Procedura “Gestione delle Violazioni di Dati Personali”

Emissione del documento		Approvazione del documento	
Responsabile Area giuridico-amministrativa del Settore Affari generali ARS	Data: 24/10/2022	Direzione ARS	Data: 24/10/2022

Data	Versione	Modifiche
24/10/2022	1.0	Predisposizione e approvazione prima versione del documento

Sommario

1 Scopo e Campo di applicazione

La presente procedura intende descrivere il processo adottato dall'Agenzia Regionale Sanitaria Marche (di seguito, il "Titolare" o l'"Organizzazione") per la gestione delle violazioni dei dati personali nel rispetto delle normative vigenti in materia di protezione dei dati personali.

Nello specifico, la presente procedura riguarda tutti gli incidenti di sicurezza che comportano, anche accidentalmente, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Lo scopo della procedura è quello di provvedere tempestivamente agli adempimenti necessari nel caso in cui si verifichi una presunta violazione di dati personali, nonché di dare istruzioni al personale circa le modalità di gestione di un episodio di violazione di dati personali, attribuendo responsabilità, funzioni e compiti. La procedura si applica quindi a tutto il personale dell'Organizzazione, nonché a tutti i soggetti che a diverso titolo svolgono attività di trattamento di dati personali per l'Organizzazione, indipendentemente dalla modalità di trattamento (informatica o cartacea).

2 Definizioni

Termine	Definizione
Autorità di controllo	Autorità pubbliche indipendenti incaricate nei singoli Paesi UE di sorvegliare l'applicazione del GDPR al fine di tutelare i diritti e le libertà fondamentali degli interessati (in Italia, il Garante per la protezione dei dati personali).
Data Protection Officer o "**DPO**"	Responsabile della protezione dei dati di cui agli artt. 37-39 del GDPR.
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.
General Data Protection Regulation o "**GDPR**"	Regolamento (UE) 2016/679 del 27 aprile 2016 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.
Incidente di Sicurezza	Un singolo o una serie di non voluti o inaspettati eventi di sicurezza che hanno un'alta probabilità di compromettere le attività dell'Organizzazione e di minacciare la sicurezza delle informazioni ed in particolare la loro riservatezza, integrità e disponibilità.
Interessati	Persone fisiche a cui si riferiscono i dati personali.
Linee Guida dell'ex WP29 (oggi "EDPB") sul data breach	Linee guida in materia di notifica di un data breach adottate dall'ex WP29 (oggi "European Data Protection Board" o "EDPB") il 3 Ottobre 2017, come riviste e adottate il 6 Febbraio 2018 ("*Guidelines on Personal data breach notification under Regulation 2016/679*" - WP250rev.01).

