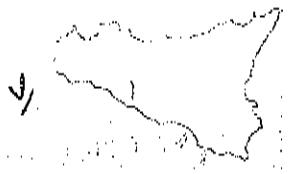


Regione Siciliana

Azienda Sanitaria Provinciale di

AGRIGENTO

DELIBERAZIONE DIREZIONE GENERALE N. 1076 DEL 11 NOV. 2019

OGGETTO: Definizione del nuovo modello organizzativo Privacy aziendale. GDPR 2016/679.

STRUTTURA PROPONENTE: Direzione Generale – Ufficio Privacy

PROPOSTA N.1338 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 UOC SEF e P.
ASP 7 AGRIGENTO
Il Direttore U.O. Patrimonio
Dr. Antonino Fiorentino

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 Mazzarà, 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 con Deliberazione n. 1018 del 25/05/2018 avente ad oggetto "Organizzazione trattamento e protezione dei dati. Nomina del responsabile della protezione dei dati e dei Responsabili del trattamento dei dati, ai sensi del Regolamento (UE) 2016/679", si è provveduto, tra gli altri, a nominare il Dott. Antonino Fiorentino Responsabile della Protezione dei dati e la Dott.ssa M. Giovanna Matteliano supporto al predetto RDP, nelle more dell' istituzione di un apposito Ufficio privacy , incardinato alle dipendenze della Direzione Generale;

Vista

- la necessità di ottemperare agli obblighi imposti dal Regolamento Europeo Privacy UE/2016/679 o GDPR(GeneralDataProtectionRegulation) che stabilisce le nuove norme in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché le norme relative alla libera circolazione di tali dati

Ritenuto,

- necessario realizzare un "modello organizzativo" da implementare in base ad una preliminare analisi dei rischi e ad un'autovalutazione finalizzata all'adozione delle migliori strategie volte a presidiare i trattamenti di dati effettuati, abbandonando l'approccio meramente formale del D.Lgs. 196/2003, limitato alla mera adozione di una lista "minima" di misure di sicurezza, realizzando, piuttosto, un sistema organizzativo caratterizzato da un'attenzione multidisciplinare alle specificità della struttura e della tipologia di trattamento, sia dal punto di vista della sicurezza informatica e in conformità agli obblighi legali, sia in considerazione del modello di archiviazione e gestione dei dati trattati. Tutto questo prevedendo, al contempo, non solo l'introduzione di nuove figure soggettive e professionali che dovranno presidiare i processi organizzativi interni per garantire un corretto trattamento dei dati personali, tra cui la figura del Responsabile della Protezione dei dati personali (DPO), ma altresì l'adozione di nuove misure tecniche e organizzative volte a garantire l'integrità e la riservatezza dei dati, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico, nonché la verifica e la valutazione dell'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;

Verificato

- che il GDPR introduce una nuova terminologia per le figure che rilevano ai fini della privacy e che tale terminologia parzialmente muta la precedente usata nella documentazione interna dell'ASP di Agrigento;

- che si rende necessario ridefinire i ruoli e le responsabilità relative alla privacy per rendere aderente la struttura organizzativa aziendale agli adempimenti previsti dal GDPR;

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;

Considerato

- Il Team RTI Almaviva SPA/Almawave srl./Indra Italia Spa/Pricewaterhouse Coopers Advisory Spa, ha predisposto un modello organizzativo in materia di protezione dei dati personali, sulla base di informazioni già in possesso di questa Azienda e verificate dall'Ufficio Privacy aziendale, che tiene conto degli intervenuti aggiornamenti legislativi – Regolamento UE 2016/679 e D. lgs 196/03 come adeguato con il D. Lgs 101/2018, in vigore dal 19/09/2018;

Ritenuto

- Pertanto, di dovere approvare il modello organizzativo in materia di protezione dei dati personali al fine di formalizzare le linee guida che l'ASP di Agrigento intende applicare per assicurare che i trattamenti di dati personali di cui è titolare siano effettuati in conformità alle disposizioni previste dal Regolamento UE 2016/679 e dal Codice Privacy come adeguato con il D.LGS 101/2018;

PROPONE

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

- Di approvare il modello organizzativo in materia di protezione dei dati personali (Allegato A) al fine di formalizzare le linee guida che l'ASP di Agrigento intende applicare per assicurare che i trattamenti di dati personali di cui è titolare siano effettuati in conformità alle disposizioni previste dal Regolamento UE 2016/679 e dal Codice Privacy come adeguato con il D.LGS 101/201, modello elaborato dal Team RTI Almaviva SPA/Almawave srl./Indra Italia Spa/Pricewaterhouse Coopers Advisory Spa e verificato dall'Ufficio Privacy;
- Di precisare:
    1. Che il "modello organizzativo" abbandona l'approccio meramente formale del D.Lgs. 196/2003, limitato alla mera adozione di una lista "minima" di misure di sicurezza, e realizza, piuttosto, un sistema organizzativo caratterizzato da un'attenzione multidisciplinare alle specificità della struttura e della tipologia di trattamento, sia dal punto di vista della sicurezza informatica e in conformità agli obblighi legali, sia in considerazione del modello di archiviazione e gestione dei dati trattati. Tutto questo prevedendo, al contempo, non solo l'introduzione di nuove figure soggettive e professionali che dovranno presidiare i processi organizzativi interni per garantire un corretto trattamento dei dati personali, tra cui la figura del

Responsabile della Protezione dei dati personali (DPO), ma altresì l'adozione di nuove misure tecniche e organizzative volte a garantire l'integrità e la riservatezza dei dati, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico, nonché la verifica e la valutazione dell'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;

- Di disporre la pubblicazione del presente atto, nonché dell' allegato A del precedente punto 1 del dispositivo, sul sito web aziendale, Sezione Privacy;
- Munire il presente atto della clausola di immediata esecutività, al fine di dare avvio al sistema aziendale privacy in conformità con l'intervenuto quadro normativo di riferimento;
- 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 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 di 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 SEGRETERIA ATTI, PROPOSTE
DI ATTI E DELIBERA
Dott.ssa Patrizia Tedesco

ALL. A

Modello organizzativo in materia

di protezione dei dati personali

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

1. INTRODUZIONE

Il presente documento descrive il modello organizzativo di cui si è dotata l'Azienda Sanitaria Provinciale di Agrigento (di seguito anche "ASP Agrigento") in riferimento ai trattamenti di dati personali di soggetti persone fisiche, in coerenza alla normativa vigente, tra cui, in particolare, il Regolamento europeo 2016/679 (di seguito, per brevità, "Regolamento" o "GDPR").

Inoltre, all'interno del presente documento, è descritta la struttura organizzativa dell'ASP Agrigento, i ruoli e le responsabilità dei soggetti che effettuano i trattamenti, nonché i principi che regolamentano e disciplinano le modalità di esecuzione delle attività di trattamento di dati personali eseguite.

Il modello organizzativo ivi descritto ha l'obiettivo di formalizzare le linee guida che ASP Agrigento ha adottato e intende applicare per assicurare che i trattamenti di dati personali di cui è titolare siano effettuati in conformità alle disposizioni previste dalla normativa in materia.

Tale politica si applica a tutti i dipendenti e collaboratori dell'ASP Agrigento. A tal fine, ASP Agrigento si assicura che, al momento dell'assunzione, ciascun dipendente e / o collaboratore riceva una copia del presente documento, dichiarando di averne preso visione.

