all'Interessato attraverso un'adeguata informativa.

3. Privacy by Design e by Default – art. 25

Dovranno essere attuate a livello organizzativo, procedurale e tecnologico, soluzioni volte a garantire l'applicazione dei principi di Privacy by Design e Privacy by Default (di seguito by D&D), ossia di protezione dei dati personali fin dalla progettazione e protezione degli stessi per impostazione predefinita.

Misure da implementare (2/2)

4. Data Protection Impact Assessment (DPIA) – art. 35

Per ogni trattamento dovrà essere definito il livello di criticità delle informazioni attraverso un approccio risk-based, definendo la necessità di effettuare un Data Protection Impact Assessment (di seguito anche DPIA – Valutazione degli impatti) . In particolare ogni trattamento, in un momento precedente all'entrata a regime di un nuovo servizio/processo che comporta il trattamento di dati personali, dovrà essere valutato con l'obiettivo di definire se il trattamento stesso possa comportare un rischio per le libertà dell'Interessato.

5. Gestione dei diritti degli Interessati – art. 12

Devono essere previste misure a livello organizzativo, procedurale e tecnologico volte a garantire all'Interessato l'esercizio dei propri diritti e a fornire a quest'ultimo le informazioni di cui necessita; le richieste degli Interessati devono essere ricevute, prese in carico ed evase senza ingiustificato ritardo ed anche qualora, a seguito di opportuna valutazione, si ritenesse di non dar seguito a quanto ricevuto, è comunque obbligatorio fornire riscontro all'istante in ordine alle ragioni che hanno determinato la mancata risposta.

6. Rilevazione e Gestione del Data Breach – art. 33

In caso di rilevazione di una violazione di dati personali (Data Breach), il Titolare del trattamento, ovvero qualsiasi figura interna alle Misericordie che riceva una segnalazione di sospetta o avvenuta violazione dei dati personali, ha la responsabilità di portare l'avvenimento immediatamente all'attenzione del Titolare del trattamento e del DPO, laddove presente.

LINEE GUIDA

Focus: Registro delle Attività di Trattamento

Contenuti del Registro predisposto dal Titolare del Trattamento

- il nome e i dati di contatto del Titolare, di eventuali contitolari del trattamento, del rappresentante del Titolare del trattamento e del Data Protection Officer (DPO), laddove nominato;
- le finalità del trattamento;
- la descrizione delle categorie di interessati e delle categorie di dati personali trattati;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi o organizzazioni internazionali;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale;
- ove possibile, i termini previsti per la cancellazione delle diverse categorie di dati personali;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative poste in essere per il trattamento in sicurezza dei dati.

1

Contenuti del Registro predisposto dal Responsabile del Trattamento

- il nome e i dati di contatto del Responsabile o dei responsabili del trattamento, di ogni Titolare del trattamento per conto del quale agisce il Responsabile del trattamento, del rappresentante del Titolare del trattamento o del Responsabile del trattamento e, ove applicabile, del Data Protection Officer;
- le categorie dei trattamenti effettuati per conto di ogni Titolare del trattamento;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative per assicurare la sicurezza del trattamento.

2

Modalità di tenuta e aggiornamento del Registro

I registri del trattamento andranno mantenuti ed aggiornati periodicamente, si consiglia ogni quattro mesi, prevedendo:

- l'eliminazione dei trattamenti di dati personali non più effettuati;
- l'integrazione dei trattamenti in precedenza non censiti (ad es. da censire in seguito alla realizzazione di un nuovo servizio/processo che comporta il trattamento di dati personali);
- la modifica delle informazioni relative ai trattamenti ancora in essere, laddove queste risultino non più corrispondenti ai trattamenti effettuati (ad es. nei casi in cui siano intervenute modifiche organizzative o di processo che possano comportare modifiche nell'esecuzione del trattamento);
- l'aggiornamento anche dei registri dei trattamenti redatti dalla Misericordia in qualità di Responsabile Esterno di Trattamento.

3

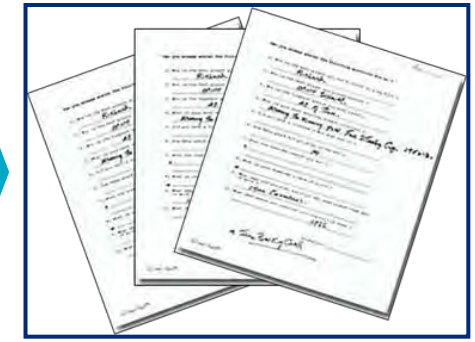
PDF

Qui di fianco il collegamento al file pdf: «Template del Registro delle attività dei Trattamenti»