Termine	Definizione
Provvedimento del Garante per la protezione dei dati personali	Provvedimento sulla notifica delle violazioni dei dati personali (data breach) adottato dal Garante italiano per la protezione dei dati personali il 30 luglio 2019.
Responsabile dei sistemi e dei servizi informativi	Risorsa esperta e responsabile del sistema informatico utilizzato per il trattamento dei dati personali.
Referente per la sicurezza dei sistemi informatici	Risorsa esperta nella sicurezza dei sistemi informatici utilizzati per la creazione e la gestione dei documenti e per il trattamento dei dati personali
Referente per la gestione della convenzione con la Regione Marche per l'utilizzo e la gestione dei sistemi e servizi informatici regionali	Risorsa esperta per la gestione degli aspetti tecnici e operativi inerenti all'utilizzo e la gestione dei sistemi e servizi informatici regionali
Esperto Informatico a supporto del DPO	Risorsa esperta che supporta il DPO nella classificazione e analisi dell'incidente coordinandosi con le risorse esperte, interne all'ARS, in materia di sistemi informativi e informatici
Responsabile dell'Area giuridico-amministrativa	Risorsa esperta e responsabile dell'Area giuridico-amministrativa dell'Organizzazione, individuata dal Titolare per il coordinamento di tutti gli aspetti legati alla protezione dei dati personali, nel rispetto delle norme applicabili in materia.
"Gruppo per la gestione delle violazioni di dati personali" o "Gruppo di risposta"	Gruppo coordinato dal Responsabile dell'Area giuridico-amministrativa del Settore Affari Generali ARS e composto, oltreché dal responsabile stesso, dal referente per la gestione della convenzione con la Regione Marche per l'utilizzo e la gestione dei sistemi e servizi informatici regionali o da un suo delegato, dal referente della sicurezza dei sistemi informatici, dal Dirigente del settore HTA, tecnologie biomediche e sistemi informativi o da un suo delegato, dall'esperto informatico a supporto del DPO, nonché dal DPO, per l'analisi e classificazione dell'incidente.
Referente Interno del trattamento	Persone fisiche cui sono attribuiti dal Titolare specifici compiti e funzioni connessi al trattamento di dati personali, nell'ambito del Settore che dirigono o della Posizione Organizzativa di cui sono responsabili, nel rispetto degli artt. 29 del GDPR e 2-*quaterdecies* del D.Lgs. 196/2003, come modificato e adeguato al GDPR dal D.Lgs. 101/2018.
Responsabile del Trattamento	Persona fisica o giuridica, autorità pubblica, servizio o altro organismo che tratta dati personali per conto del Titolare del Trattamento ai sensi dell'art. 28 del GDPR.
Soggetti autorizzati al trattamento	Persone fisiche espressamente autorizzate a compiere operazioni di Trattamento dall'Organizzazione e che agiscono sotto la diretta autorità di questa ultima, che sono state appositamente designate e istruite dal Titolare ai sensi degli artt. 29 del GDPR e 2-*quaterdecies* del D.Lgs. 196/2003, come modificato e adeguato al GDPR dal D.Lgs. 101/2018.

Termine	Definizione
Titolare del trattamento o "Titolare"	Persona fisica o giuridica, autorità pubblica, 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.
Trattamento di dati personali	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.
Violazione di dati personali o "**data breach**"	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
Accountability	Principio cardine della disciplina vigente in materia di protezione dei dati personali (art. 5 par. 2 GDPR), per cui il Titolare è tenuto a mettere in atto misure tecniche e organizzative adeguate ed efficaci a tutelare i diritti e le libertà degli interessati, avendo la responsabilità di ogni trattamento dei dati effettuato, oltre all'essere in grado di dimostrare la conformità delle attività previste dalla disciplina, compresa la stessa efficacie delle misure adottate.

3 Requisiti normativi

Requisito	Descrizione
Obbligo di notifica di un Data Breach (art. 33 par.1 GDPR)	Il GDPR introduce l'obbligo, in capo a tutti i Titolari del trattamento, di notificare alla competente autorità di controllo l'eventuale violazione dei dati personali subita, "*senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza*". Qualora la notifica all'autorità di controllo competente non sia effettuata entro 72 ore, è corredata dei motivi del ritardo. L'obbligo non sussiste qualora sia "*improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche*".
Obbligo di notifica al Titolare da parte del Responsabile (art. 33 par.2 GDPR)	Il Responsabile è tenuto ad informare il Titolare, senza ingiustificato ritardo, di una eventuale violazione dei dati che sta trattando per conto del Titolare, dopo esserne venuto a conoscenza.
Obbligo di comunicazione agli interessati (art. 34 GDPR)	La violazione dei dati personali deve essere comunicata senza ingiustificato ritardo anche agli interessati i cui dati personali sono stati coinvolti nella violazione laddove sia "suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche".

4 Descrizione delle attività

4.1 Rilevazione dell'incidente di sicurezza e Gruppo di risposta

Qualsiasi Soggetto Autorizzato al trattamento, anche per il tramite del proprio Referente, che rilevi direttamente o venga a conoscenza tramite terzi di un incidente di Sicurezza è tenuto a comunicarlo tempestivamente, a mezzo e-mail, entro e non oltre le 12 ore, al *"Gruppo per la gestione delle violazioni di dati personali"* o *"Gruppo di risposta"* ovvero il Gruppo coordinato dal **Responsabile dell'Area giuridico-amministrativa** e, costituito dallo stesso, dal **referente** per la gestione della convenzione con la Regione Marche per l'utilizzo e la gestione dei sistemi e servizi informatici regionali o **da un suo delegato**, dal **referente** della sicurezza dei sistemi informatici, dal Dirigente del settore HTA, tecnologie biomediche e sistemi informativi o **da un suo delegato**, dall'esperto informatico a supporto del DPO, nonché dal DPO, per l'analisi e classificazione dell'incidente nonché dal **DPO**, per l'analisi e classificazione dell'incidente.