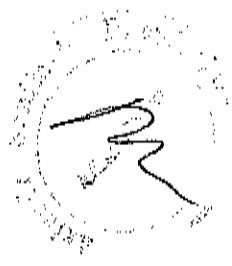
Per la descrizione e la trattazione di dettaglio dei processi aziendali connessi ai trattamenti di dati personali quali, a titolo esemplificativo e non esaustivo, la valutazione d'impatto sulla protezione dei dati personali (DPIA) o la gestione e notifica delle violazioni di dati personali (Data Breach), si fa rimando agli appositi documenti.

2. TERMINI E DEFINIZIONI

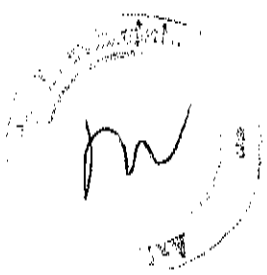
Al fine di una piena comprensione e attuazione del presente documento, si riportano i principali termini utilizzati e le relative definizioni:

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 i dati personali che lo riguardano siano oggetto di trattamento.
Dati biometrici	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, ad esempio, l'immagine facciale o i dati dattiloscopici.
Dati genetici	Dati personali relativi alle caratteristiche genetiche ereditarie o acquisite dell'interessato idonei a fornire informazioni univoche sulla fisiologia o sulla salute e che risultano in particolare dall'analisi di un campione biologico della persona fisica.
Dati giudiziari	Dati personali idonei a rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato.
Dati personali	Qualunque informazione relativa a persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, mediante riferimento a qualsiasi altra informazione, 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, generica, 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, idonei a rivelare informazioni relative al suo stato di salute, ad esempio, certificato medico, cartella clinica, etc.
Dati sensibili	Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

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.
Autorizzato	La persona fisica autorizzata a compiere operazioni di trattamento dal Titolare o dal Responsabile.
Informativa	Informazioni che il Titolare del trattamento deve fornire ad ogni interessato, verbalmente o per iscritto, quando i dati sono raccolti presso l'interessato stesso oppure presso terzi. L'informativa deve precisare sinteticamente e in modo colloquiale: quali sono gli scopi e le modalità del trattamento; se l'interessato è obbligato o no a fornire i dati; quali sono le conseguenze se i dati non vengono forniti; a chi possono essere comunicati o diffusi i dati; quali sono i diritti riconosciuti all'interessato; chi sono il Titolare e l'eventuale Responsabile del trattamento e dove sono raggiungibili (indirizzo, telefono, fax, etc.).
Interessato	La persona fisica cui si riferiscono i dati personali.
Privacy by Design e by Default	Configurare il trattamento dei dati personali prevedendo, fin dalle fasi di progettazione, misure indispensabili per soddisfare i requisiti del regolamento e tutelare i diritti degli interessati. Ciò richiede un'analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili.



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.
Rischio	Scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità.
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.
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.



3. STRUTTURA ORGANIZZATIVA E RUOLI

3.1 TITOLARE DEL TRATTAMENTO

Titolare del trattamento dei dati personali è, ai sensi dell'art. 4 del GDPR, "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali*" ("**Titolare**").

Alla luce della suddetta definizione, ASP Agrigento risulta Titolare dei trattamenti di dati personali effettuati e mappati nel relativo Registro delle attività di trattamento e relativamente ai quali determina finalità e modalità di trattamento.

Il Titolare è la struttura nel suo complesso e cioè il soggetto al quale competono le scelte di fondo sulla raccolta e sull'utilizzazione dei dati personali. Il Titolare agisce per mezzo del Direttore Generale *pro tempore*. Tuttavia, non devono essere considerati come Titolari le singole persone fisiche che amministrano l'ASP Agrigento o che la rappresentano, quali ad esempio il Direttore Generale.

L'art. 24 GDPR stabilisce la responsabilità generale del Titolare per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. In particolare, il Titolare deve essere in grado di dimostrare la conformità delle attività di trattamento con il GDPR stesso e deve mettere in atto misure adeguate ed efficaci volte a garantire ciò. Tali misure devono tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.

Inoltre, al fine di dimostrare la conformità delle sue azioni con il GDPR, il Titolare deve adottare politiche interne e attuare misure che soddisfino i principi della protezione dei dati di *default* e fin dalla progettazione.

Il Titolare delega lo svolgimento di parte delle proprie attività a soggetti interni (i.e.: Delegati Interni al trattamento e soggetti Autorizzati al trattamento), nonché nomina Responsabili del trattamento i soggetti esterni che, nell'esecuzione di un servizio a favore di ASP Agrigento, trattano i dati personali in titolarità di ASP Agrigento. Il Titolare ha la responsabilità di individuare al riguardo soggetti che presentino garanzie sufficienti per mettere in atto le prescritte misure tecniche e organizzative adeguate.

3.2 DPO - DATA PROTECTION OFFICER

ASP Agrigento, in adempimento a quanto previsto dal Regolamento, ha provveduto alla nomina di un DPO interno alla propria organizzazione.

Fermo restando quanto sopra, il Titolare deve, inoltre, accertare che il soggetto individuato non sia tra coloro che svolgono un ruolo che comporta la definizione delle finalità o modalità del trattamento dei dati personali, in quanto ciò determinerebbe una situazione di conflitto d'interessi e, quindi, una violazione del requisito dell'indipendenza.

A tal fine, si ritengono senz'altro in conflitto d'interessi le seguenti posizioni di management di alto livello: Direttore Generale, Direttore Amministrativo e Direttore Sanitario, non escludendo comunque a priori che conflitti si possano determinare anche con posizioni diverse, anche di livello e funzioni inferiori, nonché in caso di DPO di nomina esterna.

La scelta del DPO in ASP Agrigento avviene a seguito di una analisi effettuata sulla base dei seguenti parametri:

a) conoscenza specialistica della normativa e della prassi in materia di protezione dei dati personali, eventualmente anche attraverso lo svolgimento di specifici corsi di formazione;
b) conoscenza dello specifico settore di attività e della struttura organizzativa di ASP Agrigento, buona familiarità con le operazioni di trattamento svolte, nonché con i sistemi informativi e le esigenze di sicurezza;
c) caratteristiche personali di integrità ed etica professionale;
d) posizionamento di rilievo all'interno dell'organizzazione che gli consenta di interagire direttamente con i vertici in una condizione di indipendenza;
e) tempo a disposizione sufficiente per lo svolgimento dei compiti demandati al ruolo ricoperto;
f) compatibilità delle ulteriori mansioni svolte, affinché queste non determinino una situazione di "conflitto di interessi".

ASP Agrigento designa il DPO con apposito atto di nomina, disciplinante l'attribuzione dei relativi compiti, poteri, durata, cessazione del rapporto e responsabilità.

