	Riferimento	Versione	Data
Regione Siciliana sito ufficiale www.regione.sicilia.it		*1.0*	*20-12-2018*
ASP 8 SIRACUSA AZIENDA SANITARIA PROVINCIALE	**Procedura aziendale**	Numero Pagine Documento ***41***	Stato documento ***In via di definizione*** Ambito ***Uso Pubblico***[1]

Procedura sulla gestione delle violazioni di dati personali

(Data Breach)

sulla base del Regolamento UE 2016/679

LISTA DISTRIBUZIONE

ASP di Siracusa	☐ *Direzione Generale* ☐ *Direzione Amministrativa* ☐ *Direzione Sanitaria* ☐ *Delegati al Trattamento del Dati Personali* ☐ *Responsabili e Sub-Responsabili del Trattamento*

Elaborato da:	***ing.* Stefano SALEMI** RPD - Responsabile della Protezione dei Dati	
Verificato da:	GLPD – Gruppo di Lavoro per la Protezione dei Dati	

[1] Vedere pagina 2 per la classificazione completa del documento.

QUESTO DOCUMENTO E' CLASSIFICATO COME:

USO INTERNO

Classificazione Italia	Classificazione NATO	Descrizione	Modalità di consegna
Pubblico	**Unclassified**	Informazioni per tutti, non c'è confidenzialità	Invio a mezzo email o standard
Uso Interno	**Confidential**	Informazioni di proprietà dell'azienda, di libera circolazione all'interno della stessa	Invio a mezzo email o standard
Confidenziale	**Secret**	Informazioni di proprietà aziendale soggette a restrizioni nella divulgazione	Invio a mezzo email con applicazione di cifratura o invio a mezzo corriere s.p.m. c/o referente Cliente
Esclusivo	**Top Secret**	Informazioni aziendali di particolare rilevanza soggette al massimo delle restrizioni di sicurezza	Invio a mezzo email con applicazione di cifratura o invio a mezzo corriere s.p.m. c/o referente Cliente

Sommario

I. Scopo e Campo di applicazione

La presente procedura sulla gestione delle violazioni di dati personali (detta anche "**Procedura Data Breach**") ha lo scopo di fornire le indicazioni pratiche della Azienda in caso di violazione dei dati personali, nel rispetto della normativa in materia di trattamento dati personali, garantendo in particolare l'aderenza ai principi e alle disposizioni contenute nel Regolamento UE 2016/679 sulla Protezione dei Dati Personali (da ora in poi, **GDPR** – GENERAL DATA PROTECTION REGULATION).

Si possono distinguere tre tipi di violazioni:

1. **Violazione di riservatezza**: quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale;
2. **Violazione di integrità**: quando si verifica un'alterazione di dati personali non autorizzata o accidentale;
3. **Violazione di disponibilità**: quando si verifica perdita, inaccessibilità o distruzione, accidentale o non autorizzata, di dati personali (un incidente che determini la non disponibilità di dati per un periodo di tempo deve essere comunque considerato violazione).

In questo documento, si sintetizzano le regole per garantire il rispetto dei principi esposti nonché la realizzabilità tecnica e la sostenibilità organizzativa, nella gestione del **data breach**, sotto i diversi aspetti relativi a:

- Modalità e profili di segnalazione al Titolare;
- Modalità e profili di segnalazione all'Autorità Garante;
- Valutazione dell'evento accaduto;
- Eventuale comunicazione agli interessati.

La presente procedura si applica all'Azienda Sanitaria Provinciale di Siracusa (da ora in poi, ASP), nella qualità di Titolare del trattamento, nonché alla Società,/Ditta designata Responsabile del trattamento.

II. Normativa di riferimento

GDPR – considerando n.85

Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata. Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

GDPR – considerando n.86

Il titolare del trattamento dovrebbe comunicare all'interessato la violazione dei dati personali senza indebito ritardo, qualora questa violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica, al fine di consentirgli di prendere le precauzioni necessarie. La comunicazione dovrebbe descrivere la natura della violazione dei dati personali e formulare raccomandazioni per la persona fisica interessata intese ad attenuare i potenziali effetti negativi. Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti quali le autorità incaricate dell'applicazione della legge. Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione agli interessati fosse tempestiva, ma la necessità di attuare opportune misure per

contrastare violazioni di dati personali ripetute o analoghe potrebbe giustificare tempi più lunghi per la comunicazione.

GDPR – considerando n.87

È opportuno verificare se siano state messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali e informare tempestivamente l'autorità di controllo e l'interessato. È opportuno stabilire il fatto che la notifica sia stata trasmessa senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione dei dati personali e delle sue conseguenze e effetti negativi per l'interessato. Siffatta notifica può dar luogo a un intervento dell'autorità di controllo nell'ambito dei suoi compiti e poteri previsti dal presente regolamento.

GDPR – considerando n.88

Nel definire modalità dettagliate relative al formato e alle procedure applicabili alla notifica delle violazioni di dati personali, è opportuno tenere debitamente conto delle circostanze di tale violazione, ad esempio stabilire se i dati personali fossero o meno protetti con misure tecniche adeguate di protezione atte a limitare efficacemente il rischio di furto d'identità o altre forme di abuso. Inoltre, è opportuno che tali modalità e procedure tengano conto dei legittimi interessi delle autorità incaricate dell'applicazione della legge, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali.

