Servizio Sanitario Nazionale – Regione Sicilia
AZIENDA SANITARIA PROVINCIALE AGRIGENTO
Viale Della Vittoria n. 321, Agrigento 92100
Web: www.aspag.it

GDPR – GENERAL DATA PROTECTION REGULATION

IL REGOLAMENTO N.679 2016 UE SULLA PROTEZIONE DEI DATI PERSONALI

RESPONSABILITA' E ADEMPIMENTI PER GLI AUTORIZZATI AL TRATTAMENTO

Direzione Generale- Ufficio Privacy
Dott.ssa Maria Giovanna Matteliano

INDICE ARGOMENTI

1. Basi Normative (GDPR, Codice, diritti interessati)
2. Informative e consenso
3. Sistema gestione: soggetti privacy
4. Le Istruzioni per gli Autorizzati al Trattamento
5. La gestione del rilascio dei Referti
6. Le misure di sicurezza
7. Data Breach
8. Cenni su Apparato sanzionatorio

1. Basi normative

- **Regolamento UE 679/2016** pubblicato sulla Gazzetta Ufficiale dell'UE il **4 maggio 2016**, entrato in vigore in vigore il **24 maggio del 2016**, definitivamente applicabile dal **25 maggio 2018**
- **D. Lvo 196/2003** *adeguato con* ***decreto 101 del 10/08/18***
- **Provvedimenti del Garante** per la protezione dei dati personali

Basi normative: definizioni

- **«Trattamento»**: 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.

Trattamento è **qualsiasi tipo di operazione** effettuata sui dati, anche un semplice accesso o l'osservazione di un'immagine.

ESEMPIO → raccolta, registrazione, organizzazione, strutturazione, conservazione, consultazione, etc.

Basi normative: definizioni

- **«Dato personale»**: **qualsiasi** informazione riguardante una persona fisica (di seguito definita **"INTERESSATO"**) **identificata o identificabile.**

Si **considera identificabile** → la persona fisica che può essere identificata, direttamente o indirettamente

ESEMPIO → nome, dati relativi all'ubicazione, un identificativo online, uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale, etc.

Basi normative: definizioni

- **«Dati particolari»: (Art. 9 GDPR)** dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale, o all'orientamento sessuale della persona.

È posto il divieto di trattare questo tipo di dati

Tranne nei casi…

Basi normative: definizioni

DEROGHE DIVIETO (art. 9 – GDPR/ art. 2-septies 193/2003)

il trattamento dei dati particolari è consentito se il trattamento è effettuato:

- previo **CONSENSO ESPLICITO**
- **per assolvere obblighi ed esercitare diritti del titolare** del trattamento o dell'**interessato** in materia di **diritto del lavoro e sicurezza e protezione sociale (es. sorveglianza sanitaria)**
- per tutelare **un interesse vitale dell'interessato (es. prestazione sanitaria di urgenza)**
- nell'ambito di legittime attività **di un ente senza scopo di lucro (es. Sindacati)**
- su **dati manifestamente resi pubblici dall'interessato (es. immagine su social network)**
- se **finalizzato alla difesa in giudizio (es. citazione testimoniale, atti giudiziari)**
- **motivi di interesse pubblico** in proporzione alla finalità perseguita **(es. dati trattati dalle PA)**
- se necessario **per finalità di medicina preventiva o medicina del lavoro (es. valutazione capacità lavorativa)**
- se necessario per motivi di **interesse pubblico nel settore della sanità pubblica (quali protezione da gravi minacce per la salute pubblica)**

Basi normative: I PRINCIPI – ART 5 GDPR

ART 5. GDPR: I 6 principi della protezione dei dati

- **1. Liceità, correttezza e trasparenza**
- La AsL deve assicurarsi che le loro attività di raccolta dei dati personali degli utenti non infrangano la legge e che non nascondano nulla agli interessati.
- Per fare ciò, è necessario mettere a disposizione del pubblico l'informativa sulla privacy, ossia un documento che spiega in maniera chiara, concisa ma completa le finalità della raccolta dei dati e come l'azienda intenda usarli.
- **2. Limitazione della finalità**
- La ASL deve raccogliere i dati personali solamente per uno scopo preciso, scopo che va indicato in modo chiaro nell'informativa sulla privacy. Inoltre, tali dati vanno tenuti solo per il tempo necessario a completare lo scopo per cui sono stati raccolti.
- **3. Minimizzazione dei dati**
- Le organizzazioni possono elaborare solo i dati personali necessari al raggiungimento della finalità per i quali sono trattati. Per esempio, per compilare la cartella clinica del pz. Non è necessario trattare dati riguardanti il suo orientamento politico.
- **4. Esattezza**
- L'accuratezza dei dati personali è parte integrante della loro protezione. Il GDPR afferma che "devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti". Gli interessati hanno il diritto di chiedere che i propri dati personali inesatti o incompleti vengano cancellati o rettificati .
- **5. Limitazione della conservazione**
- La ASL deve eliminare i dati personali quando non sono più necessari ai propri scopi. (es una cartella clinica va conservata per sempre; una lastra RX per dieci anni)
- **6. Integrità e riservatezza**
- Il GDPR afferma che i dati personali devono essere "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".