ASP Agrigento, inoltre, ha assicurato l'adozione di misure idonee a garantire che il DPO:

- possa usufruire di adeguate infrastrutture e risorse umane e finanziarie, nonché, a seconda delle eventuali ulteriori funzioni svolte dal soggetto di volta in volta designato, di tempo sufficiente per l'espletamento dei suoi compiti. Le infrastrutture e le risorse attribuite al DPO e al suo eventuale team devono essere rivalutate con cadenza annuale alla luce della complessità e/o sensibilità dei trattamenti effettuati da ASP Agrigento;
- abbia una posizione tale da poter interagire direttamente con i vertici gerarchici di ASP Agrigento e, se consulente esterno, gli sia garantita la possibilità di avere un contatto diretto con gli stessi;
- non riceva alcuna istruzione operativa e/o strategica per l'esecuzione dei suoi compiti;
- non sia rimosso o penalizzato professionalmente in conseguenza dello svolgimento dei suoi compiti;
- abbia accesso ai dati personali e ai trattamenti effettuati dalla società, al fine di mantenere la propria conoscenza specialistica dell'organizzazione privacy di ASP Agrigento;
- se dipendente, sia messo nella condizione di poter curare il proprio aggiornamento in materia di protezione dei dati personali, partecipando ad appositi corsi di formazione che accrescano di continuo il livello delle proprie competenze.

In seguito alla designazione, ASP Agrigento provvede a:

a) comunicare ufficialmente la nomina a tutto il personale, in modo da garantire che il ruolo e le funzioni del DPO siano note a tutta la società;

b) pubblicarne i dati di contatto, in modo che questi siano accessibili da parte degli interessati (a titolo esemplificativo e non esaustivo: sul sito Internet e sulle informative rese agli interessati);

c) comunicare i dati di contatto all'Autorità di Controllo.

Con specifico riferimento a quanto previsto alle precedenti lettere b) e c), i dati di contatto del DPO dovrebbero comprendere tutte quelle informazioni che consentono agli interessati e all'Autorità di Controllo di raggiungere facilmente il DPO (i.e. recapito postale e/o indirizzo e-mail dedicato).

Il DPO è tenuto ad assolvere gli obblighi enucleati dall'art. 39 del Regolamento e di seguito indicati:

a) informare e fornire consulenza al Titolare nonché ai dipendenti in merito agli obblighi derivanti dalla normativa in materia di protezione dei dati personali;

b) sorvegliare l'osservanza del Regolamento e della normativa privacy in generale, nonché delle politiche del Titolare in materia di protezione dei dati, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle attività di controllo connesse;

c) fornire, qualora fosse richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;

d) cooperare con l'Autorità di Controllo;

e) fungere da punto di contatto per l'Autorità di Controllo per questioni connesse al trattamento ed effettuare consultazioni relativamente a qualunque altra questione e, per gli interessati, anche in merito all'esercizio dei diritti ad essi attribuiti dal Regolamento.

f) tenere il Registro delle attività di trattamento.

Fermo restando quanto sopra, il DPO riferisce direttamente al vertice gerarchico di ASP Agrigento ogni problematica, violazione ed esigenza, rispettando il segreto e la riservatezza in merito all'adempimento dei propri compiti.

Inoltre, al fine di consentire al DPO di svolgere i compiti sopra elencati, ASP Agrigento tutta e, in particolare, gli Autorizzati devono porre in essere tutte le misure idonee a far sì che esso sia tempestivamente ed adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali e, in particolare, garantire che:

- in ottemperanza al principio di *privacy by design* di cui all'art. 25 del GDPR, il DPO sia invitato a partecipare su base regolare alle riunioni in cui siano assunte decisioni che impattano sulla protezione dei dati personali;
- i pareri espressi dal DPO ricevano sempre la dovuta considerazione. Laddove si dovesse verificare una circostanza che determina un disaccordo tra i Responsabili di processo e la posizione del DPO, ASP Agrigento deve documentare le motivazioni che hanno portato all'adozione della condotta difforme da quella raccomandata dal DPO;
- il DPO sia tempestivamente informato e consultato nell'eventualità in cui si verifichi una violazione dei dati o altro incidente avente ad oggetto gli stessi.

Nello svolgimento dei compiti sopra indicati, il DPO deve adottare un approccio basato sul rischio, definendo sempre un ordine di priorità delle attività da svolgersi e concentrandosi sulle questioni che presentino maggiori rischi per la protezione dei dati. Fermo restando ciò, il DPO non deve in ogni caso mancare di sorvegliare il grado di conformità anche dei trattamenti associati ad un livello di rischio comparativamente inferiore.

3.3 DELEGATO INTERNO DEL TRATTAMENTO

Considerata la complessità della struttura aziendale e i trattamenti di dati personali effettuati dal Titolare, quest'ultimo ravvisa la necessità di nominare uno o più **Delegati interni del trattamento** dei dati personali che lo affianchino, al fine di garantire il pieno rispetto dei principi e delle disposizioni di cui al GDPR.

La designazione di un Delegato interno del trattamento non appare incompatibile con il dettato del GDPR, in particolare con riferimento a strutture organizzative di particolare complessità ove risulta opportuno definire una struttura privacy adeguata che permetta di stabilire in modo puntuale i ruoli e le responsabilità dei soggetti che trattano i dati personali in titolarità dell'ASP Agrigento.

Ciò posto, il Delegato interno del trattamento deve essere individuato e nominato con apposito atto dal Titolare, in ragione delle competenze dimostrate in termini di affidabilità, esperienza e capacità nello svolgimento dei compiti cui è preposto. Ai fini di individuare il soggetto idoneo a cui indirizzare la nomina a Delegato interno del trattamento, il Titolare dovrà altresì tenere in considerazione l'adeguatezza delle garanzie prestate dal soggetto in ordine al rispetto delle vigenti disposizioni in materia di protezione dei dati personali, con particolare riferimento al profilo della sicurezza.

In aggiunta, in riferimento ai criteri utilizzati ai fini dell'identificazione del Delegato interno del trattamento, si precisa che le nomine saranno conferite tenuto conto del ruolo e delle mansioni attribuite al dipendente nel contratto di lavoro in essere tra lo stesso e il Titolare; inoltre, il Delegato interno del trattamento sarà individuato nella persona del Direttore ovvero del Responsabile della Funzione impattata dai trattamenti che, alla luce del Registro delle attività di trattamento predisposto dal Titolare e mantenuto dal DPO, risultano essere riconducibili alla Funzione stessa.

In tale contesto, il Delegato interno del trattamento si impegnerà ad adempiere alle istruzioni enucleate e descritte nell'atto di nomina.

3.4 PERSONA AUTORIZZATA AL TRATTAMENTO (INCARICATO)

ASP Agrigento, in qualità di Titolare, ravvisa la necessità di individuare i soggetti interni da autorizzare a compiere operazioni di trattamento di dati personali contenuti in banche dati elettroniche e/o cartacee.

Ai sensi della normativa vigente, tali soggetti sono designati "Autorizzati" o "Incaricati", ovvero "le *persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare del trattamento*".

Pertanto, in ottemperanza a quanto previsto dalle disposizioni normative, ogni dipendente o collaboratore del Titolare che, per le mansioni assegnate, debba trattare dati personali, deve essere designato per iscritto mediante una lettera di conferimento dell'incarico al trattamento dei dati personali, con la specificazione, anche per gruppi omogenei di lavoro, dei compiti che gli sono affidati, nonché delle banche dati cui avrà accesso nello svolgimento delle proprie mansioni.

La designazione dell'Autorizzato, di competenza di ciascun Delegato interno del trattamento, sarà effettuata in ragione della subordinazione del dipendente al Direttore ovvero al Responsabile della Funzione a cui è addetto il soggetto individuato come Incaricato.