Il *"Gruppo per la gestione di violazioni di dati personali"* può essere implementato di volta in volta da ulteriori professionalità interne o figure qualora, avuto riguardo alla tipologia ed alla natura della eventuale violazione riscontrata, la suddetta violazione veda coinvolte altre strutture o richieda specifiche competenze.

4.2 Analisi e classificazione dell'incidente di sicurezza come Violazione di dati

Il *Gruppo di Risposta*, per le rispettive aree di competenza, si occupa di:

- individuare e prendere in carico gli incidenti di sicurezza nelle modalità già previste dall'Organizzazione per la gestione di incidenti nei diversi ambiti, tenendo adeguatamente traccia delle segnalazioni e delle modalità di gestione;
- acquisire gli elementi necessari per confermare (o escludere) che l'incidente di sicurezza costituisca una Violazione di dati personali, tenuto conto che una Violazione di dati personali può riguardare, congiuntamente o disgiuntamente, la riservatezza, la disponibilità, l'integrità dei dati o la resilienza dei sistemi su cui sono conservati i dati. A tal fine, al fine di meglio comprendere il contesto, le cause e le conseguenze della violazione, è riconosciuto un ampio potere di verifica;
- quando ha un ragionevole grado di certezza che l'incidente di sicurezza abbia coinvolto dati personali, qualificare l'incidente come "Violazione di dati personali";
- da questo momento, ovvero dal momento in cui si è venuti a conoscenza della Violazione di dati personali, decorre il termine per l'eventuale notifica all'Autorità di Controllo, che in ogni caso non deve superare le 72 ore.

Qualificato l'incidente come "Violazione di dati personali", il *Gruppo di Risposta*, a prescindere dall'eventuale notifica, si occupa di registrare la violazione nell'apposito Registro, occupandosi di:

- effettuare una valutazione della probabilità e gravità del rischio per i diritti e le libertà degli interessati derivanti dalla violazione di dati personali;
- definire un piano di gestione della violazione, comprensivo di: azioni volte a mitigare gli impatti negativi della violazione, valutazione sulla notifica della violazione all'Autorità di Controllo ed eventuale comunicazione della violazione agli interessati;
- proporre l'adozione di misure volte a mitigare gli impatti negativi della violazione ed evitare che l'evento si ripeta in futuro, documentando e riportando costantemente l'esito delle azioni svolte.

Laddove la Violazione di dati personali sia posta in essere da un Responsabile ex art. 28 GDPR, il Titolare può richiedere ogni documentazione inerente alla gestione della violazione stessa ed effettuare degli audit di verifica.

4.3 Notifica della violazione all'Autorità di Controllo

La notifica[1] della violazione all'Autorità di Controllo è obbligatoria, a meno che il *Gruppo di Risposta*, sentito il parere del DPO, ritenga improbabile la sussistenza di un grave rischio per i diritti e le libertà degli interessati. In caso di rischio non improbabile, il *Gruppo di Risposta* predispone la notifica utilizzando il modello previsto dall'Autorità Garante e il DPO la revisiona per approvazione. Il Titolare, con il supporto del DPO, procede successivamente all'invio della notifica all'Autorità di Controllo. La notifica, almeno preliminare, deve essere effettuata senza ingiustificato ritardo e, comunque, entro 72 ore; qualora non sia effettuata **entro le 72 ore**, la stessa dovrà essere corredata con le motivazioni del ritardo.

4.4 Comunicazione della violazione agli Interessati

In caso di violazione "suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche" [2], il *Gruppo di Risposta* si occupa di valutare, in base alla numerosità e tipologia degli interessati, nonché in relazione alla natura della violazione e dei dati compromessi, il contenuto della comunicazione[3] agli interessati e stabilire le relative modalità di invio:

- trasmissione di una comunicazione personale agli interessati attraverso il mezzo considerato più idoneo (es. posta ordinaria, posta elettronica, SMS, Messaggi, …)[4]; oppure
- comunicazione pubblica, o simile, sui media ritenuti più idonei sulla base della tipologia degli interessati da raggiungere (es. siti istituzionali dell'Organizzazione, giornali, televisioni, radio o altro), ma solo quando la comunicazione individuale agli interessati richiederebbe sforzi sproporzionati.