2. Informativa e Consenso: chiarimenti del Garante

Trattamento di particolari categorie di dati per finalità di cura - Chiarimenti del Garante sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario - 7 marzo 2019:

- TRATTAMENTO DATI NECESSARI PER FINALITA' DI CURA: NON E' RICHIESTO IL CONSENSO MA E' OBBLIGATORIA L' INFORMATIVA
- TRATTAMENTO DATI PER FINALITA' NON STRETTAMENTE NECESSARIE ALLA CURA (chiamata telefonica, trasmissione referto, ecc.): E' RICHIESTO IL CONSENSO PRECEDUTO DALL' INFORMATIVA

Informativa e Consenso (artt. 13-14 GDPR)

Informativa

•**Art. 13** Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato (es. compilare un form online, raccolta dati allo sportello etc).

•**Art. 14** Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato (es. quando un soggetto diverso riceve i dati personali per finalità diverse)

Sul sito aziendale è stata pubblicata la Procedura relativa alla "Informativa Unica" al trattamento dei dati personali ai sensi dell'art. 13 del REG.UE 679/2016 (GDPR)

Consenso dell'interessato

- qualsiasi **manifestazione di volontà** libera, specifica, informata e inequivocabile dell'interessato con cui lo stesso manifesta il proprio assenso;
- **dichiarazione o azione positiva inequivocabile** che i dati personali che lo riguardano siano oggetto di trattamento;

Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.

Informativa e Consenso: Informativa ASP AG

L'informativa deve contenere le seguenti informazioni:

- ✓ Chi è il **titolare** del trattamento
- ✓ Chi è il responsabile della protezione dei dati (**DPO**)
- ✓ Quali sono le **finalità** del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- ✓ Le basi **giuridiche**
- ✓ gli eventuali **destinatari** o le eventuali categorie di destinatari dei dati personali;
- ✓ Eventuale **trasferimento** dei dati personali a un paese terzo
- ✓ Il periodo di **conservazione** dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- ✓ L'esercizio dei **diritti** dell'interessato
- ✓ Il diritto di **revocare** il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento
- ✓ Il diritto di proporre **reclamo** a un'autorità di controllo;
- ✓ **Natura** del conferimento, ovvero se la comunicazione di dati personali è un obbligo legale o contrattuale
- ✓ l'esistenza di un processo decisionale automatizzato, compresa la **profilazione** di cui all'articolo 22, paragrafi 1 e 4.

Informativa e Consenso: procedura aziendale per il rilascio dell' Informativa

Si premette che a fronte di un primo Modello di "Informativa unica" la Asp di Agrigento, per il tramite dell'Ufficio protezione dei dati , predisporrà una serie di Modelli di Informativa specifica per le singole UOC/UOSD.

Ciascun Direttore di Dipartimento, di UOC o di UOSD dovrà farsi garante del rispetto delle seguenti regole in merito alla Informativa (unica e specifica) attualmente in uso:

a) L**a Informativa va affissa nei locali di transito e nelle sale di attesa degli Uffici di prenotazione, di Accettazione, del Dipartimento e della UOC/UOSD di competenza**.

b) **L' Informativa va pubblicata sul sito web aziendale della Asp, a cura della competente funzione aziendale.**

c) **Copia di tale modello di Informativa unica deve essere resa disponibile agli assistiti che ne facciano richiesta**.

d) **L' Informativa unica va prima illustrata, nei suoi contenuti, e poi – se richiesto dall'interessato – consegnatagli**.

e) **Colui che rilascia la Informativa unica deve adottare una metodica che consenta la sua annotazione in modo da permetterne la verifica ad altre UOC che, anche in tempi diversi, trattano dati relativi al medesimo interessato** (D.Lgs. n. 196/2003 integrato con le modifiche introdotte dal D.Lgs. n. 101/2018, art. 79, paragrafo 2).