GDPR – articolo n.33 – Notifica di una violazione dei dati personali all'autorità di controllo

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e

le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

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

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

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

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

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

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

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

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

GDPR – articolo n.34 – Comunicazione di una violazione dei dati personali all'interessato

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

2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e

contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).

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

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

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

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

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

III. FASE 1: RACCOLTA DELLE INFORMAZIONI

Canali interni

Le segnalazioni interne di eventi anomali possono:

- Pervenire dal personale dell'Azienda;
- Essere inoltrate dal Responsabile della Protezione dei Dati.

Canali esterni

Le segnalazioni possono pervenire anche da fonti esterne, o anche dall'analisi di informazioni presenti sul web, ovvero dai Responsabili del trattamento.

Inoltre, ogni Interessato può segnalare, anche solo in caso di sospetto, che i propri Dati Personali siano stati utilizzati abusivamente o fraudolentemente da un terzo; in tal caso, l'interessato può richiedere all'Azienda la verifica dell'eventuale violazione.

Le segnalazioni, a qualunque soggetto/funzione pervengano, devono essere tempestivamente comunicate al Responsabile della Protezione dei Dati, comunque non oltre 12 ore dalla conoscenza della violazione, ove possibile a mezzo PEC, al seguente indirizzo: rdp@asp.sr.it

La presa in carico di tutte le segnalazioni è di responsabilità del Responsabile della Protezione dei Dati che provvederà a gestirle coinvolgendo le altre funzioni interessate secondo quanto specificato nella presente procedura.

IV. FASE 2: ANALISI DELLE SEGNALAZIONI (Data Breach presso l'ASP, in qualità di Titolare)

Analisi preliminare e elaborazione della scheda evento

Il Responsabile della Protezione dei Dati avvia un'analisi preliminare finalizzata alla raccolta dei dati concernenti l'anomalia e alla compilazione della Scheda Evento (allegato A) della presente procedura contenente tutte le informazioni raccolte:

- Data evento anomalo;
- Data presunta di avvenuta violazione;
- Data e ora in cui si è avuto conoscenza della violazione;
- Fonte segnalazione;
- Tipologia violazione e di informazioni coinvolte;
- Descrizione evento anomalo;
- Numero Interessati coinvolti;
- Numerosità di Dati Personali di cui si presume una violazione;
- Indicazione del luogo in cui è avvenuta la violazione dei dati, specificando altresì se essa sia avvenuta a seguito di smarrimento di Dispositivi Mobili;
- Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione.

La Scheda Evento viene quindi destinata all'analisi di primo livello descritta di seguito.

Analisi di primo livello – Verifica della segnalazione

Obiettivo dell'analisi di primo livello è quella di verificare che la segnalazione non si tratti di un cd. "falso positivo". Nel caso la violazione sui dati personali venga accertata, il Responsabile della Protezione dei Dati, responsabile dell'analisi di primo livello, con la collaborazione delle direzioni coinvolte dalla violazione, recupera le informazioni di dettaglio sull'evento necessarie alle analisi di secondo livello, e le riporta nella Scheda Evento. Nel caso in cui l'evento segnalato risulti essere un falso positivo, si chiude l'incidente.

L'evento viene comunque inserito a cura del Responsabile della Protezione dei Dati nel Registro dei data Breach (allegato C) della presente procedura, nell'apposita sezione dedicata agli "eventi falsi positivi".

Analisi di secondo livello – Scheda violazione dati

L'analisi di secondo livello, finalizzata alla valutazione d'impatto, viene effettuata dal Gruppo di Lavoro per la Protezione dei Dati (GLPD), coordinato dal Responsabile della Protezione dei Dati e alla presenza del Commissario/Direttore Generale.

Dall'analisi congiunta di tutte le informazioni raccolte si redige una Scheda Violazione Dati (allegato B) della presente procedura, per le conseguenti valutazioni.

Il GLPD classifica l'evento tra i seguenti casi:

Classificazione evento	
Codice	**Descrizione**
CLEV01	Distruzione di dati illecita
CLEV02	Perdita di dati illecita
CLEV03	Modifica di dati illecita
CLEV04	Distruzione di dati accidentale
CLEV05	Perdita di dati accidentale
CLEV06	Modifica di dati accidentale
CLEV07	Divulgazione non autorizzata
CLEV08	Accesso ai dati personali illecito

La violazione deve essere valutata secondo i livelli di rischio:

Classificazione livello di rischio		
Codice	**Colore**	**Descrizione**
CLRS01	Bianco	**NULLO**
CLRS02	Verde	**BASSO**
CLRS03	Giallo	**MEDIO**
CLRS04	Rosso	**ALTO**

Il rischio va riferito alla probabilità che si verifichi una delle seguenti condizioni a danno di persone fisiche anche diverse dall'interessato a cui si riferiscono i dati, a causa della violazione dei Dati Personali:

- 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;
- Danno economico o sociale significativo;
- Privazione o limitazione di diritti o libertà;
- Impedito controllo sui dati personali all'interessato;
- Danni fisici, materiali o immateriali alle persone fisiche.