Il *Gruppo di Risposta* predispone il draft della comunicazione e il DPO la revisiona per approvazione. Di conseguenza, il Titolare invia la comunicazione agli interessati secondo le modalità definite e gestisce successivamente il rapporto con gli stessi.

4.5 Chiusura della violazione di dati personali

Il *Gruppo per la gestione della violazione dei dati personali*, con il supporto del DPO, si occupa di:

- aggiornare il "Registro delle violazioni sui dati personali";
- monitorare eventuali conseguenze della violazione;
- prevedere la conservazione e l'archiviazione della documentazione relativa alla violazione[5].

[1] La notifica deve almeno: 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; 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; descrivere le probabili conseguenze della violazione dei dati personali; 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.

[2] Non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni: l'Organizzazione 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; l'Organizzazione 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.

[3] La comunicazione deve almeno: descrivere in linguaggio chiaro e semplice della natura della violazione; comunicare il nome e i dati di contatto del DPO o di altro punto di contatto; descrivere le probabili conseguenze della violazione dei dati personali; 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] Al fine di rendere la comunicazione chiara e trasparente dovrebbero essere utilizzati messaggi dedicati a tal scopo, evitando di inserire l'informazione sulla Violazione all'interno di altre comunicazioni agli interessati, come newsletter (Linee Guida dell'ex WP29 sul Data Breach).

[5] Durante l'intera gestione della crisi e dopo l'uscita della crisi, il Titolare del trattamento deve fornire e mantenere una traccia cartacea della violazione di dati personali che indica il suo contesto, i suoi effetti e le misure adottate per porre rimedio. Questo documento sarà giuridicamente vincolante e potrà essere fatto valere nei casi di controllo del Garante per la protezione dei dati personali.

5 Metodologia e strumenti

5.1 Determinazione del rischio per i diritti e libertà degli interessati

Il considerando 75 del GDPR precisa che esiste un "rischio" per i diritti e le libertà delle persone fisiche se il trattamento può cagionare un danno fisico, materiale o immateriale, agli interessati, inclusi discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione o qualsiasi altro danno economico o sociale significativo.

Il considerando 76 prevede che il rischio debba essere valutato secondo un'analisi oggettiva riguardo natura, ambito di applicazione, contesto e finalità di trattamento.

Come raccomandato dall'ex WP29, nel valutare il rischio derivante da una violazione, il titolare del trattamento dovrebbe considerare tanto la gravità dei potenziali impatti sui diritti e le libertà degli interessati, quanto la probabilità che gli stessi si verifichino. Il Gruppo dei Garanti precisa: "*se le conseguenze di una violazione sono più gravi, il rischio è più elevato; analogamente, se la probabilità che tali conseguenze si verifichino è maggiore, maggiore è anche il rischio*".

L'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) ha elaborato raccomandazioni in merito a una metodologia di valutazione della "gravità di una violazione" che possono essere utili per i titolari e i responsabili del trattamento nella progettazione del loro piano di risposta per la gestione delle violazioni, che si rimette in allegato alla presente procedura. Secondo tale metodologia, la gravità di un *data breach* è la "*stima della rilevanza del potenziale impatto sugli individui derivante dal data breach*".

5.2 Determinazione della necessità di effettuare la Notifica all'Autorità di Controllo

L'obbligo di notifica all'Autorità di Controllo non sussiste qualora sia "*improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche*". La valutazione che deve essere effettuata è dunque relativa alla probabilità che tale rischio sussista, indipendentemente dall'entità dell'impatto sugli interessati.

In ogni caso, laddove l'impatto per gli interessati sia del tutto trascurabile, il Titolare potrebbe valutare non necessaria la notifica.