Al momento dell'assunzione di nuovo personale addetto alle funzioni preposte al trattamento dei dati personali, il Delegato interno del trattamento dei dati personali dei dipendenti (Responsabile Risorse Umane) – dopo essersi coordinato con il Delegato interno del trattamento della Direzione o Funzione di destinazione iniziale - provvede alla consegna della relativa lettera di designazione ad "Autorizzato" o "Incaricato", così come di volta in volta integrato sulla base del dettaglio delle attività di trattamento autorizzate in funzione dell'unità organizzativa di pertinenza (le "Istruzioni per unità").

È onere del singolo incaricato, in ipotesi di trasferimento ad una diversa funzione, prendere prontamente visione delle Istruzioni per unità contenute nell'apposita sezione della Intranet aziendale.

3.5 RESPONSABILE (ESTERNO) DEL TRATTAMENTO

ASP Agrigento, in qualità Titolare, per effetto della conclusione ed esecuzione di specifici contratti, ha demandato alcuni servizi che prevedono il trattamento di dati personali in sua titolarità a soggetti esterni alla propria struttura. In tali casi, i soggetti esterni sono nominati Responsabili del trattamento, intesi, ai sensi dell'art. 4 del GDPR, come "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*".

Il Responsabile esterno del trattamento deve essere nominato, con apposito contratto o atto giuridico, dal DPO, in considerazione delle esigenze manifestate dalle singole Direzioni aziendali in merito all'esigenza di esternalizzare alcuni servizi che prevedono il trattamento di dati personali.

Secondo la normativa vigente, il Responsabile esterno è tenuto a presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato.

Il Responsabile esterno, inoltre, non può ricorrere ad un altro Responsabile senza previa autorizzazione scritta, specifica o generale, di ASP Agrigento. In caso di autorizzazione, il Responsabile esterno è tenuto a nominare il subfornitore Responsabile del trattamento e ad imporre allo stesso, tramite contratto o atto giuridico, i medesimi doveri in materia di protezione dei dati personali che il Titolare gli ha prescritto.

I trattamenti da parte di un Responsabile esterno del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri; tale contratto tra ASP Agrigento ed il Responsabile esterno del trattamento, oltre a vincolare a vicenda le due figure, deve prevedere la materia disciplinata, la durata del trattamento, la natura e le finalità del trattamento nonché il tipo di dati personali e le categorie di interessati a cui gli stessi dati si riferiscono.

Il GDPR prevede una serie di condizioni in rapporto ai criteri di selezione, individuazione e nomina del Responsabile esterno, come trattato in dettaglio nel successivo capitolo 4 "*Processo di nomina del Responsabile esterno del trattamento*".

4. PROCESSO DI NOMINA DEL RESPONSABILE ESTERNO DEL TRATTAMENTO

Come anticipato al precedente capitolo 3, il ruolo di Responsabile Esterno del trattamento dei dati è attribuito ai soggetti esterni a ASP Agrigento (*e.g.* fornitori esterni) cui vengono delegate attività di competenza aziendale o che svolgono attività connesse, strumentali e di supporto, ivi incluse le attività manutentive, che comportano l'uso di dati personali, comuni e/o sensibili di cui ASP Agrigento è Titolare.

Ogniqualvolta un trattamento di dati personali sia effettuato per conto di ASP Agrigento da parte di un soggetto terzo, gli Autorizzati o Incaricati della Direzione aziendale di volta in volta coinvolta sono tenuti a darne comunicazione, senza ritardo, al Delegato interno del trattamento che si attiverà per svolgere le necessarie valutazioni, condividendole con il DPO. In particolare, gli Incaricati devono fornire ogni informazione relativa al trattamento oggetto dell'esternalizzazione, ivi inclusa: l'indicazione della tipologia dei dati trattati, le finalità del trattamento, le categorie di interessati coinvolte, etc.

Sulla base di tali informazioni, sotto la guida del DPO, deve essere verificato che il soggetto individuato possieda caratteristiche idonee a garantire un livello di protezione dei dati personali in titolarità di ASP Agrigento adeguato, anche sotto il profilo della sicurezza, coinvolgendo eventualmente il Responsabile dei Sistemi Informativi qualora i dati vengano conservati su o trattati mediante sistemi informativi.

Una volta verificato il possesso da parte del soggetto delle caratteristiche idonee ad assicurare che il trattamento di dati esternalizzato sia effettuato in conformità ai requisiti normativi applicabili, devono essere posti in essere tutti gli adempimenti necessari a far sì che il trattamento dei dati di ASP Agrigento da parte di tale soggetto sia disciplinato da un apposito contratto che vincoli il terzo agli obblighi ed alle istruzioni imposte dal Titolare.

Il contratto o altro atto giuridico deve prevedere, in particolare, che il Responsabile esterno:

- tratti i dati personali soltanto su istruzione documentata di ASP Agrigento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa ASP Agrigento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
- garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- adotti tutte le misure richieste ai sensi dell'articolo 32 del GDPR;
- rispetti le condizioni di cui ai par. 2 e 4, art. 28 del GDPR per ricorrere a un altro responsabile del trattamento;
- tenendo conto della natura del trattamento, assista ASP Agrigento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
- assista ASP Agrigento nel garantire il rispetto degli obblighi di cui agli artt. 32 - 36 del GDPR, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

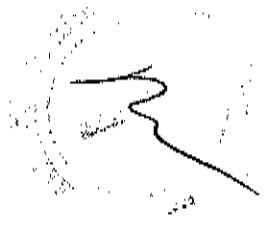
- su scelta di ASP Agrigento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e
- metta a disposizione di ASP Agrigento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzate dal titolare del trattamento o da un altro soggetto da questi incaricato.

Tale contratto deve, altresì, prevedere il diritto di ASP Agrigento di risolvere il contratto stesso in caso di inadempimento da parte del soggetto designato agli obblighi previsti in forza dell'atto di nomina.

Il DPO provvede infatti a effettuare, per conto di ASP Agrigento, una verifica sull'operato dei Responsabili del trattamento, al fine di monitorare il rispetto della normativa in materia di protezione dei dati personali e delle istruzioni impartite.
Il DPO effettuerà le verifiche secondo una logica *risk based* e sulla base di un piano e di una metodologia che avrà cura di definire.
Qualora dalle verifiche risultassero fattori di criticità, il DPO valuta eventuali azioni per la loro mitigazione avvalendosi, se necessario, della consulenza dei Delegati interni del trattamento coinvolti. In caso di inadempimento grave e non risolvibile da parte del Responsabile degli obblighi ad esso imposti, come già detto in precedenza, il DPO pone in essere tutte le azioni necessarie a determinare la cessazione degli effetti dell'atto stesso, nonché del contratto di servizi sottoscritto con il Responsabile.

La designazione del Responsabile esterno è di competenza del DPO per conto del Titolare. La designazione è effettuata tramite atto di nomina, individuando le istruzioni cui il Responsabile esterno dovrà attenersi nel trattamento dei dati in titolarità di ASP Agrigento. Tale atto di nomina deve essere allegato al contratto tra ASP Agrigento ed il Responsabile esterno.

Il DPO è tenuto, inoltre, all'aggiornamento tempestivo del Registro dei Trattamenti di ASP Agrigento con le informazioni relative al Responsabile esterno del trattamento designato e alle caratteristiche del trattamento effettuato, in ottemperanza a quanto disposto dal "*Mantenimento del Registro delle attività di trattamento*" di cui al capitolo 8 della presente *policy*.