Saranno inoltre valutate, come variabili qualitative dell'impatto temuto, le seguenti eventuali condizioni:

a) Che si tratti di dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché di dati genetici, dati relativi alla salute o dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;

b) Che si tratti di dati relativi a 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;

c) Che si tratti di dati di persone fisiche vulnerabili, in particolare minori;

d) Che il trattamento riguardi una notevole quantità di Dati Personali;

e) Che il trattamento riguardi un vasto numero di Interessati.

Il GLPD deve provvedere affinché vengano tempestivamente adottate misure che consentono di minimizzare le conseguenze negative della violazione.

V. FASE 3: NOTIFICA E COMUNICAZIONE

Notifica alla Autorità di Controllo

Redatta la Scheda di Valutazione Dati, il GLPD deve valutare le azioni da intraprendere ed avviare la notificazione verso l'Autorità di Controllo e, ove necessario, la comunicazione agli Interessati, verificando e validando la documentazione pervenuta dalle precedenti fasi di lavoro.

Il Responsabile della Protezione dei Dati notifica la violazione all'Autorità di Controllo competente 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 e dunque sia stato dallo stesso classificato "NULLO".

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

La notifica all'Autorità di Controllo deve:

a) descrivere, ove possibile:

   i. la natura della Violazione dei Dati Personali compresi;

   ii. le categorie e il numero approssimativo di Interessati in questione;

   iii. le categorie e il numero minimo approssimativo di registrazioni dei Dati Personali in questione;

b) comunicare il nome e i dati di contato del Responsabile della Protezione dei Dati o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le probabili conseguenze della Violazione dei Dati Personali;

d) descrivere le misure adottate o di cui si propone l'adozione da parte dell'Azienda per porre rimedio alla Violazione dei Dati Personali e anche, se del caso, per attenuarne i possibili effetti negativi.

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

Comunicazione della violazione all'interessato

Il Responsabile della Protezione dei Dati, sentita la Direzione Generale, deve informare gli interessati dell'evento anomalo, in tutti i casi in cui, a norma degli articoli 33 e 34 del GDPR, il GLPD valuti che la violazione risulta presentare rischi classificati come "ALTO" nella Scheda Violazione Dati per i diritti e le libertà delle persone fisiche.

La comunicazione deve essere rivolta all'interessato senza ingiustificato ritardo dall'avvenuta conoscenza e valutazione della violazione, attraverso il canale di comunicazione ritenuto più idoneo; deve essere effettuata ad opera del GLPD e deve essere intellegibile, coincisa, trasparente e facilmente accessibile; deve essere utilizzato un linguaggio semplice e chiaro adottando, se possibile, la stessa lingua parlata dall'Interessato. Rispetto alle modalità della comunicazione si applicano quelle ritenute più idonee dal GLPD.

La comunicazione di Data Breach all'Interessato deve contenere le seguenti informazioni:

a) data e ora della violazione, anche solo presunta, e data e ora in cui si è avuto conoscenza della stessa;

b) la natura della Violazione dei Dati Personali;

c) il nome e i dati di contatto del Responsabile della Protezione dei Dati;

d) le probabili conseguenze della Violazione dei Dati Personali;

e) la descrizione delle misure adottate o di cui si propone l'adozione da parte dell'Azienda per porre rimedio alla Violazione dei Dati Personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Non è richiesta la comunicazione all'Interessato se è soddisfatta una delle seguenti condizioni:

- sono state messe in atto le misure tecniche ed 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; salvo i casi in cui la violazione della sicurezza ha comportato la distruzione o la perdita dei Dati Personali degli Interessati;

- sono state successivamente adottate misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà delle persone fisiche; in tal caso è necessario documentare le misure nella scheda di violazione;
- 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.

L'Azienda riporta in calce un Modello di comunicazione all'Interessato della Violazione dei Dati Personali.

VI. FASE 4: REGISTRAZIONE SEGNALAZIONE NEL REGISTRO DEI DATA BREACH

Nel Registro dei data Breach (allegato C della presente procedura), il Responsabile della Protezione dei Dati documenta ogni singolo evento, sia esso, FALSO, IRRILEVANTE ovvero RILEVANTE; **in questi due ultimi** casi, devono essere indicate nel registro:

- le conseguenze del Data Breach;
- i provvedimenti adottati per porvi rimedio o attenuarne le conseguenze;
- l'eventuale notificazione all'Autorità di Controllo;
- l'eventuale comunicazione all'Interessato.

Tale documentazione consente all'Autorità di Controllo di verificare il rispetto delle norme in materia di notificazione delle Violazioni di Dati Personali.

Il Registro dei Data Breach è tenuto a cura del Responsabile della Protezione dei Dati sotto la responsabilità dell'Azienda, Titolare del trattamento.