5.3 Determinazione della necessità di effettuare la Comunicazione agli Interessati

La Comunicazione agli interessati è obbligatoria se "*la violazione di dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche*". Resta inteso che nel caso in cui il Titolare abbia già effettuato la Notifica all'Autorità di Controllo, la sussistenza di tale rischio è già stata valutata come probabile. Per questo motivo, nel determinare la necessità di effettuare una Comunicazione agli interessati, il Titolare deve valutare, non già la probabilità di realizzazione del rischio, ma la gravità dell'impatto potenziale, che deve essere tale da determinare un rischio elevato per i diritti e le libertà degli interessati.

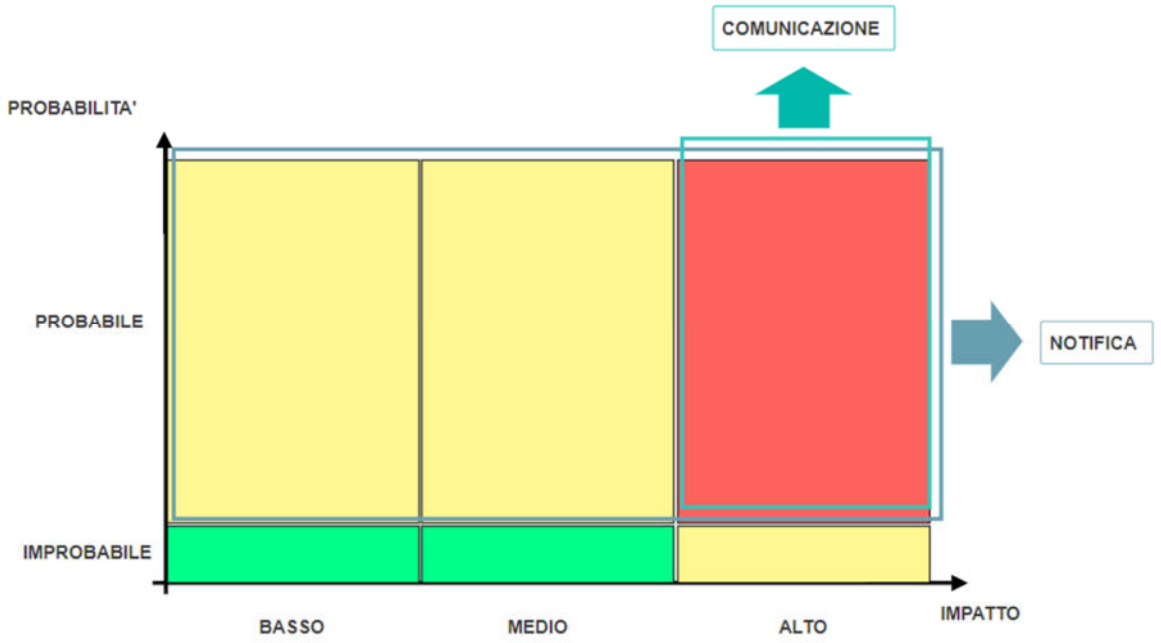
In particolare, si ritiene la gravità del rischio direttamente proporzionale alla gravità della violazione. Laddove non siano state individuate condizioni di "impatto elevato", non è comunque possibile escludere a priori la sussistenza di un rischio elevato per l'interessato. In questi casi, è necessario:

- valutare se la probabilità sia estremamente elevata (e, di conseguenza, l'evento sia presumibilmente "certo"): in tal caso, anche laddove l'impatto non sia significativo, il Titolare deve riconsiderare con attenzione se il rischio a cui sono esposti i diritti e le libertà degli interessati risulti complessivamente elevato.
- considerare con maggiore precisione l'estensione della violazione: infatti, anche quando l'impatto su un singolo interessato potrebbe essere limitato, se la violazione dovesse coinvolgere un numero elevato di interessati, l'incidente potrebbe comunque comportare un rischio elevato. Ad esempio, un attacco informatico che sottrae esclusivamente dati anagrafici correlati agli indirizzi e-mail degli interessati potrebbe essere valutato ad impatto

trascurabile, ma se gli interessati fossero migliaia, queste informazioni potrebbero essere utilizzate per campagne di phishing con conseguenze anche gravi per tutte le vittime;

- laddove, eseguendo gli step sopra descritti e documentandone i razionali, il rischio continua ad essere non elevato, è possibile concludere che non sussista "un rischio elevato per i diritti e le libertà delle persone fisiche".

