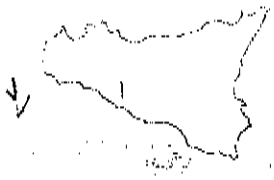


63Regione Siciliana

Azienda Sanitaria Provinciale di

AGRIGENTO

DELIBERAZIONE DIREZIONE GENERALE N. 1073 DEL 11 NOV. 2019

OGGETTO: Adempimenti in applicazione del Regolamento UE 2016/679 – Approvazione procedura aziendale per la gestione delle violazioni dei dati personali (Data Breach) ai sensi dell'art. 33 del Regolamento.

STRUTTURA PROPONENTE: Direzione Generale – Ufficio Privacy

PROPOSTA N. 1342 DEL 04/11/2019

Il Responsabile del procedimento
Dott.ssa Maria Giovanna Matteliano

Il Responsabile delle Protezione dei dati
Dott. Antonino Fiorentino

VISTO CONTABILE

Si attesta la copertura finanziaria:
( ) come da prospetto allegato (ALL. N. _____) che è parte integrante della presente delibera.

Non comporta ordine di spesa

( ) Autorizzazione n. _____ del _____ C.E. _____ / C.P. _____

IL RESPONSABILE DEL PROCEDIMENTO

IL DIRETTORE U.O.S.E.P.
Il Direttore U.O. Patrimonio
Dr. Antonino Lo Valle

Da notificare a: Direzione Generale- Ufficio Privacy

RICEVUTA DALL'UFFICIO ATTI DELIBERATIVI IN DATA 05-11-2019

L'anno duemiladiciannove il giorno UNDICI del mese di NOVEMBRE nella sede dell'Azienda Sanitaria Provinciale di Agrigento

IL DIRETTORE GENERALE

Dott. Giorgio Giulio Santonocito, nominato con Decreto del Presidente della Regione Siciliana n.186/Serv.1/S.G. del 04/04/2019, coadiuvato dal Direttore Amministrativo, dott. Alessandro Mazzara, nominato con delibera n. 414 del 17/06/2019 e dal Direttore Sanitario, dott. Gaetano Mancuso, nominato con delibera n. 415 del 17/06/2019, con l'assistenza del Segretario verbalizzante Dott.ssa PATRIZIA TEDESCO adotta la presente delibera sulla base della proposta di seguito riportata.

PROPOSTA

Il Responsabile della Protezione dati (DPO) Dott. Antonino Fiorentino

Visto l'Atto Aziendale di questa ASP, adottato con delibera n. 667 del 03/05/2017 ed approvato con D.A. n. 1082 del 30/05/2017, di cui si è preso atto con Delibera n. 816 del 09/06/2017;

Premesso :

- Che il Regolamento (UE) 2016/679 – denominato "Regolamento generale sulla protezione dei dati", in sigla RGPD – detta una nuova disciplina in materia di trattamento dei dati personali, prevedendo tra gli elementi caratterizzanti e innovativi il "principio di responsabilizzazione" (c.d. accountability) e ponendo al centro del nuovo quadro normativo nuovi adempimenti, tra cui quelli previsto dagli artt. 33 e 34 del Regolamento (UE) 2016/679, e segnatamente quello relativo all'adozione di una specifica procedura disciplinante la gestione delle violazioni dei dati personali ("data breach");

Evidenziato

- che l'art.33 del GPDR recita " In caso di violazioni di dati personali, il Titolare del Trattamento notifica la violazione all'autorità di controllo competente a norma dell'art. 55 senza ingiustificato ritardo e, ove possibile, entro le 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.
- che ai sensi dell'art.34 del GDPR, 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 deve comunicare la violazione all'interessato senza ingiustificato ritardo;

Considerato

- che per violazione dei dati personali si intende una situazione in cui i dati personali, sensibili, protetti o riservati vengono: distrutti, consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato e la mancata notifica può comportare ulteriori accertamenti da parte del Garante poiché può rappresentare un indizio di carenze che, se accertate, possono dar luogo a sanzioni;
- Che per quanto sopra, si constata l'esigenza di predisporre una procedura organizzativa interna per la gestione di eventuali violazioni concrete, potenziali o sospette di dati personali per adempiere agli obblighi imposti dalla normativa europea ed evitare rischi per i diritti e le libertà degli interessati, nonchè danni economici per l'Azienda Sanitaria Provinciale di Agrigento, significando che, dette violazioni di dati personali sono gestite dal Titolare del trattamento, per il tramite del Responsabile della Protezione Dati;

Ritenuto

- pertanto, necessario approvare la procedura per la gestione e notifica dei data Breach che comprende il flusso degli adempimenti in caso di presunta o accertata violazione di dati personali degli incidenti di sicurezza, che copre le seguenti fasi:

  Rilevazione e segnalazione del data breach;
  Analisi del data breach;
  Risposta e notifica del data breach;
  Registrazione del data breach.

Richiamata
la Deliberazione del Commissario Straordinario n° 311 del 21/02/2019 è stata formalizzata l'adesione al Contratto quadro SPC Cloud- lotto 4 sottoscritto tra RTI Almaviva SPA/Almawave srl./Indra Italia Spa/Pricewaterhouse Coopers Advisory Spa, (fornitore)- approvazione progetto dei fabbisogni Asp Agrigento per le attività di supporto e professionali per l'adeguamento al GDPR, considerata la mole e la qualità dei dati ordinatoriamente trattati da questa ASP;

Dato atto
Che, la procedura approvata con il presente provvedimento, elaborata dal Team RTI Almaviva SPA/Almawave srl./Indra Italia Spa/Pricewaterhouse Coopers Advisory Spa e verificata dall'Ufficio Privacy aziendale, sarà soggetta ad aggiornamento costante, anche in funzione di eventuali criticità riscontrate in sede di prima applicazione;

PROPONE

Per le motivazioni espresse in premessa che si intendono qui riportate:

- **Di approvare** la procedura per la gestione e notifica dei data Breach, elaborata dal Team RTI Almaviva SPA/Almawave srl./Indra Italia Spa/Pricewaterhouse Coopers Advisory Spa e verificata dall'Ufficio Privacy aziendale , che comprende il flusso degli adempimenti in caso di presunta o accertata violazione di dati personali degli incidenti di sicurezza, che copre le seguenti fasi:
  - Rilevazione e segnalazione del data breach;
  - Analisi del data breach;
  - Risposta e notifica del data breach;
  - Registrazione del data breach.
- **Di precisare** la procedura approvata con il presente provvedimento, elaborata dal Team RTI Almaviva SPA/Almawave srl./Indra Italia Spa/Pricewaterhouse Coopers Advisory Spa e verificata dall'Ufficio Privacy aziendale, sarà soggetta ad aggiornamento costante, anche in funzione di eventuali criticità riscontrate in sede di prima applicazione
- **Di notificare** il presente provvedimento a tutte le strutture aziendali tramite la pubblicazione sul sito web aziendale, Sezione Privacy, nonché in tutte le sedi dell'Azienda Sanitaria Provinciale di Agrigento;
- **Munire** il presente atto della clausola di immediata esecutività, attesa la necessità di provvedere con l'urgenza del caso;
- **Che** l'esecuzione della deliberazione verrà curata dalla Direzione Generale – Ufficio Privacy;
- **Attesta,** altresì, che la presente proposta, a seguito dell'istruttoria effettuata, nella forma e nella sostanza, è legittima e pienamente conforme alla normativa che disciplina la fattispecie trattata.

Dott. Antonino Fiorentino
Responsabile della Protezione dati

SULLA SUPERIORE PROPOSTA VENGONO ESPRESSI

Parere favorevole
Data 07/11/2019

Il Direttore Amministrativo
Dott. Alessandro Mazzara

Parere favorevole
Data 07/11/2019

Il Direttore Sanitario
Dott. Gaetano Mancuso

IL DIRETTORE GENERALE

Vista la superiore proposta di deliberazione, formulata dal Responsabile della Protezione dei Dati Dott. Antonino Fiorentino, a seguito dell'istruttoria effettuata, nella forma e nella sostanza, ne ha attestato la legittimità e la piena conformità alla normativa che disciplina la fattispecie trattata;

Ritenuto di condividere il contenuto della medesima proposta;

Tenuto conto dei pareri espressi dal Direttore Amministrativo e dal Direttore Sanitario;

DELIBERA

di approvare la superiore proposta, che qui si intende integralmente riportata e trascritta, per come sopra formulata e sottoscritta dal dott. Antonino Fiorentino Responsabile della Protezione dati.

Il Direttore Amministrativo
Dott. Alessandro Mazzara

Il Direttore Sanitario
Dott. Gaetano Mancuso

IL DIRETTORE GENERALE
Dott. Giorgio Giulio Santonocito

Il Segretario verbalizzante
IL TITOLARE DI POSIZIONE ORGANIZZATIVA
UFFICIO DI SEGRETERIA PROPOSTE
DI ATTI E AMMA
Dott.ssa Patrizia Tedesco

ALL. A

Processo di gestione e notifica

dei *data breach*

Il Direttore Generale
dell'ASP di Agrigento
Dott. Giorgio Giulio Santonocito

1. INTRODUZIONE

1.1 SCOPO DEL DOCUMENTO

Il Regolamento Europeo 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali ha introdotto l'obbligo, in capo al Titolare del trattamento, di notificare all'Autorità di Controllo la violazione dei dati personali 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 libertà delle persone fisiche cui i dati violati si riferiscono.
Nel caso in cui la suddetta violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento deve comunicare la violazione senza ingiustificato ritardo anche agli interessati stessi.

L'art. 4 comma 12 del disposto normativo definisce la "Violazione dei Dati Personali" come "*violazione della 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, memorizzati o comunque trattati*".

Pertanto, per *data breach*, ai fini del presente documento, si intende qualunque incidente di sicurezza che comporta la compromissione dei dati personali trattati da ASP Agrigento mediante il supporto di strumenti elettronici (*e.g. database*, applicazioni, *tool*, etc.), e / o fisici (*e.g.* documentazione cartacea).

Sulla base delle *Guidelines* ENISA (European Network and Information Security Agency) le violazioni dei dati personali (di seguito anche "data breach") sono classificate in 6 tipologie:

- *Unauthorized access:* accesso ai dati da parte di soggetti (interni o esterni) non aventi diritto;
- *Loss:* indisponibilità temporanea dei dati;
- *Destruction:* indisponibilità irreversibile dei dati;
- *Transmission:* comunicazione (fortuita o intenzionale) dei dati verso destinatari non autorizzati;
- *Alteration or Modification:* modifica impropria (accidentale o intenzionale) dei dati;
- *Disclosure:* divulgazione impropria di informazioni riservate.

Inoltre, il WP29 spiega come i *data breach* possano essere categorizzati sulla base dei parametri di Information security compromessi. Pertanto, è possibile distinguere tra:

- "Violazione della riservatezza" - in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali.
- "Violazione della disponibilità" - in caso di perdita accidentale o non autorizzata di accesso o distruzione di dati personali.
- "Violazione dell'integrità" - in caso di alterazione non autorizzata o accidentale dei dati personali.

Scopo del presente documento è descrivere il processo operativo di cui si è dotata ASP Agrigento in merito alla gestione, l'analisi e la notifica delle violazioni di dati personale all'Autorità di Controllo ed agli interessati, laddove necessario, in conformità a quanto disposto dalla normativa sopra citata.
Nel caso in cui il *data breach* si configuri come incidente di sicurezza informatica, tale processo sarà prontamente avviato contestualmente al processo operativo di Gestione degli Incidenti di Sicurezza, in capo ai Sistemi Informativi di ASP Agrigento, ente aziendale preposto alla gestione di tali incidenti.

Il documento è valido per tutti quei trattamenti di cui ASP Agrigento è titolare del trattamento.