VII. FASE 5: ANALISI POST VIOLAZIONE

L'ultima fase del processo di gestione delle Violazioni di dati Personali prevede la raccolta finale delle evidenze, l'analisi delle informazioni giunte sul contesto di violazione osservato, e la valutazione delle stesse al fine di effettuare un'analisi post-incidente, per verificare l'efficacia e l'efficienza delle azioni intraprese durante la gestione dell'evento ed identificare possibili aree di miglioramento.

Tale attività prevede il coinvolgimento della struttura informatica aziendale, con eventuale supporto da parte di altre aree funzionali.

VIII. DATA BREACH PRESSO LA SOCIETA' O UN TERZO IN QUALITA' DI RESPONSABILE

Obblighi di comunicazione della Società quando opera in qualità di Responsabile

Quando la Società agisce in qualità di Responsabile, in caso di Violazione dei Dati Personali, deve informare il Titolare del trattamento, senza ingiustificato ritardo secondo i tempi e i modi concordati nel contratto per il trattamento dei dati personali trasmesso da quest'ultimo.

Obblighi di comunicazione di un Responsabile dei confronti dell'Azienda Sanitaria

Quando un terzo agisce in qualità di Responsabile del Trattamento, in caso di Violazione dei Dati Personali, deve informare l'Azienda (che agisce in qualità di Titolare), senza ingiustificato ritardo e non al più tardi di 24 ore dal momento in cui ha conoscenza della violazione, inviando una comunicazione via PEC ai seguenti indirizzi:

- direzione.generale@asp.sr.it
- rpd@asp.sr.it

e successivamente collaborare con l'Azienda per consentirle di adempiere agli obblighi previsti dalla normativa agli articoli 33 e 34 del GDPR.

La procedura che segue è riportata nel contratto per il trattamento dei Dati Personali (tra Titolare del trattamento e Responsabile esterno del trattamento), salvo diversamente concordata con il Responsabile.

Il Responsabile deve assistere l'Azienda avviando un'analisi preliminare finalizzata alla raccolta dei dati concernenti l'anomalia e alla compilazione della Scheda Evento utilizzando il modello allegato alla presente procedura, contenente tutte le informazioni raccolte:

- Data evento, anche la data presunta di avvenuta violazione (in tal caso va specificato);
- Data e ora in cui si è avuto conoscenza della violazione;

- Fonte segnalazione;
- Tipologia violazione e di informazioni coinvolte;
- Descrizione evento anomalo;
- Numero Interessati coinvolti;
- Numerosità di dati personali di cui si presume una violazione;
- Indicazione della data, anche presunta, della violazione e del momento in cui se ne è avuta conoscenza;
- Indicazione del luogo in cui è avvenuta la violazione dei dati, specificando altresì se ess sia avvenuta a seguito di smarrimento di Dispositivi Mobili;
- Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione.

Una volta condotta l'analisi preliminare, il Responsabile deve condurre un'analisi di primo livello per verificare che la segnalazione non tratti un falso positivo; all'esito dell'accertamento, qualora si tratti di un falso positivo, il Responsabile deve comunicarlo immediatamente all'Azienda (agli stessi indirizzi di cui sopra), al fine di consentirle di inserire l'evento nella sezione "eventi falsi positivi" del Registro dei Data Breach (allegato C).

In caso contrario, il Responsabile recupera le informazioni di dettaglio sull'evento necessarie alle analisi di secondo livello e le riporta nella Scheda Evento che deve essere inviata, via PEC, tempestivamente e non oltre 24 ore dalla conoscenza della violazione, al Responsabile della Protezione dei Dati dell'ASP.

L'evento deve essere inserito dall'Azienda in un apposito Registro dei Data Breach il cui modello è allegato alla presente procedura.

L'Azienda, una vota ricevuta la Scheda Evento deve procedere secondo le prescrizioni di cui ai paragrafi IV (Analisi di secondo livello – Scheda violazione dati); V; VI e VII della presente procedura.

SCENARI DI DATA BREACH

Di seguito sono illustrati alcuni esempi non esaustivi, di possibili violazioni di dati personali, allo scopo di supportare i soggetti coinvolti nella procedura, nella valutazione in merito alla necessità di effettuare o meno la notifica di Data Breach.

Tipo di Violazione (Breach)	Definizione	Estensione minima o Soglia di segnalazione	Esempi
Distruzione	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non è più nella disponibilità del Titolare, né di altri. In caso di richiesta del dato da parte dell'interessato, non sarebbe possibile produrlo.	✓ Dati non recuperabili o provenienti da procedure non ripetibili. *Rientrano in tali casi di segnalazione, i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione*	RIENTRANO NELLA CASISTICA ✓ Rottura di un apparecchio elettromedicale prima di inviare al sistema centrale il dato (immagine, valori, ecc…); ✓ Guasto non riparabile dell'hard disk contenente uno o più referti che erano salvati localmente; ✓ Incendio di archivio cartaceo delle cartelle cliniche; ✓ Distruzione di campioni biologici. <u>NON</u> RIENTRANO NELLA CASISTICA ✓ Rottura di un PC o di una Pen drive USB che non contengono dati personali originali (in unica copia); ✓ Distruzione di un documento, ad esempio a causa di un guasto di sistema, durante la sua stesura nell'apposito applicativo.