5. PRINCIPI APPLICABILI AL TRATTAMENTO DI DATI PERSONALI

TRATTAMENTO DI DATI PERSONALI

Ai sensi dell'art. 4 del Regolamento, con l'espressione "trattamento di dati personali" s'intende "*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*", in particolare:

a) la **raccolta** dei dati;
b) la **registrazione** dei dati, ovvero il loro inserimento su supporti, automatizzati o manuali, al fine di rendere i dati disponibili per successivi trattamenti;
c) l'**organizzazione** dei dati in senso stretto, ovvero il permesso di lavorazione che ne favorisca la fruibilità attraverso l'aggregazione o la disaggregazione, l'accorpamento, la catalogazione etc.;
d) la **conservazione** dei dati alla quale la legge dedica particolari attenzioni sotto il profilo della sicurezza;
e) l'**adattamento** o la **modifica** dei dati registrati in relazione a variazioni o a nuove acquisizioni;
f) l'**estrazione**, ipotesi specifica che rientra nell'ipotesi più generale dell'elaborazione;
g) la **consultazione**;
h) l'**uso**;
i) la **comunicazione**, ovvero la trasmissione dei dati ad uno o più soggetti determinati, in qualunque forma, mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione; non è comunicazione la trasmissione dei dati allo stesso interessato, al Delegato interno, al Responsabile e agli Incaricati del trattamento;
j) il **raffronto** o l'**interconnessione**, ovvero la messa in relazione di banche dati diverse e distinte fra loro al fine di compiere ulteriori processi di elaborazione, selezione, estrazione o raffronto;
k) la **limitazione**;
l) la **cancellazione**;
m) la **distruzione**.

Il trattamento di dati personali è esercitabile solo da parte del Titolare, dei Delegati interni, dei Responsabili esterni e degli Autorizzati o Incaricati. Non è consentito il trattamento da parte di persone non autorizzate. Il trattamento dei dati, anche di natura sensibile o giudiziaria, effettuato da ASP Agrigento è diretto all'espletamento delle finalità strettamente connesse ad attività di cura e di assistenza.

In particolare, a titolo esemplificativo e non esaustivo, per le attività di: erogare servizi di assistenza e cura sanitaria, conclusione, gestione ed esecuzione dei contratti, instaurazione e di gestione dei rapporti di lavoro con i propri dipendenti.

I dati personali oggetto del trattamento, come previsto dall'art. 5 del GDPR, devono essere:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza");
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità ("limitazione delle finalità");

- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati");
- esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ("esattezza");
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati ("limitazione della conservazione");
- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

ASP Agrigento è competente per il rispetto dei principi sopra elencati tramite l'adozione di misure tecniche e organizzative adeguate e deve essere in grado di dimostrare l'adeguatezza di tali misure.

CONDIZIONI DI LICEITÀ

Come sancito dall'art. 6 del Regolamento, il trattamento è lecito solo se non contrario alle disposizioni di legge e se effettuato nelle ipotesi in cui ricorra almeno una delle seguenti condizioni:

- l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
- il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
- il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
- il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

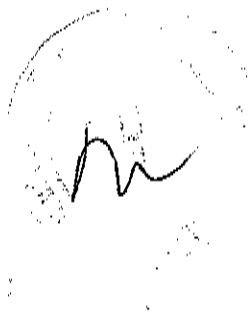
TRASFERIMENTO DI DATI PERSONALI ALL'ESTERO

Come sancito dall'art. 44 del Regolamento "*qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di cui al presente capo, fatte salve le altre disposizioni del presente regolamento*".

In particolare, ASP Agrigento deve tenere in considerazione che il trasferimento – a soggetti stabiliti fuori dall'Unione Europea – di dati personali di cui essa è Titolare richiede, alternativamente, la sussistenza di almeno una delle seguenti condizioni:

a) il trasferimento verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione Europea ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato;

b) nel caso in cui non siano state emanate decisioni di adeguatezza, il trasferimento dei dati personali deve essere effettuato sulla base di accordi contrattuali, stipulati tra ASP Agrigento ed i soggetti destinatari dei dati stabiliti fuori dall'Unione Europea (*e.g.* Responsabili Esterni), che forniscano garanzie adeguate agli utenti (ad esempio l'esercizio da parte di questi dei diritti a loro accordati dal GDPR).



6. PRIVACY BY DESIGN E BY DEFAULT

L'articolo 25 del GDPR pone l'obbligo per ASP Agrigento di:

- mettere in atto misure tecniche ed organizzative adeguate a proteggere i dati personali sia al momento della determinazione dei mezzi di trattamento sia all'atto di trattamento stesso (i.e. principio di "Privacy by Design");
- mettere in atto misure tecniche ed organizzative idonee a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari al perseguimento delle specifiche finalità per cui sono raccolti e per il periodo strettamente necessario a tale fine (i.e. principio di "Privacy by Default")

ASP Agrigento riconosce e promuove il valore e i benefici di un approccio proattivo all'adozione di prassi e tecniche di tutela dei dati personali degli interessati, a partire dalla fase di *design* di nuove iniziative e/o di sistemi, in maniera consistente su tutti i programmi e progetti intrapresi.

A tal fine, i Delegati interni dei trattamenti eseguiti per conto di ASP Agrigento devono considerare la tutela dei diritti e delle libertà degli interessati quale requisito fondamentale nello sviluppo di nuovi servizi e/o trattamenti, riconoscendo i potenziali rischi e le limitazioni che potrebbero derivare per tali diritti e libertà.

In particolare, nello sviluppo di qualsivoglia nuovo servizio o trattamento che abbia ad oggetto un trattamento dei dati personali o nell'ipotesi di modifiche di servizi o trattamenti già realizzati o resi da ASP Agrigento o di cambiamenti significativi nelle modalità di progettazione, produzione, esecuzione e formazione di tali servizi e/o trattamenti, nonché in tutte le occasioni in cui i Delegati interni del trattamento intendano procedere con iniziative di qualsivoglia natura che abbiano come destinatari pazienti, dipendenti o altre categorie di interessati, questi devono provvedere a coinvolgere nel progetto il DPO, in modo tale da eseguire di concerto una valutazione circa gli impatti che potrebbero derivare agli interessati a seguito del trattamento dei dati personali.

PRINCIPIO DI MINIMIZZAZIONE

I Delegati interni del trattamento e gli Autorizzati dovranno attenersi al principio di minimizzazione dei dati, in forza del quale non dovranno essere richiesti agli interessati o, più in generale, non dovranno essere trattati dati personali ulteriori o eccedenti rispetto a quelli strettamente necessari al perseguimento delle finalità di trattamento.

PERIODO DI CONSERVAZIONE DEI DATI PERSONALI

I dati personali raccolti non devono essere trattati per un periodo eccedente quello strettamente necessario per il raggiungimento delle finalità perseguite da ASP Agrigento.

Pertanto, al fine di ottemperare ai principi di Privacy by Design e Privacy by Default, i Delegati interni del Trattamento, fin dalla fase progettuale del servizio, del trattamento e/o iniziativa devono, con il supporto del DPO, svolgere specifiche valutazioni sulla durata del trattamento e relativo periodo di conservazione dei dati personali, anche in virtù di eventuali obblighi di legge.