3. Sistema gestione: soggetti privacy

- TITOLARE DEL TRATTAMENTO

ASP DI AGRIGENTO

- RESPONSABILI DEL TRATTAMENTO

Organizzazioni esterne autorizzate al trattamento dati

- RESPONSABILE DELLA PROTEZIONE DATI (DPO)

Dott. MARCO LO BRUTTO

- DELEGATI AL TRATTAMENTO

Direttori e Dirigenti UOC/UOSD

- AUTORIZZATI AL TRATTAMENTO

Personale autorizzato dai Direttori e Dirigenti UOC/UOSD

- DESTINATARI DEL TRATTAMENTO

Personale Interno, Regione, Altre ASP,ECC..

Sistema di gestione: IL TITOLARE DEL TRATTAMENTO

il titolare del trattamento determina le finalità e i mezzi del trattamento di dati personali.

Articolo 24 **Responsabilità del titolare del trattamento**

Tenuto conto della:

- **natura**,
- **ambito di applicazione**,
- **contesto,**
- **finalità del trattamento**,
- **rischi** aventi probabilità e gravità diverse **per i diritti e le libertà delle persone fisiche**.

il titolare del trattamento mette in atto

misure tecniche e organizzative adeguate

Sistema di gestione: IL RESPONSABILE DEL TRATTAMENTO (Art. 28)

il Responsabile del trattamento determina le finalità e i mezzi del trattamento di dati personali.

Il titolare del trattamento ricorre UNICAMENTE

a Responsabili del trattamento che presentino **garanzie sufficienti** per mettere in atto misure tecniche e organizzative adeguate

Redazione **contratto o altro atto giuridico** da cui emergano i suoi obblighi.

Sistema di gestione: Responsabile della Protezione dei dati (DPO)

RPD (Responsabile della Protezione dei dati) o DPO (Data Protection Officer)

Nuova figura professionale, obbligatoria presso:

- Aziende Pubbliche

(caso della ASP DI AGRIGENTO)

- Aziende che effettuano un **monitoraggio regolare e sistematico degli interessati su larga scala**

- Aziende che trattano i **dati particolari ex art.9 GDPR**

(caso della ASP DI AGRIGENTO)

Sistema di gestione: funzioni e poteri del DPO

Il DPO deve:

- fornire **istruzioni al titolare**, al responsabile del trattamento e ai dipendenti
- **verificare** l'attuazione e l'applicazione della normativa
- **fornire pareri** in merito alla valutazione d'impatto sulla protezione dei dati e vigilare sui relativi adempimenti
- fungere da **punto di contatto con gli interessati e con il Garante**
- rispettare l'obbligo di **riservatezza** in merito all'adempimento dei propri compiti

Sistema di gestione: DESTINATARIO DEL TRATTAMENTO

Destinatario

Soggetto che riceve comunicazione di dati personali,
che si tratti o meno di terzi.

Sistema di gestione: deleghe interne

Funzioni aziendali

ASP DI AGRIGENTO
Direttore Generale

Direttori UOC

Dirigenti UOSD

Personale UOC

Personale UOSD

Ruoli Privacy

Titolare del Trattamento

Org. Esterna

Resp. del Trattamento

Delegati al trattamento dei dati

Soggetti Autorizzati del Trattamento

Sistema di gestione: Soggetti Delegati al Trattamento

ASP DI AGRIGENTO – Titolare del trattamento

Designa per iscritto
i soggetti Delegati al trattamento dei dati personali

Sistema di gestione: Delegati interni

È fatto obbligo al Delegato di:

- a) **nominare i Soggetti Autorizzati al Trattamento dei dati** (ex Incaricati al Trattamento dei Dati) ai sensi dell'art. 29 del Reg. UE 679/2016 e dell'art. 2-quaterdecies del Codice, conferendo loro apposite istruzioni sulle norme e le procedure da osservare e provvedendo alla relativa formazione;
- b) **redigere ed aggiornare una lista nominativa dei Soggetti Autorizzati al Trattamento** e verificare annualmente l'ambito del trattamento consentito ai medesimi e ogni volta che si verifichi un caso di modifica dell'assegnazione degli incarichi (es.: quiescenza, trasferimento, nuovo autorizzato);
- c) **controllare le operazioni di trattamento** svolte dagli autorizzati e la conformità all'ambito di trattamento consentito;
- d) **attuare gli obblighi di informazione** (Informativa ex Artt. 13-14 del Regolamento) ed acquisizione del consenso, quando richiesto, nei confronti degli interessati;