1.2 TERMINI E DEFINIZIONI

Attore	Divisione / Dipartimento / Area di ASP Agrigento coinvolta nei task della Procedura
Autorità di Controllo	Autorità dello stabilimento principale del Titolare del Trattamento. In Italia corrisponde al Garante per la protezione dei dati personali
Data breach	*(def. ENISA)* Illecito perpetrato sul patrimonio informativo aziendale conservato o, comunque trattato, mediante supporti elettronici e / o fisici, così categorizzabile: *Accesso non autorizzato, Rivelazione, Modifica o Alterazione, Perdita, Distruzione*
Data Leak	Trasferimento non autorizzato di informazioni da un dispositivo elettronico verso l'esterno
Disponibilità	Proprietà del dato di essere presente e utilizzabile nei tempi, nei luoghi e nelle modalità adeguati alle necessità operative aziendali
ENISA	*European Network and Information Security Agency*
Evento di sicurezza	Qualsiasi occorrenza anomala in ambito Sicurezza IT che non sia un falso positivo ed osservabile sia attraverso piattaforme di monitoraggio sia attraverso interazioni umane e che, a valle di una fase di triage, può essere identificata come incidente di sicurezza
Falso positivo	Evento che si rivela, dopo attenta analisi, non impattante in termini di sicurezza
GP	*Garante Privacy*
HW	*Hardware*
IDS	*Intrusion Detection System*
IPS	*Intrusion Prevention System*
Impatto	Effetto causato dall'avvenuta violazione della sicurezza sugli asset ICT e/o sul patrimonio informativo aziendale
Incidente di sicurezza	• Violazione o una potenziale violazione dei requisiti di RID del patrimonio informativo aziendale che possono impattare Informazioni/Sistemi/Applicazioni/Pacchetti Applicativi • qualsiasi violazione o minaccia di violazione di policy aziendali • comportamenti definiti e codificati che possono configurare un illecito informatico

Integrità	Proprietà del dato di essere presente, corretto e valido. L'integrità viene valutata secondo tre elementi caratterizzanti: • la completezza, cioè il dato deve essere presente nella sua totalità • l'accuratezza, ovvero ogni elemento del dato deve essere privo di errori al momento del suo ingresso nel sistema • la validità, ovvero il dato deve derivare da processi elaborativi validi ed autorizzati
Minaccia	Tipo di azione, sia deliberata che accidentale, che può in qualsiasi modo arrecare direttamente o indirettamente un danno all'integrità, alla riservatezza o disponibilità di un dato
RID	Riservatezza - Integrità - Disponibilità
Rilevazione	Qualsiasi segnalazione di potenziale evento di sicurezza o occorrenza osservabile in un sistema o rete
Riservatezza	Proprietà del dato di essere conoscibile solo ad alcuni soggetti, normalmente individuati dal "proprietario" del dato stesso e non ad altri
SW	Software
WP29	Organismo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro dell'Unione Europea, dal GEPD (Garante europeo della protezione dei dati), nonché da un rappresentante della Commissione Europea
Autorizzato	La persona fisica autorizzata a compiere operazioni di trattamento dal Titolare o dal Responsabile
Interessato	La persona fisica cui si riferiscono i dati personali
Delegato interno del trattamento	Sono le persone fisiche cui, all'interno della propria struttura, il Titolare ha assegnato ruoli che comportano il coordinamento di attività di trattamento di dati personali. Corrispondono ai responsabili dei Dipartimenti/Direttori dei Presidi Ospedalieri di ASP Agrigento al cui interno sono previsti processi che comportano il trattamento di dati personali. Per tali soggetti è prevista la programmazione e l'erogazione di piani di formazione in materia di protezione e tutela dei dati personali costante e sistematica.

DPO	Data Protection Officer Ha il compito di informare e fornire consulenza al Titolare, sorvegliare l'osservanza della normativa in materia di protezione dei dati personali e fornire, ogniqualvolta richiesto, un parere in merito agli adempimenti in materia di protezione dei dati personali, quali, a titolo esemplificativo, DPIA, Privacy by Design, gestione richieste interessati, misure di sicurezza, etc
Titolare del trattamento	La persona fisica o giuridica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali
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

1.3 DOCUMENTAZIONE DI RIFERIMENTO

[1] Regolamento Europeo 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, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

[2] Article 29 Data Protection Working Party – Guidelines on Personal Data breach Notification under Regulation 2016/679 Adopted on 3 October 2017

[3] GUIDELINES ENISA – "Recommendations on technical implementation guidelines of Article 4"

[4] ENISA – "Data breach notifications in the EU"

[5] Procedura di Gestione degli eventi ed incidenti di sicurezza

2. PROCESSO DI GESTIONE DEL DATA BREACH

Il nuovo obbligo di notifica, come rilevato dal WP29, offre numerosi benefici ai Titolari del Trattamento.
Un'opportuna gestione del *data breach* può rappresentare uno strumento per incrementare la conformità in relazione alla protezione dei dati personali: comunicare una violazione all'Autorità di Controllo ed agli interessati consente infatti, al Titolare del Trattamento, di raccogliere e fornire informazioni circa i rischi scaturiti dalla violazione e le azioni che possono essere adottate per proteggersi dalle potenziali conseguenze.

In tale ottica, al fine di consentire una gestione efficace e tempestiva delle violazioni di dati personali, ASP Agrigento si è dotata di un processo strutturato che copre le seguenti fasi:

- Rilevazione e segnalazione del *data breach*;
- Analisi del *data breach*;
- Risposta e notifica del *data breach*;
- Registrazione del *data breach*.

Le suddette fasi corrispondono principalmente, nel caso in cui l'incidente di sicurezza sfrutti come vettore un *asset* informatico di ASP Agrigento, alle fasi previste dal processo di gestione degli eventi ed incidenti di sicurezza informatica. In tale evenienza, infatti, come rilevato in precedenza, il processo di gestione del *data breach*, oggetto della presente procedura, è prontamente attivato nel caso in cui, a valle di una fase di analisi e classificazione dell'incidente di sicurezza informatica occorso, emerga la fattispecie di violazione di dati personali.