Perdita	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non è più nella disponibilità del Titolare, ma potrebbe essere nella disponibilità di terzi (lecitamente o illecitamente). In caso di richiesta del dato da parte dell'interessato, non sarebbe possibile produrlo, ed è possibile che terzi possano avere impropriamente accesso al dato.	✓ Dati non recuperabili o provenienti da procedure non ripetibili. ✓ Dati relativi a più assistiti, relativi a interi episodi o relativi a tipologie di dato la cui indisponibilità lede i diritti fondamentali dell'Interessato o relativi a tipologie di dato la cui divulgazione conseguente alla perdita possa ledere i diritti fondamentali dell'interessato. *Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.*	RIENTRANO NELLA CASISTICA ✓ Smarrimento di Pen drive USB contenente dati originali; ✓ Smarrimento di fascicolo cartaceo personale dipendente; ✓ Infezione da ransomware che provoca la crittografia di tutti i dati. Non sono disponibili backup e i dati non possono essere ripristinati. Durante le indagini, diventa chiaro che l'unica funzionalità del ransomware era quella di crittografare i dati e che non c'erano altri malware presenti nel sistema. <u>NON</u> RIENTRANO NELLA CASISTICA ✓ Smarrimento di un documento, ad esempio a causa di un guasto di sistema, appena avvenuta la stampa; ✓ Furto di una Pen drive USB contenente dati crittografati. Se i dati sono stati crittografati con un algoritmo avanzato, ed esiste il backup dei dati contenuti nella chiavetta, e la chiave crittografica non è stata compromessa, ed i dati possono essere ripristinati in tempo utile allora non è necessario eseguire la notifica all'Autorità.

Modifica	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, è stato irreversibilmente modificato, senza possibilità di ripristinare lo stato originale. In caso di richiesta del dato da parte dell'Interessato non sarebbe possibile produrlo con certezza che non sia stato alterato.	✓ Modifiche sistematiche su più casi. *Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.*	RIENTRANO NELLA CASISTICA ✓ Guasto tecnico che altera parte dei contenuti di un sistema clinico, compromettendo anche i backup; ✓ Azione involontaria, o fraudolente, di un utente che porta all'alterazione di dati sanitari in modo non tracciato e irreversibile. <u>NON</u> RIENTRANO NELLA CASISTICA ✓ Guasto tecnico che altera parte dei documenti di un sistema clinico, rilevato e sanato tramite operazioni di recovery; ✓ Azione involontaria di un utente che porta all'alterazione di dati tracciata e reversibile; ✓ Modifica di un documento non ancora validato dal proprio autore.
Divulgazione non autorizzata	Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente), a seguito di incidente o azione fraudolenta, viene trasmesso a terze parti senza il consenso dell'Interessato o in violazione del regolamento dell'organizzazione.	*Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.*	RIENTRANO NELLA CASISTICA ✓ Consegna di un CD con dati dei pazienti ad altra struttura senza autorizzazione. <u>NON</u> RIENTRANO NELLA CASISTICA ✓ Il medico sul proprio sistema dipartimentale seleziona il paziente Mario Rossi ma visita il paziente Luca Bianchi. Inserisce anamnesi e gli altri valori di refertazione. ✓ Infezione virale di un PC con un virus che non trasmette dati su internet; ✓ Trasmissione non autorizzata di un documento non ancora validato dal proprio autore.

Accesso non autorizzato	Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente) sono stati resi disponibili per un intervallo di tempo a persone (anche incaricati dal Titolare) non titolati ad accedere al dato secondo principio di pertinenza e non eccedenza, o secondo i regolamenti dell'organizzazione.	*Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.*	RIENTRANO NELLA CASISTICA ✓ Accesso alla rete aziendale da persone esterne all'organizzazione che sfruttano vulnerabilità di sistemi; ✓ Accesso da parte di un utente a dati non di sua pertinenza a seguito di configurazione errata dei permessi di accesso ad un sistema clinico. NON RIENTRANO NELLA CASISTICA ✓ Accesso da parte di un utente a dati di sua pertinenza, a cui segue un uso improprio degli stessi; ✓ Accesso non autorizzato di un documento non ancora validato dal proprio autore.
Indisponibilità temporanea	Un insieme di dati personali, a seguito di incidente, azione fraudolenta o involontaria, è non disponibile per un periodo di tempo che lede i diritti dell'Interessato.	*Indisponibilità dei dati personali oltre i tempi definiti a livello aziendale.*	RIENTRANO NELLA CASISTICA ✓ Cancellazione accidentale dei dati da parte di una persona non autorizzata e successivo ripristino da backup; ✓ Le cartelle cliniche non sono disponibili per un periodo di 30 ore a causa di un attacco informatico. NON RIENTRANO NELLA CASISTICA ✓ Indisponibilità dei dati personali a causa della manutenzione programmata del sistema in corso.