Sistema di gestione: Delegati interni

- e) **comunicare immediatamente al titolare** non oltre le 12 ore successive al loro ricevimento, ogni richiesta, ordine o attività di controllo da parte del Garante o dell'Autorità Giudiziaria
- f) ove competente (ved. Art. 6) **nominare i Responsabili del Trattamento** dei dati ai sensi dell'art. 28 del Reg. UE 679/2016, conferendo loro apposite istruzioni sulle norme e le procedure da osservare e provvedendo alla relativa formazione;
- g) **organizzare, gestire e supervisionare tutte le operazioni di trattamento** dei dati personali affinché esse vengano effettuate nel rispetto delle disposizioni normative in materia di protezione di dati personali e predisporre tutti i documenti richiesti dai relativi adempimenti;
- h) sovrintendere alla formazione dei propri collaboratori

Sistema di gestione: Soggetti Autorizzati del trattamento

Direttori e Dirigenti delle UOC e UOSD

Designano per iscritto
all'interno della U.O. e/o Ufficio di appartenenza
le persone autorizzate al trattamento dei dati personali

Sistema di gestione: SAT

Soggetto Autorizzato al Trattamento

è il soggetto persona fisica che effettua materialmente le operazioni di trattamento sui dati personali.

Con la lettera di nomina vengono fornite **agli autorizzati le istruzioni operative** (art. 29 GDPR), compresi gli obblighi inerenti le misure di sicurezza, e la **necessaria formazione**.

4. Istruzioni per i Soggetti Autorizzati al Trattamento

Il Soggetto Autorizzato effettua il trattamento dei dati personali esclusivamente sulla base delle istruzioni ricevute dal Titolare e dal Delegato interno in forma documentata.

OBBLIGHI DEL SAT:

- **trattare i dati personali** appartenenti a particolari categorie di dati art. 9 GDPR (es.: dati sanitari), osservando le maggiori cautele di trattamento che questo tipo di dati richiedono (ad esempio, ove possibile, conservarli separatamente);
- conservare adeguatamente i dati appartenenti a **particolari categorie di dati consultare esclusivamente i documenti contenenti dati personali necessari** per lo svolgimento dell'attività lavorativa prestando particolare attenzione alla custodia ed archiviazione degli stessi;

Istruzioni per i SAT

- **custodire e non divulgare le credenziali di autenticazione** (UserID e password) ricevute e necessarie per accedere ai sistemi informatici e tecnologici ed ai dati in essi contenuti necessari per lo svolgimento delle attività di trattamento previste dalla Sua mansione lavorativa;
- **custodire e tutelare l'accessibilità agli strumenti elettronici** soprattutto mentre è in corso una sessione di lavoro; utilizzare gli strumenti ed i programmi in conformità ai regolamenti aziendali al fine di proteggere i sistemi informativi e i dati ivi contenuti;
- effettuare le operazioni di trattamento solo dei dati personali necessari per lo svolgimento dell'attività lavorativa, nel **rispetto dei principi** di cui all'art. 5 del GDPR e delle **misure di sicurezza** predisposte dal Titolare del trattamento ex art. 32 del GDPR, a tutela della riservatezza degli interessati;

PRINCIPI ART. 5 GDPR

liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza, responsabilizzazione

Istruzioni per i SAT

- **non lasciare incustodito il proprio posto di lavoro** prima di aver provveduto alla messa in sicurezza dei dati. In caso di allontanamento, anche temporaneo, dal luogo ove si svolge il trattamento dei dati personali, è necessario verificare che non vi sia possibilità da parte di terzi non autorizzati e/o non legittimati di accedere ai dati personali per i quali era in corso il trattamento;
- **comunicare solo i dati personali preventivamente autorizzati** dal Titolare e/o dal Delegato interno;
- **informare** prontamente il Titolare e/o il Delegato Interno di ogni **questione** rilevante ai fini del rispetto della normativa in materia di protezione dei dati personali;
- **informare**, tempestivamente e senza ingiustificato ritardo (comunque entro e non oltre 24 ore dalla ricezione), il Titolare e/o il Delegato interno in merito a qualsiasi richiesta di accesso e di esercizio dei diritti **da parte degli interessati;**

Istruzioni per i SAT

INOLTRE:

- qualsiasi **istruzione aggiuntiva** o diversa sarà fornita dal Titolare o dal Delegato interno per iscritto (es. Procedure operative, circolari ecc…) per mezzo dei canali di comunicazione istituzionali (ad es.: posta elettronica ordinaria.
- il Soggetto Autorizzato consente al Titolare del trattamento ed al Delegato interno l'esercizio del potere di controllo e **ISPEZIONE**, prestando ogni ragionevole collaborazione alle attività di audit effettuate dal Titolare stesso, dal Delegato interno o da un altro soggetto da questi incaricato o autorizzato, con lo scopo di controllare l'adempimento degli obblighi e delle istruzioni di cui alla lettera di nomina. Il Delegato interno darà comunicazione al Soggetto Autorizzato della propria intenzione di svolgere un Audit comunicandone l'oggetto, la tempistica, la data, e la durata;