Focus: Informative sul Trattamento dei dati personali

Di seguito si riportano i principali elementi caratterizzanti l'informativa sul trattamento dei dati personali:

1. Finalità e basi giuridiche del trattamento
2. Dati personali oggetto di trattamento
3. Tempi di conservazione dei dati
4. Modalità d'uso dei dati
5. Ambito di circolazione dei dati
6. Natura del conferimento
7. Diffusione dei dati
8. Trasferimento dei dati all'estero
9. Titolare e Responsabile della Protezione dei dati
10. Esercizio dei diritti
11. Modalità di esercizio dei diritti



Sopra il collegamento al file pdf: «Template di Informativa Privacy»

Focus: Privacy by Design e by Default

a ***Privacy by Design***: definizione, già dalla fase di progettazione di qualsiasi iniziativa progettuale, degli strumenti e delle procedure improntati alla gestione in sicurezza dei dati

b ***Privacy by Default***: garantire che vengano raccolti e trattati solo i dati strettamente necessari al raggiungimento delle specifiche finalità definite, che questi ultimi siano conservati solo per il tempo strettamente necessario per perseguire l'indicata finalità e resi accessibili solo al personale espressamente e preventivamente autorizzato

Nuovo Trattamento/ modifica a trattamenti già censiti

1

Individuare:
- i dati personali che saranno oggetto di trattamento;
- la/ le finalità per la quale/ si effettua il trattamento dei dati personali in ambito

Valutare se i dati che si prevede di trattare siano quelli minimi necessari al perseguimento

Determinare il periodo di conservazione dei dati

2

Individuare:
- i dipendenti e/o collaboratori e/o altri soggetti terzi che, per lo svolgimento delle rispettive mansioni, avranno accesso ai dati personali, per prevedere le opportune nomine a responsabile del trattamento
- l'ubicazione geografica dei server sui cui risiedono, o su cui transiteranno temporaneamente, i dati oggetto di trattamento

3

3.a Qualora le nuove attività comportino un nuovo trattamento sui dati personali precedentemente non censito sul "Registro delle attività di trattamento" effettuare la DPIA e predisporre una prima versione del nuovo trattamento da censire sul Registro dei trattamenti

3.b Qualora le nuove attività comportino una modifica ad un trattamento già censito sul Registro, effettuare la DPIA e predisporre una proposta di modifica al trattamento

DPIA: RISCHIO BASSO

DPIA: RISCHIO ELEVATO

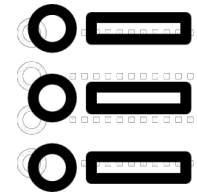
Consultazione preventiva al Garante Italiano della Privacy
(art. 36 GDPR)

Focus: Data Protection Impact Assessment (DPIA)

Il Titolare, e laddove nominato consultando il DPO, effettua una valutazione di impatto sulla protezione dei dati prima di procedere ad un nuovo trattamento, non censito nel Registro o qualora un trattamento preveda l'uso di nuove tecnologie.

Valutazione necessaria nei casi in cui:

- il trattamento comporti una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- si effettui un trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 paragrafo 1 del GDPR, o di dati relativi a condanne penali e a reati di cui all'articolo 10 del GDPR;
- si effettui un'attività di sorveglianza sistematica su larga scala di una zona accessibile al pubblico.



Contenuti minimi della valutazione:

- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal Titolare del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Focus: Gestione dei diritti degli Interessati

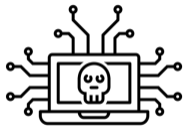
Le attività relative alla gestione delle istanze degli Interessati in relazione all'esercizio dei propri diritti in materia di protezione dei dati personali si articolano, principalmente, nelle seguenti macro fasi:

1	**Ricezione dell'istanza degli Interessati**	Il punto di contatto, per indirizzare le richieste degli Intressati relative all'esercizio dei loro diritti, è il Titolare del trattamento, contattabile attraverso uno specifico indirizzo di posta elettronica, come comunicato nelle informative privacy erogate agli stessi Interessati. Il Titolare, o eventualmente il DPO, ha il compito di prendere in carico la richiesta dell'Interessato, gestire e coordinare internamente le attività per l'evasione della richiesta e fornire riscontro all'Interessato.
2	**Presa in carico dell'istanza**	Ricevuta la richiesta da parte dell'Interessato, il Titolare o il DPO censisce la richiesta sul Registro delle istanze degli Interessati (di seguito anche "Registro delle istanze").
3	**Valutazione dell'istanza**	A seguito della presa in carico dell'istanza inviata dall'Interessato, il Titolare, o eventualmente il DPO, effettua una valutazione della stessa. In particolare, basandosi anche sullo storico delle richieste ricevute da parte del soggetto richiedente, il Titolare valuta l'eventuale ripetitività della richiesta e la sua fondatezza. Qualora dalla valutazione emerga che l'istanza sia manifestamente infondata o ripetitiva, il Titolare del trattamento valuta l'opportunità di rifiutare di soddisfare la richiesta indicando gli elementi che dimostrino il carattere manifestamente infondato o eccessivo della richiesta medesima o di richiedere all'interessato un contributo spese basato sui costi amministrativi sostenuti.
4	**Gestione e coordinamento delle attività interne per l'evasione dell'istanza**	Qualora la richiesta sia fondata, il Titolare coinvolge i soggetti interni alle Misericordie che, nell'ambito delle loro attività, effettuano un trattamento di dati personali dell'Interessato per ottenere supporto in merito all'evasione della richiesta secondo le modalità descritte nel paragrafo. Qualora la richiesta sia infondata, il Titolare provvede autonomamente a fornire riscontro all'Interessato
5	**Elaborazione ed invio della risposta / del riscontro all'Interessato**	Il riscontro all'Interessato deve essere fornito via e-mail o a mezzo di posta, in forma concisa trasparente e intellegibile, e deve essere predisposto con linguaggio semplice e chiaro. Qualora l'interessato dovesse presentare richiesta mediante mezzi elettronici, le informazioni dovranno essere fornite preferibilmente, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'Interessato. Il riscontro all'Interessato sarà fornito dal Titolare del trattamento o eventualmente dal DPO. Il Regolamento stabilisce che il riscontro all'Interessato in merito alla richiesta di esercizio di tutti i diritti riconosciuti debba avvenire entro il termine di un mese dalla richiesta, anche qualora la risposta abbia esito negativo; tale limite temporale può essere prorogato di due mesi in casi di particolare complessità o sulla base del numero delle richieste ricevute. In caso di estensione del termine di risposta, si fornisce un riscontro agli Interessati in relazione alla motivazione della proroga ed alla dilazione delle tempistiche di risposta.
6	**Archiviazione della documentazione inerente l'istanza e la risposta all'interessato**	Il Titolare del trattamento o il DPO, laddove nominato, archivia la documentazione relativa alle istanze degli interessati ed alla loro presa in carico, valutazione ed evasione congiuntamente al Registro delle istanze debitamente aggiornato.

Focus: Rilevazione e Gestione del Data Breach

Le attività connesse alla gestione di eventuali violazioni di riservatezza dei dati (Data Breach) possono essere catalogate nelle seguenti fasi:

1. Rilevazione del Data Breach



In caso di rilevazione di una violazione di dati personali (Data Breach), il Titolare del trattamento, ovvero qualsiasi figura interna alle Misericordie che riceva una segnalazione di sospetta o avvenuta violazione dei dati personali, ha la responsabilità di portare l'avvenimento immediatamente all'attenzione del Titolare del trattamento e del DPO, laddove presente. Si tratta della fase di comunicazione in ambito interno della rilevazione del Data Breach, prodromica all'avvio dell'iter di gestione dello stesso.

2.Valutazione/ gestione del Data Breach

In seguito alla ricezione delle informazioni, il Titolare del trattamento, o il DPO, effettua una valutazione degli impatti sulle libertà e sui diritti degli interessati i cui dati sono stati oggetto di Data Breach. Nell'esecuzione della valutazione di impatto, andranno tenuti in considerazione i seguenti elementi minimi: il tipo di violazione verificatosi che può influenzare il livello di rischio per gli individui coinvolti; la natura, la categoria e il volume dei dati; la facilità di identificazione delle persone; le conseguenze per gli individui coinvolti; la tipologia ed il numero di soggetti coinvolti.

3. Notifica al Garante

Eseguita la valutazione di impatto, qualora questa evidenzi un probabile danno verso le libertà ed i diritti dei soggetti i cui dati sono oggetto della violazione, il Titolare del trattamento di concerto con il DPO laddove nominato, procede alle attività rivolte alla notifica della violazione all'Autorità di controllo. In questo contesto, la notifica deve essere effettuata entro 72 ore dal momento dell'intercettazione del Data Breach.

4.Comunicazione agli Interessati

Qualora all'esito della valutazione di impatto, risultasse che la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, si rende necessario per il Titolare prevedere la comunicazione di detta violazione, con il supporto del DPO laddove nominato, anche a tutti gli interessati oggetto della stessa, senza ingiustificato ritardo al fine di mettere i soggetti Interessati nella condizione di porre in essere tutte le misure possibili per limitare gli effetti negativi della violazione.

5. Archiviazione della risposta finita

Il Titolare del trattamento ha la responsabilità di archivio delle documentazione relativa alle notifiche inviate all'Autorità Competenti ed agli Interessati.

MARSH RISK CONSULTING