Si precisa tuttavia che nel caso in cui sia difficile valutare se un rischio sia effettivamente elevato, è comunque preferibile effettuare la Comunicazione agli interessati, in quanto potrebbe consentire loro di evitare o mitigare il danno derivante dalla violazione.



Legenda:

- Rischio elevato
- Rischio non elevato
- Rischio non significativo

6 Responsabilità disciplinare in caso di violazione della presente procedura

A seguito della approvazione della presente procedura, verranno organizzate sessioni formative, di concerto con il DPO e del comparto dirigenziale al fine di formare e responsabilizzare al meglio il personale, nel rispetto del principio di *Accountability*.

Una volta concluso il percorso formativo, la stessa sarà a tutti gli effetti una procedura interna con valore di regolamentazione e, in quanto tale, passibile di valutazione disciplinare, così come previsto per ogni violazione delle procedure interne.

7 Allegati

Gli strumenti utili e complementari nell'esecuzione delle attività sopra descritte sono i seguenti:

Nome	Descrizione	Allegato
Tipologie di violazioni	Documento che descrive le tipologie di violazioni di dati personali	Allegato 1
Tipologie di evento	Documento che descrive le tipologie di eventi che possono generare una violazione dei dati personali	Allegato 2
Fattori da considerare quando si valuta il rischio	Documento che descrive i fattori da considerare quando si valuta il rischio per i diritti e le libertà per le persone fisiche	Allegato 3
Modulo di notifica all'Autorità di Controllo	Modulo da utilizzare per effettuare la notifica al Garante	Allegato 4
Registro delle Violazioni	Documento in cui inserire i dettagli relativi alle violazioni di dati personali.	Allegato 5

8 Scheda di sintesi della procedura "Gestione delle Violazioni di Dati Personali":

Chi deve segnalare?	Chiunque ne venga a conoscenza
A chi si deve segnalare?	Al *"Gruppo per la gestione delle violazioni di dati personali"* o *"Gruppo di Risposta"* coordinato dal **Responsabile dell'Area giuridico-amministrativa del Settore Affari Generali ARS** e, composto, oltreché dal responsabile stesso, dal **referente** per la gestione della convenzione con la Regione Marche per l'utilizzo e la gestione dei sistemi e servizi informatici regionali o **da un suo delegato**, dal **referente** della sicurezza dei sistemi informatici, dal Dirigente del settore HTA, tecnologie biomediche e sistemi informativi o **da un suo delegato**, dall'esperto informatico a supporto del DPO, nonché dal DPO, per l'analisi e classificazione dell'incidente.
Come segnalare?	Preferibilmente mediante comunicazione scritta trasmessa via e-mail o, comunque, laddove non è

	possibile, procedere immediatamente anche telefonicamente o di persona. A tal fine, la segnalazione può essere trasmessa ai seguenti indirizzo mail: affarigeneraliars@regione.marche.it; dpo.ars@regione.marche.it;
Quando segnalare?	Tempestivamente, e comunque non oltre le 12 ore dalla presa di conoscenza dell'evento che potrebbe aver dato luogo ad una possibile violazione di dati personali.
Quando effettuare la notifica all'Autorità?	Quando il *Gruppo di risposta* ritenga probabile la sussistenza di un grave rischio per i diritti e le libertà degli interessati, il Titolare, con il supporto del DPO, procede all'invio della notifica all'Autorità di Controllo. La notifica, almeno preliminare, deve essere effettuata entro 72 ore dalla conoscenza della violazione.
Quando effettuare la comunicazione agli Interessati?	In caso di violazione "suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche", il *Gruppo di risposta* valuta il contenuto della comunicazione e le relative modalità di invio. Una volta approvate, il Titolare invia la comunicazione.
Quando va registrata la violazione dei dati?	Sempre, a prescindere dalla notifica e/o dalla comunicazione.
Cosa succede se violo la procedura?	Dopo apposita formazione, la presente procedura avrà a tutti gli effetti valore di regolamento aziendale, pertanto la violazione può provocare un provvedimento disciplinare.