Istruzioni per i SAT

- il Soggetto Autorizzato al Trattamento si impegna a **collaborare** con gli altri Soggetti Autorizzati al Trattamento, al fine di armonizzare e coordinare l'intero processo di trattamento dei Dati Personali;
- gli obblighi relativi alla **riservatezza** ed alla comunicazione dovranno essere osservati anche in seguito a modifica della presente autorizzazione e/o cessazione del rapporto di lavoro;

Resta inteso che qualora il SAT tratti autonomamente i dati personali, in ***violazione*** delle istruzioni impartite dal Titolare e/o dal Delegato interno, *si assumerà i conseguenti oneri, rischi e responsabilità,* in quanto sarà considerato, a sua volta, Titolare del trattamento.

5. La Gestione dei Rilascio dei Referti

*Dal punto di vista del trattamento dei dati personali, il **processo di gestione dei referti** è una attività **CRITICA**, pertanto è stata redatta una specifica procedura che aiuta il personale coinvolto nella gestione, a svolgere il proprio lavoro, limitando al minimo qualsiasi rischio collegato a perdita, distrazione, scambio, ecc.*

DEFINIZIONE DI REFERTO:

- "**referto medico**": la relazione scritta rilasciata dal medico sullo stato clinico del paziente dopo un esame clinico o strumentale;
- "**referto di laboratorio, radiologico, elettrocardiografico, elettroencefalografico,** ecc.: ogni relazione scritta rilasciata dal medico che ha sottoposto un paziente a un esame strumentale, in cui egli interpreta il risultato dell'esame.

La Gestione dei Rilascio dei Referti

CRITERI da valutare nella redazione dei un REFERTO:

- **Rintracciabilità:**

per rintracciabilità si intende la possibilità di poter risalire a tutte le attività e agli esecutori che sono intervenuti nelle varie fasi propedeutiche alla compilazione del referto con i relativi, ed eventuali, allegati. Nella compilazione del referto devono essere identificabili gli autori con firma leggibile (nome e cognome riconoscibili).

- **Chiarezza:**

la chiarezza riguarda la grafia e l'esposizione. Il testo deve essere chiaramente leggibile e l'esposizione deve essere diretta e non dare adito a diverse interpretazioni.

- **Accuratezza:**

ogni Unità Operativa dovrà garantire l'accuratezza dei dati prodotti e delle loro eventuali trascrizioni con corrispondenza tra esami strumentali prescritti, esami eseguiti e refertati e corrispondenza tra il referto e la documentazione allegata.

- **Veridicità:**

tutti gli esami clinici e strumentali sui quali si basa la redazione del referto debbono essere veritieri e corrispondenti ai dati oggettivi relativi al paziente.

- **Minimizzazione:**

i dati riportati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

La Gestione dei Rilascio dei Referti

Modalità di rilascio del referto medico:

- Il referto medico può essere rilasciato all'interessato, munito di documento di riconoscimento valido o al delegato munito di documento di riconoscimento proprio, di delega firmata e di documento di riconoscimento del delegante.
- In casi specifici (ad es: HIV+, IVG, ecc.) per i quali la tutela del segreto professionale ed i motivi di riservatezza della diagnosi richiedano una tutela particolare, *non trova applicazione l'istituto della delega* ed il rilascio di copia del referto medico avviene esclusivamente nelle mani dell'interessato.

La Gestione dei Rilascio dei Referti

- **consegna a mano**, il rilascio del referto viene eseguito in busta chiusa nei confronti del soggetto interessato o delegato al ritiro. Il soggetto deputato all'imbustamento dovrà accertarsi che la documentazione (referto + eventuali esami) appartenga a colui che la richiede.

- **spedizione a mezzo posta tradizionale,** il soggetto deputato all'imbustamento dovrà accertarsi che ci sia esatta corrispondenza tra l'indirizzo comunicato dal richiedente e quello riportato sulla busta. Al fine di garantire una maggiore sicurezza circa la integrità della documentazione e la corrispondenza tra il referto e la documentazione ad esso allegata, il soggetto deputato all'imbustamento dovrà accertarsi che la documentazione (referto + esami) appartenga a colui che la richiede.