Sulla base delle risultanze della valutazione svolta, devono essere identificati appositi presidi e processi volti a garantire che i dati personali non siano trattati e conservati per un periodo superiore a quello strettamente necessario al perseguimento delle finalità previste, salvo l'adempimento di specifici obblighi di conservazione imposti dalla legge.

ACCESSO AI DATI PERSONALI

Nello sviluppo del servizio, trattamento e/o iniziativa i Delegati interni del Trattamento, di concerto con il Responsabile dei Sistemi Informativi, dovranno mettere in atto misure tecniche

ed organizzative idonee ad assicurare che, per impostazione predefinita, i dati personali non siano resi accessibili ad un numero indefinito di persone e che, al contrario, l'accessibilità agli stessi sia segregata sulla base del principio di necessità. In tal senso, l'accesso dovrà essere reso disponibile esclusivamente a quei soggetti che sono tenuti al trattamento di quei dati personali per il raggiungimento delle finalità perseguite da ASP Agrigento.

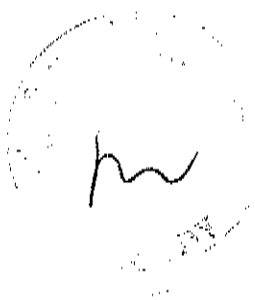
MISURE DI SICUREZZA

I Delegati interni del trattamento, con il supporto del DPO e del Responsabile dei Sistemi Informativi di ASP Agrigento, devono valutare le misure di sicurezza logiche o fisiche da applicare al trattamento, al fine di assicurare che, per impostazione predefinita, siano implementate le più stringenti possibili, individuando specifici presidi volti a prevenire eventi di violazione interni o esterni all'azienda.

Al fine di assicurare un'efficace protezione dei dati personali degli interessati su tutta la filiera di elaborazione e conservazione, ASP Agrigento, mediante il Responsabile dei Sistemi Informativi, deve dotarsi di tecnologie di sicurezza all'avanguardia, non limitandosi a salvaguardare la confidenzialità, l'integrità e la disponibilità delle informazioni per tutto il periodo di durata del trattamento, ma anche assicurando la loro eliminazione sicura o in alternativa la loro anonimizzazione irreversibile, al termine dello stesso, o in seguito a richieste degli interessati, nel rispetto dei diritti all'oblio e alla limitazione.

Sulla base dei suddetti principi, tutte le nuove iniziative che prevedono il trattamento di dati personali devono essere valutate con attenzione dai singoli Delegati interni del trattamento competenti, chiedendo la consulenza del DPO, utilizzando criteri appropriati al grado di sensibilità dei dati stessi e tenendo sempre in considerazione il punto di vista degli interessati, ad esempio la propensione o la reticenza alla condivisione delle informazioni riguardanti la propria sfera personale, al fine di garantirne il rispetto.

Il DPO è tenuto a verificare e monitorare l'effettiva applicazione dei principi di Privacy by Design e Privacy by Default ai processi aziendali, nonché alle iniziative, ai sistemi / applicazioni utilizzati ovvero, in generale, a tutte le attività di trattamento eseguite da ASP Agrigento in qualità di Titolare.



7. GESTIONE DEI DIRITTI DELL'INTERESSATO

Ai sensi della normativa vigente, l'Interessato gode del diritto di:

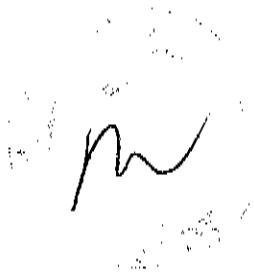
- **ricevere un'informativa** contenente i seguenti elementi:
  - identità e dati di contatto del Titolare;
  - finalità di trattamento cui sono destinati i dati personali, nonché la base giuridica del trattamento;
  - ove applicabile, i legittimi interessi perseguiti dal Titolare o da terzi;
  - i destinatari o le categorie di destinatari dei dati personali;
  - l'intenzione del Titolare di trasferire i dati personali ad un paese terzo o a un'organizzazione internazionale;
  - il periodo di conservazione dei dati personali o, se non è possibile, i criteri utilizzati per determinare tale periodo;
  - la possibilità di esercitare i diritti riconosciuti all'interessato, ivi inclusi il diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento e il diritto di proporre reclamo all'Autorità di Controllo;
  - la natura obbligatoria o facoltativa del conferimento dei dati;
- **revocare**, in qualsiasi momento, **il consenso**, senza alcun condizionamento e con la stessa facilità con cui è stato prestato;
- **accesso**, consistente nell'ottenere da ASP Agrigento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso a tali dati – compresa una copia degli stessi – ed alle informazioni elencate all'articolo 15 GDPR;
- **rettifica**, consistente nella possibilità di ottenere da ASP Agrigento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo e/o l'integrazione dei dati personali incompleti;
- **cancellazione** (**c.d. diritto all'oblio**), consistente nella facoltà di ottenere da ASP Agrigento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo nel rispetto delle condizioni della normativa;
- **limitazione di trattamento**, consistente nella possibilità di ottenere da ASP Agrigento la limitazione (temporanea) del trattamento al ricorrere di una delle seguenti ipotesi:
  - l'interessato contesta l'esattezza dei dati personali;
  - il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali chiedendone che ne sia limitato l'utilizzo;
  - nonostante la finalità di trattamento si sia esaurita, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
  - a seguito dell'esercizio del diritto di opposizione da parte dell'interessato, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi di ASP Agrigento rispetto a quelli dell'interessato;
- ottenere la **comunicazione** da parte di ASP Agrigento a ciascuno dei destinatari cui sono trasmessi i dati personali dell'interessato, di eventuali rettifiche, cancellazioni o limitazioni del trattamento, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato;
- **portabilità dei dati**, consistente nella facoltà – nei soli casi in cui il trattamento si basa sul consenso o su un contratto ed è effettuato con mezzi automatizzati – di ricevere da ASP Agrigento, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano forniti dall'Interessato stesso, nonché la possibilità di trasmetterli ad un altro titolare senza impedimenti. Inoltre, qualora tecnicamente possibile, il diritto alla portabilità dei dati consente di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro;
- **opposizione**, consistente nel diritto di opporsi, alle condizioni e nel rispetto dei limiti previsti dalla normativa, al trattamento dei dati personali che lo riguardano qualora: (i) necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri; (ii) fondato sull'interesse legittimo del titolare; (iii) finalizzato ad attività di marketing diretto; (iv) finalizzato alla ricerca scientifica o storica o con fini statistici;
- non essere sottoposto a una decisione basata unicamente sul **trattamento automatizzato**, compresa la profilazione, che produca effetti giuridici che lo riguardano o

che incida in modo analogo significativamente sulla sua persona, salvo quanto previsto dalla normativa.