2.1 RILEVAZIONE E SEGNALAZIONE DEL DATA BREACH

La rilevazione di una violazione di dati personali è attivata mediante molteplici canali, che prevedono il coinvolgimento di attori sia interni sia esterni ad ASP Agrigento.
Nello specifico, la rilevazione può avvenire:

- ad opera dei Sistemi Informativi attraverso le proprie attività di *security* mediante sistemi e *tool* di monitoraggio dell'infrastruttura ICT di ASP Agrigento;
- a partire dalle segnalazioni dei soggetti interni autorizzati al trattamento di dati personali in modalità sia cartacea sia elettronica (*e.g.* Autorizzati ai trattamenti);
- a partire dalle segnalazioni provenienti dagli utenti finali delle risorse ICT di ASP Agrigento, quali dipendenti e/o collaboratori, nello svolgimento delle attività a loro demandate;
- a partire dalle segnalazioni provenienti dagli interessati (*e.g.* clienti);
- a partire dalle segnalazioni provenienti da soggetti terzi, quali i fornitori di prodotti / servizi in *outsourcing* che sono stati debitamente nominati Responsabili esterni del Trattamento.

RILEVAZIONE DA PARTE DEI SISTEMI INFORMATIVI

Una violazione di dati personali, nel caso in cui sfrutti una vulnerabilità informatica, è da intendersi come una tipologia specifica di "incidente di sicurezza informatica". In tale ottica, la fase di *detection* di un *data breach* è strettamente connessa alla *detection* di un evento di *information security*.
Pertanto, gli strumenti utilizzati per il monitoraggio della rete ed i sistemi delle Postazioni di Lavoro (di seguito anche "PdL") degli utenti che consentono di rilevare un *data breach*, risultano essere gli stessi utilizzati da ASP Agrigento per la rilevazione degli eventi di sicurezza.
Tali sistemi di monitoraggio di sicurezza ICT consentono, dunque, di identificare eventi che possono comportare potenziali *data breach* relativi ai dati personali, come, ad esempio:

- violazioni rilevate dai sistemi di controllo accessi logici;
- violazioni rilevate da parte delle soluzioni di *intrustion detection* e *prevention* (IDS, IPS);
- violazioni rilevate da parte del sistema di *content filtering web* ed *email*;
- violazioni rilevate da parte delle soluzioni di sicurezza delle postazioni di lavoro (*antivirus*, *antimalware*, etc.);
- violazioni rilevate da parte delle soluzioni di sicurezza dei dispositivi mobili;
- violazioni rilevate da parte del *firewall*.

SEGNALAZIONI PROVENIENTI DA UTENTI, AUTORIZZATI, INTERESSATI E SOGGETTI TERZI

Tutto il personale interno ed i collaboratori di ASP Agrigento hanno il compito di segnalare eventuali eventi rilevanti per la sicurezza dei dati personali.
I soggetti interni cui è stata conferita la nomina ad Autorizzato, sono tenuti prontamente a segnalare al Delegato interno del trattamento competente eventuali anomalie che dovessero riscontrare nell'espletamento delle attività di trattamento di loro competenza.

La segnalazione deve contenere almeno le seguenti indicazioni:

- riferimenti di contatto dell'utente segnalante;
- tipologia e descrizione del *data breach*, ovvero breve descrizione delle circostanze e delle possibili conseguenze (*e.g.* diffusione impropria dei dati);
- numero approssimativo di dati e interessati coinvolti (ragionando, a titolo esemplificativo, sul numero indicativo di righe che compongono il file / documento oggetto di violazione);
- categorie di dati coinvolti nel *breach* e categorie di interessati coinvolti;
- eventuali azioni intraprese dopo l'evento (*e.g.* sostituzione della *password* di accesso);

- soggetti informativi del potenziale evento (*e.g.* altri colleghi o il proprio responsabile di Funzione / Direzione).

Allo stesso modo, le segnalazioni di potenziali *data breach* potrebbero pervenire da parte degli interessati stessi in caso, ad esempio, di ricezioni di email / chiamate anomale, in grado di generare il sospetto che soggetti terzi non autorizzati siano entrati / stiano tentando di entrare in possesso di dati personali, la cui titolarità ricade su ASP Agrigento.

Infine, terze parti, quali i fornitori designati da ASP Agrigento Responsabili del Trattamento, hanno il compito di segnalare eventuali eventi rilevanti per la sicurezza dei dati personali.
Nei contratti con i suddetti fornitori è chiaramente inserito l'obbligo in capo a questi ultimi di informare senza ingiustificato ritardo ASP Agrigento, in qualità di Titolare del trattamento, di ogni evento di violazione della sicurezza.
A tal proposito, le violazioni dei dati personali possono altresì verificarsi mediante lo sfruttamento di vettori di attacco fisici, pertanto, ASP Agrigento si è dotata di sistemi e soluzioni di sicurezza fisica.
I sistemi di sicurezza fisica presidiano in particolare le seguenti violazioni:

- violazioni della protezione perimetrale esterna e dei locali (anti-intrusione, allagamento, incendi, etc.);
- violazioni rilevate da sistemi di video-sorveglianza posti a protezione delle aree di accesso alle sedi.

Ciascuna tipologia di rilevazione deve essere presa in carico dal Delegato interno del trattamento di ASP Agrigento competente che procede, di concerto con il DPO e, in caso di incidente di sicurezza informatica, con i Sistemi Informativi, con le attività di analisi del *data breach*.

2.2 ANALISI DEL DATA BREACH

Poiché le attività di analisi potrebbero rivelarsi onerose sia dal punto di vista del tempo necessario ad eseguirle sia delle competenze interne a ASP Agrigento per raccogliere tutto il set informativo necessario, la fase di "Analisi" può essere suddivisa in due sotto-fasi:

- Analisi preliminare;
- Analisi di dettaglio.

ANALISI PRELIMINARE

Il Delegato interno del trattamento competente è innanzitutto tenuto a verificare che nell'evento di sicurezza rilevato siano stati effettivamente violati dati personali la cui titolarità è attribuita a ASP Agrigento.
Nel caso in cui l'evento di sicurezza occorso non si configuri come *data breach*, allora l'evento è archiviato nel registro di *Incident Management*. I *data breach* sono invece inseriti e conservati all'interno di un registro apposito. È espressamente richiesto al Titolare del Trattamento, infatti, di istituire, in linea con il principio di "Accountability" enunciato dal GDPR, un registro interno delle violazioni, in cui siano documentate tutte le violazioni di dati personali, comprese le circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. La predisposizione, la gestione e la manutenzione di tale registro sono oggetto di trattazione all'interno del successivo paragrafo 2.4 "*Registrazione del data breach*".

In caso contrario, ovvero nel caso in cui l'evento di sicurezza abbia comportato la compromissione di dati personali, si procede con un'analisi di dettaglio della violazione occorsa.
L'analisi preliminare, eseguita dal Delegato interno del trattamento interessato e, in caso il *data breach* abbia sfruttato una vulnerabilità informatica, dai presidi di sicurezza interni ai Sistemi Informativi, è finalizzata alla formalizzazione di un set informativo preliminare in merito al *data breach* occorso. Tali informazioni sono raccolte coinvolgendo, laddove necessario, gli Autorizzati a trattare i dati personali oggetto di *breach*.
In tale fase, il Delegato interno del trattamento è in grado di raccogliere ed identificare generalmente le informazioni relative a:

- **Categorie di interessati** cui i dati personali violati si riferiscono (e.g. pazienti, dipendenti, etc.);
- **Categorie di dati personali compromessi** (dati personali comuni, categorie particolari di dati personali, dati personali relativi a condanne penali e reati);
- **Tipologia di *data breach***: accesso non autorizzato, perdita, alterazione, furto, disclosure, distruzione.

Nello svolgimento dell'analisi preliminare, non è possibile realizzare un *assessment* completo ed esaustivo degli impatti e delle conseguenze che il *data breach* potrebbe avere per gli interessati. In ogni caso, già in questa fase il Delegato interno del trattamento è in grado di identificare, di concerto con il DPO e, laddove necessario, con i Sistemi Informativi, le azioni di prima risposta da intraprendere nell'immediato per contenere gli impatti della violazione di dati personali.

Le risultanze dell'analisi preliminare consentono al Delegato interno del trattamento competente, con il supporto del DPO e dei soggetti interni interessati, di condurre un'analisi di dettaglio al fine di raccogliere tutte le informazioni relative al *data breach* occorso.

Le 72 ore a disposizione del Titolare del Trattamento per notificare all'Autorità di Controllo la violazione di dati personali di cui è venuto a conoscenza potrebbero rivelarsi non sufficienti per condurre un *assessment* completo ed esaustivo circa le circostanze che hanno consentito il verificarsi del *data breach* ed i relativi impatti sui diritti e le libertà degli interessati cui si riferiscono i dati personali compromessi.

A tal proposito, il Delegato interno del trattamento, di concerto con il DPO e con i Sistemi Informativi in caso di incidente di sicurezza informatica, esegue, a valle dell'analisi preliminare, un'analisi di dettaglio finalizzata all'identificazione e formalizzazione delle seguenti informazioni:

- **Identificabilità degli interessati:** ovvero la possibilità che gli interessati, cui si riferiscono i dati personali violati, possano essere identificati, sulla base dei dati che sono stati acceduti illecitamente / divulgati / sottratti. Tale parametro è strettamente connesso alla quantità ed alla tipologia di dati personali compromessi, già identificati nel corso dell'analisi preliminare;
- **Presidi di sicurezza posti in essere**: ovvero l'insieme delle misure di sicurezza tecniche e organizzative che potrebbero aver parzialmente o in toto mitigato gli impatti relativi alla violazione di dati personali. Rientrano in tale categoria i meccanismi di cifratura, soluzioni di *data masking*, meccanismi di controllo accessi, procedure di *backup* periodico, etc., messi in essere da parte dei Sistemi Informativi di ASP Agrigento;
- **Ritardi nella rilevazione del *data breach***: ovvero il tempo intercorso tra il momento in cui è avvenuta la violazione (effettivo o, in tale fase, ancora stimato) ed il momento in cui è stata rilevata. Maggiore è il ritardo, maggiore è la possibilità che il livello di esposizione al rischio sia aumentato;
- **Numero di individui interessati:** la violazione potrebbe avere interessato una sola persona, poche persone fisiche o diverse centinaia / migliaia. Maggiore è il numero di interessati impattati, maggiore è l'impatto della violazione.

In merito all'identificabilità degli interessati, risulta evidente come tale parametro sia strettamente correlato ai presidi di sicurezza posti in essere. Misure di sicurezza quali, a titolo esemplificativo, meccanismi di cifratura rendono inintelligibili i dati personali sottratti per i soggetti non autorizzati, sprovvisti di chiave di decriptazione. La pseudonimizzazione rende i dati personali non più attribuibili ad un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche atte a garantire che tali dati personali non siano attribuiti a una persona fisica identificata.

Sulla base dei suddetti parametri, i Delegati interni del trattamento competenti, con il supporto del DPO, sono in grado di valutare la severità del *data breach* relativamente ai diritti ed alle libertà degli interessati: a seconda della natura dei dati personali (*e.g.* categorie particolari di dati personali e/o dati personali relativi a condanne penali e reati), delle misure di sicurezza adottate, della tipologia di interessati (*e.g.* minori o altri soggetti vulnerabili), i danni potenziali che potrebbero colpire gli interessati possono essere particolarmente severi e consentire furti di identità, frodi, disturbi psicologici, umiliazioni, danni d'immagine / reputazione.
Come descritto all'interno del successivo paragrafo 2.3 "*Risposta e notifica del data breach*", è necessario valutare l'esigenza di comunicare agli interessati la violazione avvenuta, proprio sulla base della severità delle conseguenze per i diritti / libertà di quest'ultimi.

Tutti gli attori coinvolti nelle attività di analisi hanno il compito di raccogliere e conservare tutte le risultanze raccolte in tale fase. Tali evidenze potranno essere utilizzate sia nel corso di eventuali accertamenti condotti dall'Autorità di controllo sia per condurre successive indagini forensi.

2.3 RISPOSTA E NOTIFICA DEL DATA BREACH

A valle del completamento dell'analisi (come descritto all'interno del par. 2.2), le Direzioni coinvolte nella gestione del *data breach* dispongono di tutte le informazioni necessarie per procedere con la fase di contenimento e, contestualmente, con la notifica all'Autorità di Controllo e, nei casi previsti, con la comunicazione agli interessati.
Il DPO rappresenta il punto di contatto nei confronti dell'Autorità di controllo e per i soggetti interessati, a valle della notifica e comunicazione della violazione.
Esso inoltre garantisce la cooperazione con l'autorità di controllo in occasione di accertamenti, visite o quanto altro condotto o richiesto da parte dell'Autorità medesima.

RISPOSTA AL DATA BREACH

Nel corso di tale fase, il Delegato interno del trattamento interessato, insieme al DPO e, laddove necessario, i Sistemi Informativi, identifica le azioni di rientro da implementare e predispone un Piano di Risposta al *data breach* rilevato.

Il Piano di Risposta è attuato da parte del Delegato interno del trattamento/Autorizzati e dei Sistemi Informativi.
Le azioni di risposta da eseguire possono includere, a titolo esemplificativo e non esaustivo:

- reset delle *password* per tutti i sistemi e le applicazioni compromessi;
- disabilitazione o cancellazione di tutte le credenziali compromesse;
- identificazione e disinstallazione di tutti i *software* non licenziati né autorizzati; la rilevazione di tale anomalia può avvenire, ad esempio, mediante confronto dei *checksum* mediante programmi di *integrity checking*;
- limitare l'accesso ai servizi oggetto della violazione. Il primo passo da eseguire, in una procedura di ripristino delle normali funzionalità, è limitare o addirittura bloccare gli accessi a tutti i servizi. Dopo aver determinato il *subset* di servizi compromessi, soltanto gli accessi a tali servizi devono essere limitati. In tale fase, potrebbe rivelarsi utile eseguire una copia dei sistemi corrotti per ulteriori indagini mediante l'utilizzo di *tool* che assicurino l'integrità dei dati;
- nel caso in cui il *data breach* abbia riguardato dati cifrati, allora tali dati devono essere nuovamente cifrati utilizzando un'altra chiave.

NOTIFICA DEL DATA BREACH AL GARANTE DELLA PROTEZIONE DEI DATI PERSONALI

La fase di analisi fornisce al DPO tutti gli strumenti necessari a identificare e valutare le conseguenze negative e gli impatti causati dalla violazione di dati personali rilevata.
Nel caso in cui dovesse risultare improbabile che il *data breach* presenti rischi per i diritti e le libertà degli interessati, la notifica all'Autorità di Controllo risulta essere non obbligatoria. Ciò vale, ad esempio, per i dati personali già contenuti in archivi pubblici e la cui divulgazione non costituisce un rischio per le persone fisiche cui tali dati si riferiscono.
Nel caso di dati sottoposti a meccanismi di cifratura o, comunque, resi inintelligibili per eventuali terze parti non autorizzate, invece, è necessario valutare la rischiosità futura per i diritti degli interessati. Ad esempio, una chiave di cifratura potrebbe essere compromessa successivamente o potrebbero essere rilevate in un secondo momento delle vulnerabilità nel *software* di crittografia.
Pertanto, il DPO è tenuto, per ciascun *data breach* rilevato, a valutare l'esigenza di notifica all'Autorità di Controllo.

Appurata tale esigenza, il DPO provvede a predisporre la notifica all'Autorità di Controllo.
Una prima notifica deve essere inoltrata all'Autorità di Controllo entro 72 ore dal momento in cui il *data breach* è stato rilevato.

La suddetta notifica deve contenere almeno le seguenti informazioni:

- natura della violazione dei dati personali (*disclosure*, perdita, alterazione, accesso non autorizzato, etc.);
- tipologie di dati personali violati;
- categorie e numero approssimativo di interessati cui i dati compromessi si riferiscono;
- nome e dati di contatto del punto di riferimento per ASP Agrigento nei confronti dell'Autorità di Controllo;
- probabili conseguenze della violazione subita;
- descrizione delle misure che ASP Agrigento ha adottato o è in procinto di adottare al fine di mitigare le conseguenze del *data breach*.

Nel caso in cui la prima notifica all'Autorità di Controllo non sia stata eseguita entro le 72 ore previste, il DPO deve altresì elencare i motivi che hanno portato al ritardo nella comunicazione. Inoltre, la notifica può contenere anche informazioni riguardanti l'eventuale comunicazione agli interessati (se è stata inviata una notifica, il suo contenuto ed il canale di comunicazione scelto).

Inoltre, qualora non sia stato possibile fornire contestualmente tutte le informazioni mandatorie, il Delegato interno del trattamento raccoglie quanto prima le informazioni supplementari e le trasmette, non appena a disposizione, al DPO per consentire a quest'ultimo di integrare la notifica inoltrata all'Autorità di Controllo.

Le integrazioni apportate alla prima notifica possono riguardare, in particolare modo, le misure tecniche ed organizzative applicate preventivamente ai dati violati, le misure assunte per mitigare i rischi, il livello di gravità della violazione, un numero maggiormente preciso in merito agli interessati coinvolti e/o eventuali impedimenti alla notifica agli interessati, laddove prevista.

NOTIFICA DEL DATA BREACH AGLI INTERESSATI

Oltre a notificare il *data breach* all'Autorità di Controllo, ASP Agrigento è tenuta a valutare l'esigenza di procedere con la comunicazione del *data breach* anche ai soggetti interessati cui i dati violati si riferiscono.