- **spedizione a mezzo posta elettronica,** il referto dovrà essere spedito in allegato a un messaggio e-mail e non come test compreso nel corpo del messaggio

(vedasi nota prot. n. 41950 del 11.03.2024 pubblicata sul sito istituzionale)

6. Le Misure di sicurezza (Art. 32 GDPR)

il **titolare** del trattamento e il **responsabile** del trattamento mettono in atto **misure tecniche e organizzative idonee a garantire un livello di sicurezza ADEGUATO al rischio**

PER ESEMPIO:

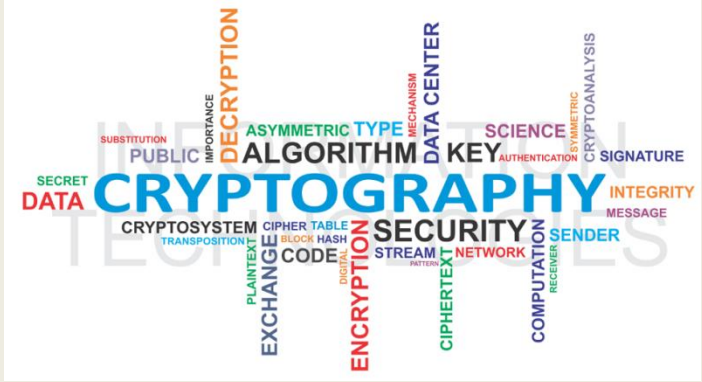
Pseudonimizzazione (o meglio Pseudo Anonimizzazione):

tecnica che consiste nel conservare i dati in una forma che **impedisce** l'identificazione del soggetto **senza** l'utilizzo di informazioni aggiuntive.

A condizione che tali informazioni aggiuntive siano conservate separatamente e con misure adeguate.

Cifratura dei dati personali

la capacità di **assicurare su base permanente** la **RISERVATEZZA**, l'**INTEGRITÀ**, la **DISPONIBILITÀ** e la **RESILIENZA** dei **sistemi e dei servizi di trattamento**.



Le Misure di sicurezza (Art. 32 GDPR) : la responsabilità e pericoli

Il lavoratore è una risorsa fondamentale per l'azienda, nonché il vero custode dell'infrastruttura informatica aziendale, pertanto:

- **comportamento senza distrazioni**
- **prontezza nell'identificare e segnalare** un' ipotetica **minaccia**

costituiscono **elementi** che **determinano** direttamente il **livello** di **sicurezza** delle informazioni all'interno della Azienda.

La sicurezza informatica potrebbe essere messa in PERICOLO poiché il lavoratore Soggetto Autorizzato al Trattamento:

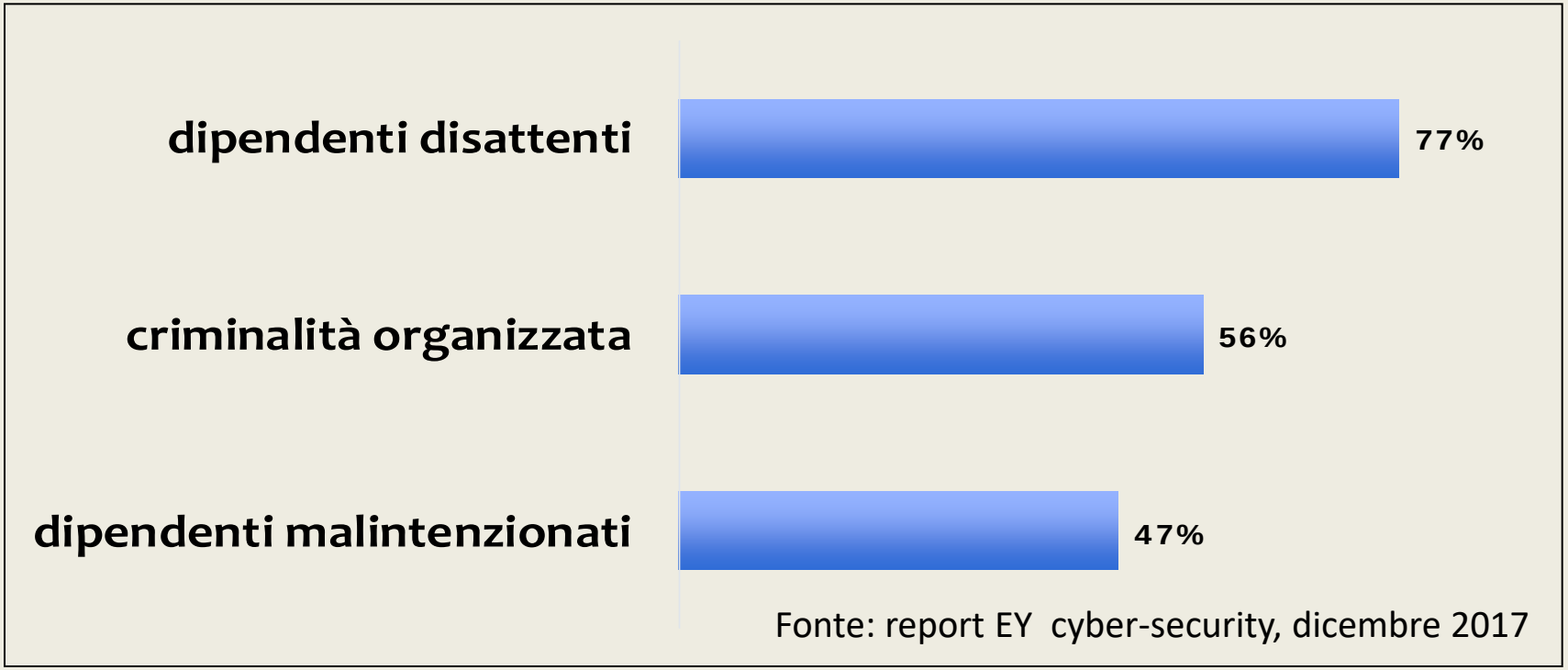
- detiene le credenziali di accesso all'infrastruttura informatica, quindi soggette a perdita, smarrimento, furto…
- potrebbe essere indotto erroneamente ad aprire un file
- detiene informazioni utili ed interessanti per comprendere il contesto della realtà aziendale