Il DPO analizza le singole richieste pervenute dagli interessati in merito all'esercizio dei propri diritti, coinvolge e verifica, di concerto con i Delegati interni del trattamento competenti, la sussistenza delle condizioni che rendono legittima la richiesta inoltrata e formalizza quindi una risposta dettagliata secondo le seguenti modalità:

- in una **forma concisa**, **trasparente**, **intelligibile** e con un **linguaggio semplice e chiaro**;
- **per iscritto** o con mezzi elettronici, se la richiesta è stata effettuata con mezzi elettronici. Una risposta orale è consentita solo su domanda espressa dall'interessato;
- **senza ingiustificato ritardo** e, al più tardi, **entro un mese** dal ricevimento della richiesta, salva la possibilità di prorogare tale termine di due mesi nei particolari casi previsti e fermo restando l'obbligo di informare comunque l'interessato del ritardo e dei motivi entro un mese dal ricevimento della richiesta. In ogni caso, se non è possibile soddisfare la richiesta entro un mese dal suo ricevimento, è necessario informare l'interessato (i) che non sarà possibile soddisfare la sua richiesta entro tale termine, (ii) sui motivi della proroga e (iii) sulla possibilità di proporre reclamo ad un'autorità di controllo e ricorso giurisdizionale;
- **gratuitamente**. Può essere addebitato un contributo ragionevole o negata la soddisfazione della richiesta, solo nel caso di richieste manifestamente infondate o eccessive, anche per la loro ripetitività;
- **dopo aver verificato l'identità dell'interessato**, eventualmente anche domandando informazioni aggiuntive.

Spetta al DPO eseguire opportunamente le attività di monitoraggio e controllo per verificare che i Delegati interni dei trattamenti competenti e gli incaricati abbiano effettivamente e adeguatamente dato seguito alle richieste degli interessati e, qualora richiesto, fornire la propria consulenza a tali soggetti.
Sulla base dei suddetti principi, ASP Agrigento ha definito un processo di gestione dei diritti degli interessati, descritto all'interno del documento "Processo per la gestione dei diritti degli interessati".



8. MANTENIMENTO DEL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

L'art. 30 del Regolamento impone a Titolari e Responsabili del trattamento, con limitate eccezioni, di tenere un Registro delle attività di trattamento svolte sotto la propria responsabilità (il "Registro").

Per tali motivi, ASP Agrigento è obbligata a dotarsi del suddetto Registro contenente, almeno, le seguenti informazioni:

a) il nome e i dati di contatto del Titolare e di eventuali Contitolari;
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali (comuni, sensibili, giudiziari);
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui all'art. 49 del GDPR, la documentazione delle garanzie adeguate;
f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'art. 32 del GDPR;
h) le condizioni di liceità del trattamento (vedi par. 6.2 "*Condizioni di liceità*").

Il Registro deve essere sempre mantenuto aggiornato rispetto alle attività di trattamento concretamente poste in essere dalle varie Direzioni aziendali.
Inoltre, il processo di verifica ed aggiornamento del Registro deve coinvolgere tutti i soggetti che trattano dati personali per conto di ASP Agrigento. In particolare, è responsabilità di ciascun Delegato interno, Incaricato e Responsabile esterno dare pronta comunicazione al DPO di qualunque iniziativa che abbia un impatto sul trattamento di dati personali effettuato.
La tenuta del Registro è demandata al DPO. Il DPO ha, infatti, la responsabilità di monitorare l'effettivo aggiornamento del Registro dei trattamenti da parte dei Delegati interni del trattamento / incaricati competenti.

9. VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

Il Regolamento europeo 2016/679 ha introdotto l'obbligo per il Titolare del trattamento di eseguire, al ricorrere di talune condizioni, una valutazione d'impatto sulla protezione dei dati (Data Protection Impact Assessment, di seguito "DPIA" o semplicemente "Valutazione").

Infatti, secondo quanto disposto dall'art. 35, paragrafo 1 del GDPR, è previsto in capo al Titolare del trattamento l'onere di procedere ad una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati "*quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.*"

L'effettiva valutazione ed esecuzione della DPIA è in carico ai singoli Delegati interni del trattamento di ASP Agrigento, eventualmente coadiuvati da soggetti interni alla propria struttura organizzativa, cui è stata debitamente conferita nomina ad incaricati.

I Delegati interni del trattamento, formalmente identificati all'interno del modello organizzativo di ASP Agrigento in materia di protezione dei dati personali e i loro collaboratori, ricevono costante e periodica formazione in materia di Privacy e Data Protection, con un focus particolare sullo svolgimento della valutazione d'impatto sulla protezione dei dati (DPIA). Il DPO ha il compito di organizzare tali sessioni di formazione per conto del Titolare, nonché monitorarne l'effettivo svolgimento.

Il Delegato interno del trattamento competente è innanzitutto tenuto a valutare l'obbligatorietà di sottoporre un particolare trattamento a DPIA, al verificarsi di specifiche condizioni.
In generale, la DPIA è obbligatoriamente richiesta per i trattamenti che consistono in:

- valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e a reati;
- sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Accertata la necessità di svolgere una valutazione d'impatto sulla protezione dei dati, il Delegato interno del trattamento coinvolge opportunamente gli altri soggetti interni ed esterni che sono o saranno (in caso di nuovi trattamenti) coinvolti nel trattamento oggetto di DPIA.
L'attività di valutazione d'impatto consta dei seguenti step operativi, opportunamente condotti dal Delegato interno del trattamento, di concerto con il DPO e, laddove necessario, coinvolgendo il Responsabile dei Sistemi Informativi di ASP Agrigento:

- identificare e analizzare i principali rischi per i diritti e le libertà degli interessati in termini di minacce e impatto;
- valutazione dei livelli di rischio *pre* e *post* identificazione delle contromisure di sicurezza (tecniche e organizzative) atte a mitigare tali rischi.

Nel caso di rischio elevato per i diritti e le libertà degli interessati, nonostante le contromisure di sicurezza identificate, il DPO procede con la consultazione preventiva dell'Autorità di Controllo e monitora l'effettiva implementazione delle relative indicazioni ricevute.

Infine, ogniqualvolta vi sia una variazione significativa della natura, delle finalità o delle modalità di trattamento, incluso l'utilizzo di nuove tecnologie, il Delegato interno del trattamento ha la responsabilità di aggiornare la valutazione d'impatto sulla protezione dei dati, al fine di monitorarne e stimarne le variazioni in termini di impatto per i diritti e le libertà degli interessati.

ASP Agrigento, in conformità alle prescrizioni normative, si è dotata di un processo di valutazione d'impatto sulla protezione dei dati e di una metodologia per l'esecuzione della

stessa. Per la trattazione di dettaglio si fa riferimento al documento "Processo per la realizzazione della valutazione d'impatto sulla protezione dei dati (DPIA)".

10. GESTIONE E NOTIFICA DEI DATA BREACH

Il Regolamento Europeo 2016/679 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.

Va inoltre rilevato che, a seconda delle circostanze, una violazione può riguardare la riservatezza, la disponibilità e l'integrità dei dati personali trattati e conservati sia su supporti elettronici sia su supporti fisici (*e.g.* archiviazione cartacea).

I soggetti interni (*e.g.* incaricati o Amministratori di Sistema) autorizzati al trattamento di dati personali, le risorse dei Sistemi Informativi, nonché i fornitori esterni debitamente designati Responsabili possono, nello svolgimento delle attività ad essi demandate, rilevare anomalie o eventi che potrebbero configurarsi come violazioni di dati personali (Data Breach).
In tale evenienza, essi sono tenuti a informare tempestivamente i Delegati interni del trattamento competenti.
Nel caso in cui la violazione di dati personali sia avvenuta mediante un vettore informatico o sia rilevato direttamente da parte dei sistemi di controllo accessi o dalle soluzioni tecnologiche a disposizione dei Sistemi Informativi, è prontamente informato anche il Responsabile dei Sistemi Informativi di ASP Agrigento.