Per stabilire la necessità di comunicazione agli interessati, il DPO deve valutare i seguenti fattori:

- se il trattamento può comportare discriminazioni, furto d'identità, perdite finanziare, disturbi psicologici, 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;
- se gli interessati rischiano di essere privati dei loro diritti o delle libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano;
- se sono trattati dati personali che rivelano l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi a condanne penali e a reati o alle relative misure di sicurezza;
- in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;
- se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori;
- se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

La comunicazione deve, pertanto, avvenire nel caso in cui la violazione di dati personali presenti un rischio elevato per i diritti e le libertà delle persone fisiche, a meno che non sia verificata almeno una di queste condizioni:

- sono state applicate adeguate misure tecniche e organizzative per proteggere i dati prima della violazione, in particolare quelle in grado di renderle inintelligibili per soggetti terzi non autorizzati (e.g. misure di cifratura);
- a valle della rilevazione del *data breach*, sono state adottate misure per impedire il concretizzarsi dei rischi per i diritti e le libertà degli interessati. Ad esempio, è già stato identificato l'eventuale terzo non autorizzato ed impedita qualunque operazione da parte di quest'ultimo;
- comunicare il *data breach* a tutti gli interessati comporta uno sforzo sproporzionato, ad esempio nel caso in cui i dati di contatto siano stati persi a causa della violazione e sono difficilmente recuperabili.

Sono da ritenersi inintelligibili i dati che:

- sono stati cifrati in modo sicuro attraverso algoritmi standardizzati o l'impiego di meccanismi di cifratura a chiave simmetrica o pubblica noti in letteratura, purché la chiave di decifrazione sia di adeguata lunghezza (espressa in numero di *bit*) e la relativa custodia sia disciplinata da *policy* interne di conservazione e purché essa non sia stata compromessa da violazioni della sicurezza e sia stata generata in modo tale da non consentirne la derivazione da parte di soggetti non autorizzati; oppure
- siano stati sostituiti da un valore di hash calcolato attraverso una funzione crittografica di *hashing* a chiave, purché la chiave utilizzata per effettuare *hashing* dei dati sia di adeguata lunghezza e la relativa custodia sia disciplinata da *policy* interne di conservazione e purché essa non sia stata compromessa da violazioni della sicurezza e sia stata generata in modo tale da non consentirne la derivazione da parte di soggetti non autorizzati; oppure
- siano stati resi anonimi con procedure tali da non consentire la reidentificazione degli interessati cui si riferiscono da parte di soggetti non autorizzati al trattamento, anche mediante il ricorso ad altre fonti informative pubbliche o disponibili presso ASP Agrigento stessa.

La comunicazione agli interessati può essere trasmessa via sms o posta elettronica, all'indirizzo fornito dall'interessato.
Il DPO e il Responsabile dei Sistemi Informativi identificano di volta in volta, sulla base della tipologia e del numero di interessati, il canale di comunicazione più opportuno per trasmettere la notifica.
In ogni caso la comunicazione agli interessati deve essere redatta con un linguaggio semplice e chiaro e deve contenere quantomeno:

- descrizione della natura della violazione dei dati personali;
- dati di contatto del DPO;
- descrizione delle probabili conseguenze della violazione;
- descrizione delle misure adottate o che ASP Agrigento intende adottare per porre rimedio alla violazione e ridurre gli effetti negativi.

La comunicazione agli interessati deve inoltre contenere, se ritenuto opportuno da parte del DPO e del Responsabile dei Sistemi Informativi, dei consigli specifici / istruzioni da seguire per ridurre le possibili conseguenze negative della violazione, come l'aggiornamento delle *password* nel caso in cui le credenziali di accesso degli interessati siano state compromesse.

2.4 REGISTRAZIONE DEL DATA BREACH

In ottica di *accountability*, al Titolare del Trattamento è richiesto di istituire un registro interno delle violazioni (di seguito anche "Data breach Inventory"), indipendentemente dalle potenziali notifiche che possono avvenire a seguito della violazione dei dati.
Il DPO, con il supporto del Responsabile dei Sistemi Informativi relativamente agli incidenti di sicurezza informatica, predispone e manutiene un registro interno in cui è documentata qualsiasi violazione dei dati personali, comprese le circostanze, le conseguenze e le misure adottate per porvi rimedio.

Nel Data breach Inventory devono essere puntualmente annotate:

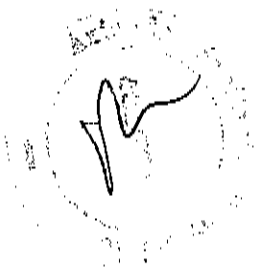
- ID del *data breach*;
- data e ora registrazione;
- nome e descrizione del trattamento;
- nome del Delegato interno del trattamento;
- nome del Responsabile esterno del trattamento (laddove previsto);
- riferimenti del DPO;
- data e ora violazione;
- descrizione violazione;
- dati personali compromessi e tipologie di interessati;
- tipologia di *data breach* e relative cause;
- conseguenze ed effetti per i diritti degli interessati;
- azioni correttive adottate da ASP Agrigento comprensive di motivazioni;
- data e ora notifica all'Autorità di Controllo;
- data e ora notifica agli interessati;
- mezzo notifica agli interessati.

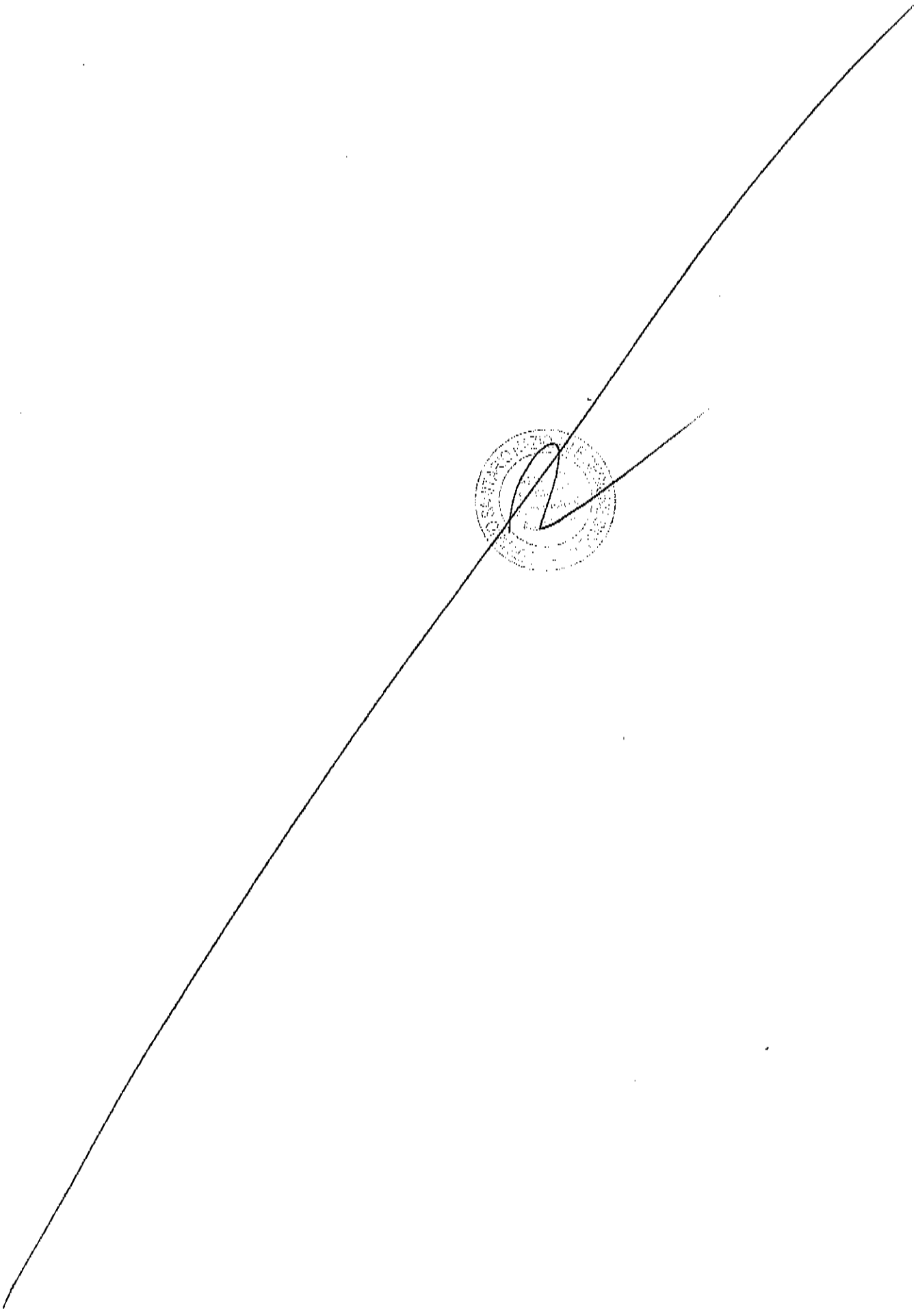
In caso di violazioni relative a incidenti di sicurezza informativa, è necessario inoltre allegare una opportuna relazione tecnica che illustri cause, evoluzione e conseguenze dell'incidente, con indicazione delle opportune azioni di rimedio per evitare che lo stesso possa occorrere nuovamente.

Qualora una violazione non venga notificata, il DPO è tenuto a documentare la giustificazione di tale decisione, ovvero i motivi per i quali si è ritenuto che la violazione non implicasse rischi per i diritti e libertà degli individui.

Il *data breach* è dunque inserito all'interno dell'apposito registro fin dalla fase di rilevazione. A valle delle attività di analisi, risposta e notifica (all'Autorità di Controllo e /o agli interessati), il *Data breach Inventory* è costantemente tenuto aggiornato con tutte le informazioni richieste.

Il DPO ha la responsabilità della tenuta del *Data breach Inventory* e dell'esecuzione di attività di monitoraggio e controllo al fine di verificare l'effettivo aggiornamento di tale registro da parte dei singoli Delegati interni del trattamento.





PUBBLICAZIONE

Si dichiara che la presente deliberazione, a cura dell'incaricato, è stata pubblicata in forma digitale all'albo pretorio on line dell'ASP di Agrigento, ai sensi e per gli effetti dell'art. 53, comma 2, della L.R. n.30 del 03/11/93 e dell'art. 32 della Legge n. 69 del 18/06/09 e s.m.i., dal _____ al _____

L'Incaricato

_____

Il Funzionario Delegato
Il Titolare di Posizione Organizzativa
Ufficio di Segreteria, Proposte di atti e Anuma
Dott.ssa Patrizia Tedesco

Notificata al Collegio Sindacale il _____ **con nota prot. n.**_____

DELIBERA SOGGETTA AL CONTROLLO

Dell'Assessorato Regionale della Salute ex L.R. n. 5/09 trasmessa in data _____ prot. n. _____

SI ATTESTA

Che l'Assessorato Regionale della Salute:

- Ha pronunciato **l'approvazione** con provvedimento n. _____ del _____
- Ha pronunciato **l'annullamento** con provvedimento n. _____ del _____

come da allegato.

Delibera divenuta esecutiva per decorrenza del termine previsto dall'art. 16 della L.R. n. 5/09 dal _____

DELIBERA NON SOGGETTA AL CONTROLLO

- Esecutiva ai sensi dell'art. 65 della L. R. n. 25/93, così come modificato dall'art. 53 della L.R. n. 30/93 s.m.i., per decorrenza del termine di 10 gg. di pubblicazione all'Albo, dal _____

X Immediatamente esecutiva dal 11 NOV. 2019

Agrigento, lì 11 NOV. 2019

Il Titolare di Posizione Organizzativa
Ufficio di Segreteria, Proposte di atti e Anuma
Dott.ssa Patrizia Tedesco

REVOCA/ANNULLAMENTO/MODIFICA

- Revoca/annullamento in autotutela con provvedimento n. _____ del _____
- Modifica con provvedimento n. _____ del _____

Agrigento, lì

Il Titolare di Posizione Organizzativa
Ufficio di Segreteria, Proposte di atti e Anuma
Dott.ssa Patrizia Tedesco