Le Misure di sicurezza (Art. 32 GDPR) Scrivania = Vettore d'attacco

Le Misure di sicurezza (Art. 32 GDPR): Scrivania a norma GDPR

Le Misure di sicurezza (Art. 32 GDPR): quando le minacce sono interne

Le cause principali della vulnerabilità informatica sono riconducili alle seguenti casistiche:



Fonte: report EY cyber-security, dicembre 2017

Le Misure di sicurezza (Art. 32 GDPR): le minacce interne

IL COMPORTAMENTO DELLE PERSONE CHE METTE A RISCHIO L'AZIENDA



INTENZIONALI

- Risentimento verso l'azienda
- Abuso di privilegi ed accessi
- Furto o danno intenzionale

ACCIDENTALI

- Violazione delle policy di sicurezza
- Errori durante il trasferimento dei file
- Mancata formazione / comprensione

COMPROMESSI

- Vittime di:
  - cyber attacchi
  - social engineering
  - Corruzione o blackmail

Le Misure di sicurezza (Art. 32 GDPR): gli Attacchi

L'intera infrastruttura dell'Azienda può essere definita come una **superficie**. Tale superficie può contenere delle aree di **vulnerabilità** che possono mettere in crisi tanto la sicurezza informatica che la sicurezza fisica.

Se tali vulnerabilità venissero sfruttate, si determinerebbe un rischio per l'intero apparato aziendale. Scopo dell'Azienda, quindi, è gestire tali rischi, riducendo le aree di vulnerabilità.

Ciò obbliga l'Azienda a redigere regolamenti sia in termini di sicurezza fisica sia informatica.

Gli attacchi determinano:

- Aumento dei costi:
  - Sanzioni pecuniarie
  - Risarcimento danni
  - Spese ripristino dei sistemi
- Danni d'immagine e reputazionali
- Danni determinati dall'uso improprio dei dati rubati

Le Misure di sicurezza (Art. 32 GDPR): gli Attacchi

Fare attenzione:

- Alle mail ricevute e ai file allegati
- Ai siti visitati! Focus su https. (https → una comunicazione web che sfrutta la crittografia)
- Alle pubblicità nelle pagine web
- Ai programmi che vengono installati
- Alle pendrive (se autorizzate) e cd inseriti

Le Misure di sicurezza (Art. 32 GDPR): ESEMPI di Attacchi

- **Ransomware**

  Ransom = riscatto. Software che blocca la macchina crittografandola e chiedendo un riscatto per “sbloccarla”.

- **Phishing/Spearphishing**

  E’ una mail fraudolenta verso un individuo, organizzazione o business.

- **Spyware**

  Raccolgono informazioni sulle attività degli utenti di un sistema.

- **Keylogger**

  Programma che registra ogni tasto premuto sulla macchina vittima.

- **Worm**

  Si diffondono sulle reti sfruttando delle vulnerabilità dei S.O. o dei programmi.

7. Data Breach

Cos'è un Data Breach?