ALLEGATI

Allegato A: SCHEDA EVENTO

Regione Siciliana
AZIENDA SANITARIA PROVINCIALE DI SIRACUSA
Corso Gelone, 17 – 96100 Siracusa (SR)
Cod. Fisc./P.IVA: 01661590891
telefono: +39 0931.724111 (*centralino*) | *fax:* +39 0931.484684
pec: direzione.generale@pec.asp.sr.it - *url:* www.asp.sr.it

Scheda Evento

Codice Identificativo	
Data evento e ora della violazione anche solo presunta[†]	
Data e ora in cui si è avuto conoscenza della violazione	
Fonte di segnalazione	
Tipologia evento anomalo	
Descrizione evento anomalo	
Numero interessati coinvolti	

[†] specificando se è presunta

Numerosità dei dati personali di cui si presume la violazione	
Data, anche presunta, della violazione e del momento in cui se ne è avuta conoscenza	
Luogo in cui è avvenuta la violazione dei dati‡	
Descrizione dei sistemi di elaborazione e/o memorizzazione dei dati coinvolti, con indicazione della loro ubicazione	

‡ Specificare se è avvenuta a seguito di smarrimento di dispositivi o di supporti portatili

Allegato B: SCHEDA VIOLAZIONE DATI

Regione Siciliana
AZIENDA SANITARIA PROVINCIALE DI SIRACUSA
Corso Gelone, 17 – 96100 Siracusa (SR)
Cod. Fisc./P.IVA: 01661590891
telefono: +39 0931.724111 (*centralino*) | *fax:* +39 0931.484684
pec: direzione.generale@pec.asp.sr.it - *url:* www.asp.sr.it

Scheda Violazione Dati

Codice Identificativo Evento[§]		
Classificazione[**]		
Rischio	Livello[††]	
	Condizioni[‡‡]	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 danno economico o sociale significativo privazione o limitazione di diritti o libertà impedito controllo sui dati personali all'interessato danni fisici, materiali o immateriali alle persone fisiche altro_____

[§] Inserire il CODICE della Scheda Evento

[**] Il GLPD classifica l'evento tra i seguenti casi: Distruzione di dati illecita; Perdita di dati illecita; Modifica di dati illecita; Distruzione di dati accidentale; Perdita di dati accidentale; Modifica di dati accidentale; Divulgazione non autorizzata; Accesso ai dati personali illecito.

[††] Il GLPD valuta il rischio secondo i seguenti livelli di rischio: NULLO; BASSO; MEDIO; ALTO

[‡‡] Il rischio va riferito alla probabilità che si verifiche una delle condizioni indicate a danno di persone fisiche anche diverse dall'interessato a cui si riferiscono i dati, a causa della violazione dei dati personali (barrare quello che interessa)

Allegato C: REGISTRO DEI DATA BREACH

Regione Siciliana
AZIENDA SANITARIA PROVINCIALE DI SIRACUSA
Corso Gelone, 17 – 96100 Siracusa (SR)
Cod. Fisc./P.IVA: 01661590891
telefono: +39 0931.724111 (*centralino*) | *fax:* +39 0931.484684
pec: direzione.generale@pec.asp.sr.it - *url:* www.asp.sr.it

Registro dei DATA BREACH

Evento				Conseguenze	Provvedimenti adottati	Notifica all'Autorità di Controllo		Comunicazione all'Interessato	
Codice	Irrilevante	Falso Positivo	Rilevante			SI/NO	Data	SI/NO	Data

Allegato D: MODELLO DI COMUNICAZIONE ALL'INTERESSATO DELLA VIOLAZIONE DEI DATI PERSONALI

Regione Siciliana
AZIENDA SANITARIA PROVINCIALE DI SIRACUSA
Corso Gelone, 17 – 96100 Siracusa (SR)
Cod. Fisc./P.IVA: 01661590891
telefono: +39 0931.724111 (*centralino*) | *fax:* +39 0931.484684
pec: direzione.generale@pec.asp.sr.it - *url:* www.asp.sr.it

Comunicazione all'Interessato della Violazione dei dati Personali

(ai sensi del Regolamento Europeo 2016/679 sulla Protezione dei dati)

Gentile Signore/a,

Secondo quanto prescritto dall'articolo 34 del Regolamento suddetto, l'Azienda Sanitaria Provinciale di Siracusa, titolare del trattamento, con la presente è a comunicarLe, l'intervenuta violazione dei Suoi dati personali (Data Breach) che si è verificata in data _____, alle ore_____; di cui si è avuto conoscenza in data_____, alle ore_____.