A valle della rilevazione / segnalazione di un potenziale *breach*, i Delegati interni del trattamento interessati, di concerto con il DPO e, in caso di incidente di sicurezza informatico, con il Responsabile IT, procedono con l'analisi della violazione occorsa, al fine di verificarne le categorie di interessati, le categorie di dati personali compromessi, nonché le altre informazioni necessarie per identificare le contromisure opportune per mitigarne i rischi nonché per eseguire la notifica all'Autorità di Controllo e, laddove necessario, agli interessati.

A titolo esemplificativo e non esaustivo, tali informazioni riguardano:

- **Identificabilità degli interessati**, ovvero la possibilità che gli interessati possano essere identificati sulla base dei dati oggetto di compromissione;
- **Misure di sicurezza** poste in essere, che potrebbero aver mitigato gli impatti derivanti dal *breach* occorso;
- **Numero di individui coinvolti**, ovvero la portata in termini numerici degli interessati coinvolti.

Terminata l'analisi del *data breach* occorso, i Delegati interni del trattamento, sentito il parere del DPO e, se necessario, con il supporto del Responsabile IT, procedono a:

- Identificare e implementare le azioni di contenimento e risoluzione al fine di mitigare gli impatti della violazione occorsa;
- Valutare l'obbligatorietà di notificare la violazione all'Autorità di Controllo;
- Valutare l'obbligo di comunicazione agli interessati, nel caso in cui la violazione occorsa presenti rischi elevati per i diritti e le libertà degli interessati medesimi.

Laddove necessario, il DPO predispone e inoltra la notifica all'Autorità di Controllo e ai soggetti interessati con tutte le informazioni previste dalla normativa vigente.

Infine, i Delegati interni dei singoli trattamenti, con la supervisione del DPO, nonché il supporto dei Sistemi Informativi in caso di incidenti di sicurezza informatica, sono tenuti a predisporre e

manutenere un registro interno in cui è documentata qualsiasi violazione dei dati personali, comprese le circostanze, le conseguenze e le misure adottate per porvi rimedio.
Il DPO ha il compito di tenere il suddetto registro e metterlo a disposizione dei singoli Delegati interni del trattamento, per consentire loro di procedere con il costante aggiornamento.

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

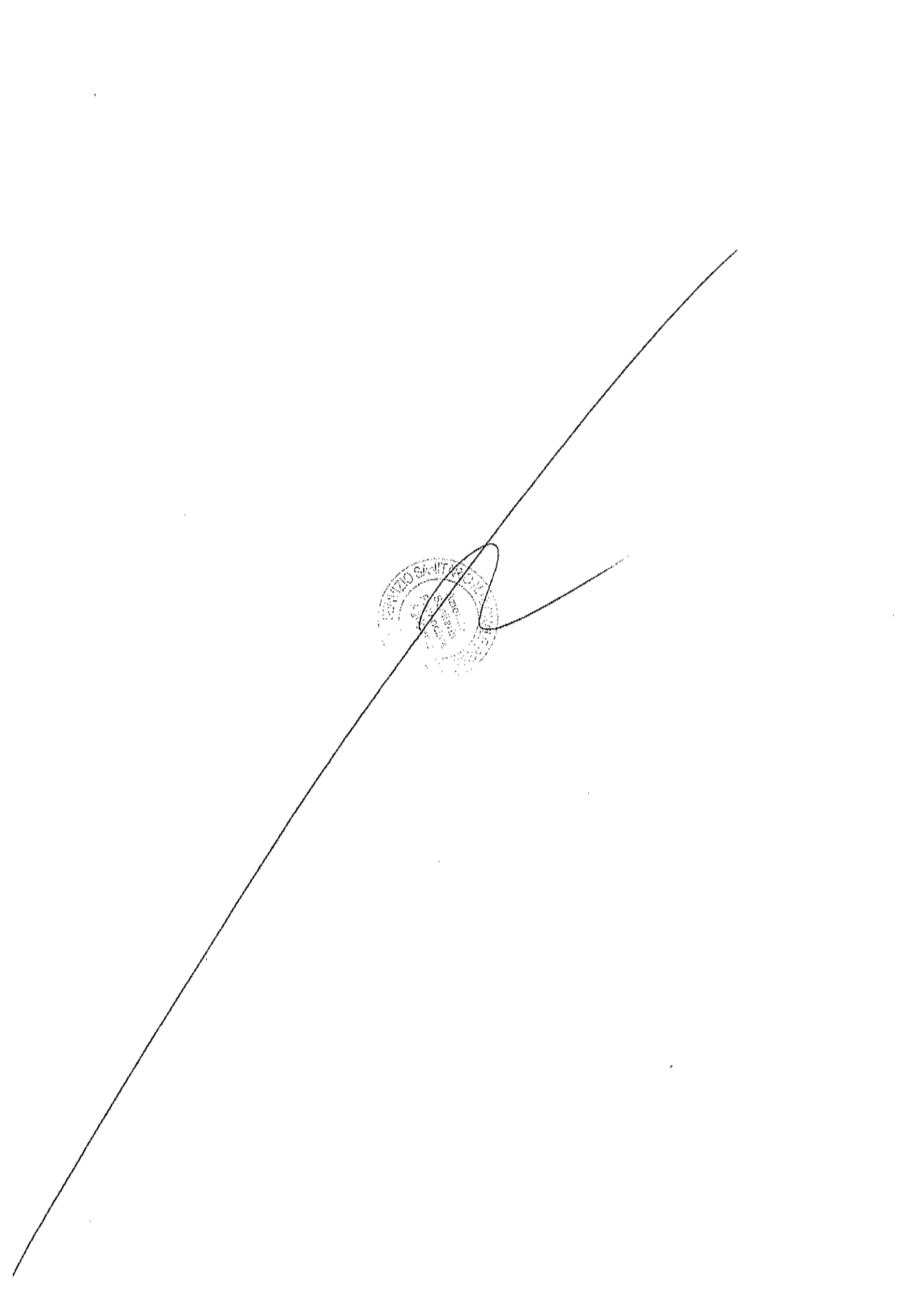
- Rilevazione e segnalazione del *data breach*
- Analisi del *data breach*
- Risposta e notifica del *data breach*
- Registrazione del *data breach*

Per la trattazione di dettaglio del suddetto processo, si fa rimando al documento "*Processo di gestione e notifica dei data breach*".

11. FORMAZIONE

La formazione in materia di privacy è considerata un'importante misura di sicurezza organizzativa per la protezione dei dati personali, che deve essere obbligatoriamente adottata da ASP Agrigento.

A tal fine, il Titolare, con il supporto e la consulenza del DPO, è tenuto a organizzare interventi di formazione e aggiornamento in materia di tutela della riservatezza e protezione dei dati personali rivolti ai suoi stessi Delegati, alle Persone Autorizzate al trattamento e a particolari categorie di soggetti esterni, autorizzati ai trattamenti di dati personali per conto di ASP Agrigento (e.g. Responsabili esterni del trattamento). La formazione è finalizzata alla conoscenza delle norme, all'adozione di idonei modelli di comportamento e procedure di trattamento, alla conoscenza delle misure di sicurezza adottate da ASP Agrigento per il trattamento e la conservazione dei dati, dei rischi individuati e delle modalità per prevenirne i danni.



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