E' una violazione dei dati personali che comporta accidentalmente o in modo illecito la ***distruzione****, la* ***perdita****, la* ***modifica****, la* ***divulgazione non autorizzata*** *o l'****accesso****.*

La procedura che gestisce il Data Breach, generalmente, inizia con una **segnalazione che il Soggetto Autorizzato al Trattamento** effettua ai Direttori e Dirigenti UOC/UOSD (Delegati interni), che a loro volta dovranno informare il Sistema Informatico ed il Responsabile Protezione Dati (DPO).

Quando bisogna effettuare una segnalazione?

- Perdita o furto di un dispositivo (es. portatile, tablet ecc.)
- Manomissione scrivania
- Si è cliccato per errore ad una mail ritenuta fraudolenta
- Malfunzionamento a livello di hardware/Software/sistema
- Il software antivirus ha segnalato un virus
- Il sistema risulta bloccato

Data Breach

Il Team di Valutazione dei Data Breach, che riceve la segnalazione:

- Valuta la segnalazione
- Verifica se si tratta di un falso positivo
- Può convocare il lavoratore per ulteriori informazioni

Se vengono violati gli *standard* di sicurezza alla base del trattamento

- Il Titolare deve informare le **autorità di controllo** entro e non oltre **72 ore.**
- Il Titolare deve tempestivamente informare i **soggetti interessati** dalla violazione quando sussiste la possibilità di una **grave lesione** dei loro diritti

Data Breach: ruolo del Soggetto Autorizzato al Trattamento

T

Violazioni di Dati Personali (cd. "Data Breach")

- Il Soggetto Autorizzato si impegna ad **informare immediatamente il Delegato interno**, senza ingiustificato ritardo dal momento in cui ne sia venuto a conoscenza, di ogni violazione della sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali trasmessi, conservati o comunque trattati.
- Il Soggetto Autorizzato si impegna inoltre, tenuto conto della natura del trattamento e delle informazioni a propria disposizione, a **prestare ogni necessaria collaborazione al Delegato interno** in relazione all'adempimento degli obblighi gravanti sul Titolare relativi alla notifica delle suddette violazioni al Garante per la Protezione dei Dati Personali ai sensi dell'art. 33 del GDPR o di comunicazione delle stesse agli interessati ai sensi dell'art. 34 del GDPR.

8. Cenni su Apparato Sanzionatorio

Art.82 DIRITTO AL RISARCIMENTO RESPONSABILITA'

Obbligo di risarcimento del danno:

Il Titolare e/o il Responsabile

sono **tenuti** a risarcire il danno cagionato all'interessato da una violazione del Regolamento.

Sono esonerati soltanto

se dimostrano che l'evento dannoso non è in alcun modo imputabile al loro operato.

Cenni su Apparato Sanzionatorio: SANZIONI

Le sanzioni devono essere in ogni singolo caso:

- ❑ **effettive**
- ❑ **proporzionate**
- ❑ **dissuasive**

<u>Parametri di riferimento:</u>

- ➢ Natura, **gravità**, durata della violazione
- ➢ **Dolo** o colpa
- ➢ Misure adottate per **attenuare il danno** subìto dagli interessati
- ➢ Grado di **responsabilità** e **tecniche organizzative** adottate per la protezione e sicurezza dei dati

Cenni su Apparato Sanzionatorio: SANZIONI

Fino a **10 milioni di Euro** o, per le imprese, fino al **2% del fatturato mondiale totale annuo** dell'esercizio precedente

Fino a **20 milioni di Euro** o, per le imprese, fino al **4% del fatturato mondiale totale annuo** dell'esercizio precedente.

Violazione delle previsioni relative a:

- **Trattamento dei dati dei minori**
- ***Privacy by design***
- ***Privacy by default***
- **Obblighi del titolare e del responsabile , anche in merito alla nomina del DPO, tenuta del registro e in materia di misure di sicurezza**

Violazione delle previsioni relative a:

- **i principi di base del trattamento**
- **Consenso dell'interessato**
- **Trasferimento dati personali in paesi extra UE**
- **Diritti degli interessati**
- **Inosservanza provvedimento del Garante (ordine di limitazione o di sospensione)**

SI RICORDA CHE SUL SITO AZIENDALE:

http://www.aspag.it/

SI TROVANO I DOCUMENTI PUBBLICATI ED UFFICIALI RELATIVI ALLA PRIVACY

GRAZIE PER L'ATTENZIONE

Direzione Generale-Ufficio Privacy

Dott. ssa Maria Giovanna Matteliano
ufficio.protezionedeidati@aspag.it