DESCRIZIONE DELLA NATURA DELLA VIOLAZIONE

Dove è avvenuta la violazione	*Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili*
Tipo di violazione	*Per esempio:* ✓ *Lettura (presumibilmente i dati non sono stati copiati)* ✓ *Copia (i dati sono ancora presenti sui sistemi del Titolare)* ✓ *Alterazione (i dati sono presenti sui sistemi del Titolare ma sono stati alterati)* ✓ *Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)* ✓ *Furto (i dati non sono più sui sistemi del Titolare e li ha l'autore della violazione)*

Dispositivo oggetto di violazione	*Per esempio:* ✓ *Computer* ✓ *Rete* ✓ *Dispositivo mobile* ✓ *Strumento di backup* ✓ *Documento cartaceo*
Tipo di dati oggetto di violazione	*Per esempio:* ✓ *Dati anagrafici (nome, cognome, telefono, mail, CF, indirizzo…)* ✓ *Dati di accesso e di identificazione (username, password, ID,…)* ✓ *Dati personali idonei a rivelare l'origine razziale ed etnica;* ✓ *Dati personali idonei a rivelare le convinzioni religiose;* ✓ *Dati personali idonei a rivelare convinzioni filosofiche o di altro genere;* ✓ *Dati personali idonei a rivelare le opinioni politiche;* ✓ *Dati personali idonei a rivelare l'adesione a partiti;* ✓ *Dati personali idonei a rivelare l'adesione a sindacati;* ✓ *Dati personali idonei a rivelare l'adesione ad associazioni od organizzazioni a carattere religioso;* ✓ *Dati personali idonei a rivelare l'adesione ad associazioni od organizzazioni a carattere filosofico;* ✓ *Dati personali idonei a rivelare l'adesione ad associazioni od organizzazioni a carattere sindacale;* ✓ *Dati personali idonei a rivelare lo stato di salute;* ✓ *Dati personali idonei a rivelare la vita sessuale;* ✓ *Dati giudiziari;* ✓ *Dati genetici;* ✓ *Dati biometrici;* ✓ *Copia per immagine su supporto informatico di documenti analogici;* ✓ *Ancora sconosciuto.*

Tale violazione è suscettibile di presentare un rischio elevato per Suoi diritti e le libertà.

DESCRIZIONE DELLE CONSEGUENZE DELLA VIOLAZIONE

Descrivere le probabili conseguenze della violazione dei dati personali

DESCRIZIONE DELLE MISURE TECNOLOGICHE E ORGANIZZATIVE ASSUNTE

Descrivere quali sono le misure tecnologiche e organizzative assunte per porre rimedio alla violazione e, se del caso, per contenere la violazione dei dati o per attenuarne i possibili effetti negativi

Per poter ottenere maggiori informazioni relativamente alla violazione in oggetto, può contattare l'ufficio scrivente del Responsabile della Protezione dei Dati – RPD (nell'accezione inglese: *Data Protection Officier – DPO*), i cui dati di contatto sono i seguenti:

Azienda Sanitaria Provinciale di Siracusa

Alla cortese att.ne del

Responsabile della Protezione dei Dati

Corso Gelone, 17 – 96100 Siracusa (SR)

e-mail: **rpd@asp.sr.it**

Siracusa, _____

Il Responsabile della Protezione dei Dati

IX. Glossario

Di seguito un breve glossario dei termini informatici utilizzati nella presente relazione. Per una più consultazione più completa si faccia riferimento alla piattaforma Wikipedia consultabile all'indirizzo web: http://it.wikipedia.org.

Termine	Significato
Archivio	Qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
Aree Sensibili	Sono quei luoghi fisici o della Rete in cui vengono trattati Dati Particolari e/o Dati Giudiziari relativi a persone fisiche e/o luoghi in cui vengono gestiti e consultati documenti riservati a cui è assolutamente vietato accedere se non per motivi di servizio;
Autorità Garante Privacy	L'autorità istituita dalla legge 31 dicembre 1996, n. 675 che rappresenta l'attuazione, a livello nazionale, di quanto previsto dall'articolo 51 del GDPR, deputata alla sorveglianza dell'applicazione del regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche coinvolte nel trattamento di dati personali, nonché di agevolare la libera circolazione dei dati personali all'interno dell'Unione Europea;
Autorità Giudiziaria	Autorità giurisdizionale competente;
Comunicazione	Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Consenso dell'Interessato	Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che lo riguardano siano oggetto di trattamento.
Credenziali di autenticazione	Consistono in un codice per l'identificazione dell'Incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'Incaricato, eventualmente associato a un codice identificativo o a una parola chiave;
Data di Cessazione	Data di cessazione, per qualsivoglia motivo, degli effetti del presente Contratto di Nomina;
Dato Anonimo	il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
Dati Biometrici	I dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

Dati Comuni	Sotto tutti i Dati Personali che non appartengono alle categorie dei Dati Particolari e Dati Giudiziari;
Dati Genetici	I dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
Dati Giudiziari	I dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza;
Dati identificativi	I dati personali che permettono l'identificazione diretta dell'interessato;
Dati Personali	Ai sensi dell'articolo 4 del GDPR, i dati personali sono "qualsiasi informazione riguardante una persona fisica identificata o identificabile; 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"
Dati relativi alla salute	i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rilevano informazioni relative al suo stato di salute;
Dati Sensibili/Particolari	I dati personali idonei a rilevare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale. I dati di salute non possono essere diffusi. I dati sensibili sono oggetto di comunicazione anche attraverso soggetti pubblici solo se previsto da legge e/o Regolamento;
Delegato e Incaricato o Persona/e Autorizzata/e	Si tratta dei Collaboratori autorizzati al trattamento dei dati personali sotto la diretta autorità del Titolare e/o del Responsabile ex artt. 4 e 29 del GDPR. Stante la definizione fornita dal Gruppo di Lavoro Articolo 29 dell'opinione 2/2017, questa definizione ricomprende: dipendenti ed ex dipendenti, dirigenti, collaboratori e lavoratori a partita IVA, part-time, contratti a termine, stage, senza distinzione di ruolo, funzione e/o livello, nonché consulenti e fornitori dell'Azienda e, più in generale, tutti colore che utilizzino ed abbiano utilizzato Strumenti Aziendali o Strumenti Personali, operino sulla Rete ovvero siano a conoscenza di informazioni aziendali rilevanti quali, a titolo esemplificativo e non esaustivo: (a) i Dati Personali di utenti/clienti, dipendenti e fornitori, compresi gli indirizzi di posta elettronica; (b) tutte le informazioni aventi ad oggetto informazioni confidenziali di natura finanziaria nonché (c) i dati e le informazioni relative ai processi aziendali.
Destinatario/i	La persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di Dati Personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di Dati Personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate Destinatari; il Trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del Trattamento;

Diffusione	Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Dispositivi Fissi	Si intendono gli strumenti informatici non facilmente removibili dal perimetro aziendale quali personal computer, server locali, stampanti affidati alle Persone Autorizzate per uso professionale;
Dispositivi Mobili	In generale si intendono quegli strumenti informatici che per loro natura sono facilmente asportabili dal perimetro aziendale quali chiavette USB, Hard Disk esterni, Tablet e Smartphone utilizzati dalle Persone Autorizzate per uso professionale;
GDPR o Regolamento	Il Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;
Interessati	Le categorie di persone fisiche a cui si riferiscono i dati Personali oggetto del Trattamento cui il Responsabile avrà accesso al fine di svolgere i Servizi;
Istruzioni	Le istruzioni dettagliate, che il Titolare fornisce;
Limitazione di trattamento	Il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro:
Normativa Privacy	Le disposizioni applicabili in materia di protezione dei dati personali previste dal GDPR e da ogni previsione normativa in vigore e/o che dovesse essere successivamente emanata, nonché i provvedimenti emanati dal Garante Privacy, dall'Article 29 Working Party e dal Comitato europeo per la protezione dei dati;
Personale	Il personale del Responsabile, ivi inclusi dipendenti, agenti, consulenti, stagisti e collaboratori, coinvolti in relazione allo svolgimento dei Servizi;
Profilazione	Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica:
Pseudonimizzazione	Il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'ausilio di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati non siano attribuiti a una persona fisica identificata o identificabile;
Provvedimento	Il provvedimento del 27 novembre 2008, comprensivo di successive modifiche, con il quale il Garante Privacy ha dettato misure ed accorgimenti per i titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema. In particolare, ai sensi del paragrafo d), del provvedimento, "nel caso di servizi di amministrazione di sistema affidati in outsourcing, il titolare o il responsabile esterno devono conservare direttamente e specificamente, per ogni

	eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema"
Registro dei Trattamenti	Il Registro delle attività di trattamento tenuto dal responsabile in ottemperanza a quanto prescritto dall'articolo 30 del GDPR;
Responsabile del Trattamento	L'articolo 4, comma 1, punto 8) del GDPR definisce Responsabile del Trattamento la "persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento";
Responsabile delle Protezione dei Dati (RPD) – o Data Protection Officier (DPO)	È una persona fisica, nominata obbligatoriamente nei casi di cui all'art. 37 del Regolamento europeo n. 679/2016 dal Titolare o dal Responsabile del trattamento e deve possedere una conoscenza specialistica della normativa e delle partiche in materia di protezione dei dati per assisterli nel rispetto, a livello interno, del predetto Regolamento.
Rete	Rappresenta il perimetro digitale dell'Azienda contenente Dati Personali e/o informazioni riservate comprensivo della rete interna (intranet) e della rete esterna (internet);
Servizi	Le prestazioni che il Responsabile deve svolgere in favore del Titolare ai sensi del Contratto, ivi inclusi gli applicativi informatici attraverso i quali tali prestazioni vengono erogate, e indicate nella relativa sezione del registro dei trattamenti del titolare;
Sub-responsabile	Soggetti terzi di cui il Responsabile si avvale per l'esecuzione dei Trattamenti dei dati Personali funzionali all'erogazione dei servizi oggetto del Contratto, previa autorizzazione del Titolare;
Strumenti Aziendali	L'insieme di Dispositivi Fissi e Dispositivi Mobili concessi in comodato d'uso dall'Azienda alle Persone Autorizzate al fine di svolgere le proprie mansioni;
Strumenti Personali	I Dispositivi Mobili di proprietà delle Persone Autorizzate, autorizzati ad essere impiegati per uso profesionale;
Terzo	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare dei dati personali sotto l'autorità del Titolare o del Responsabile della Protezione dei Dati;
Titolare del trattamento	"La persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali". In pratica, al Titolare del trattamento, spettano decisioni su come dovrà essere effettuato il trattamento di dati personali;
Trattamenti	Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati;

Violazione dei dati Personali	Ogni violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali.