GDPR – GENERAL DATA PROTECTION REGULATION

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

RESPONSABILITA' E ADEMPIMENTI

In collaborazione con Ufficio Privacy e D.P.O. - Dott. Giovanni Modesti

Argomenti

- Basi Normative
- Sistema gestione deleghe interne
- Designazione dei responsabili
- Informative e consenso
- Data breach
- Apparato sanzionatorio

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

Definizione di trattamento

- **«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

Ad Es.→ raccolta, registrazione, organizzazione, strutturazione, conservazione, consultazione, etc.

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

Definizione di dato personale

- **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.

DISCIPLINA DEI DATI PARTICOLARI

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…

DISCIPLINA DEI DATI PARTICOLARI/SALUTE

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)**

ACCOUNTABILITY

Il trattamento dei dati personali deve essere **sempre improntato** al rispetto dei principi di cui all'art.5 GDPR

il titolare del trattamento deve essere SEMPRE in grado di **comprovarlo**

Come? >> Documentando:

le misure tecniche e organizzative adeguate

I SOGGETTI DEL TRATTAMENTO

TITOLARE DEL TRATTAMENTO

ASL n. 2 di Lanciano Vasto Chieti

RESPONSABILI DEL TRATTAMENTO

Organizzazioni esterne incaricati da ASL/SATD

RESPONSABILE DELLA PROTEZIONE DATI (DPO)

Dott. Giovanni Modesti

AUTORIZZATI CON DELEGA AL TRATTAMENTO

Direttori e Dirigenti UOC/UOSD

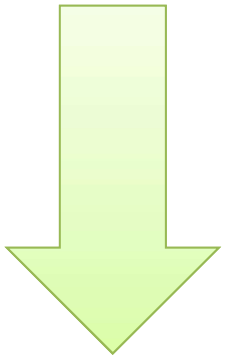
AUTORIZZATI AL TRATTAMENTO

Personale autorizzato dai Direttori e Dirigenti UOC/UOSD

DESTINATARI DEL TRATTAMENTO

Personale Interno, Regione, Altre ASL, MEF

IL TITOLARE DEL TRATTAMENTO:



determina le finalità e i mezzi del trattamento di dati personali

Responsabilità del Titolare del Trattamento

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 (= idonee)**

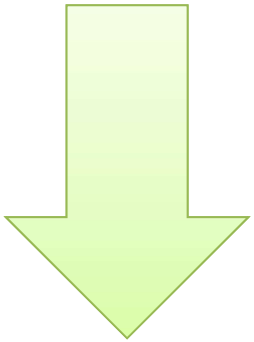
Obbligo del titolare: art. 25 GDPR

Art. 25 GDPR Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita

- privacy by Design: impone di adottare misure tecniche e organizzative per la protezione dei dati **sia** all'atto della progettazione **che** dell'esecuzione del trattamento

- privacy by Default: ricalca il principio di necessità ovvero per impostazione predefinita vengono raccolti solo i dati personali necessari per ogni specifica finalità del trattamento (**Minimizzazione**)

Responsabile del trattamento



tratta dati personali **per conto** del titolare del trattamento

Responsabile del Trattamento

Il titolare del trattamento ricorre UNICAMENTE

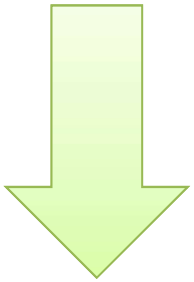
a Responsabili del trattamento che presentino **garanzie sufficienti** per mettere in atto misure tecniche e organizzative adeguate

Redazione **<u>contratto o altro atto giuridico</u>** da cui emergano i suoi obblighi.

Responsabile del Trattamento

ASL e

Direttori e Dirigenti delle UOC e UOSD



Designano per iscritto Organizzazioni esterne che trattano dati personali per conto della ASL

Sistema di gestione delle deleghe interne

Funzioni aziendali

ASL N. 2
Direttore Generale

Direttori UOC

Dirigenti UOSD

Personale UOC

Personale UOSD

Ruoli Privacy

Titolare del Trattamento

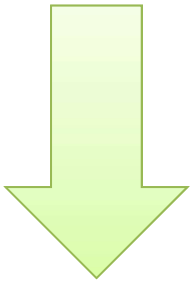
- Org. Esterna
- Resp. del Trattamento

Soggetti Autorizzati del Trattamento con Delega - SATD

- Org. Esterna
- Resp. del Trattamento

Soggetti Autorizzati del Trattamento - SAT

ASL – Titolare del trattamento



Designa per iscritto i soggetti autorizzati al trattamento dei dati personali con delega.

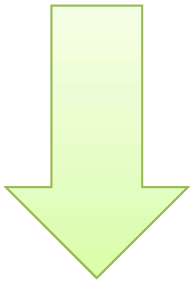
Soggetti Autorizzati del Trattamento con Delega

È fatto obbligo al SATD 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;
- 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.

Direttori e Dirigenti delle UOC e UOSD

SATD



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

Soggetto Autorizato al Trattamento SAT

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**.

Responsabile della Protezione dei dati (DPO)

Nuova figura professionale

obbligatoria presso:

Aziende Pubbliche

(caso della ASL Lanciano Vasto Chieti)

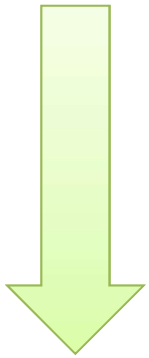
Aziende che effettuano un **monitoraggio regolare e sistematico degli interessati su larga scala**

Aziende che trattano i **dati particolari ex art.9 GDPR**
(caso della Lanciano Vasto Chieti)

Funzioni e Poteri del DPO

- 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

Destinatario



È il soggetto che riceve comunicazione di dati personali, che si tratti o meno di terzi.

Obbligo di Informativa e Consenso

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)

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 ASL

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

Adozione del Registro delle attività di trattamento

una **mappa** dettagliata di tutti i trattamenti effettuati dall'organizzazione del titolare e del responsabile, funge e **comprova** l'adeguamento al GDPR dinanzi all' autorità di controllo.

Obbligatorietà del Registro

Obbligatorio

per il titolare del trattamento (ASL) con almeno 250 dipendenti

OPPURE, al di sotto tale soglia,

se effettua un trattamento che presenti un **rischio per i diritti e le libertà degli interessati** e **non sia occasionale** o **includa dati particolari o dati relativi a condanne penali**

FORMA SCRITTA OBBLIGATORIA

è valida sia la forma cartacea che quella elettronica

REGISTRO DEL TITOLARE DEL TRATTAMENTO:

Il **registro** contiene tutte le seguenti informazioni:

- il nome e i dati di contatto del **titolare del trattamento** e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
- le **finalità** del trattamento;
- una descrizione delle **categorie di interessati** e delle **categorie di dati personali**;
- le categorie di **destinatari** a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- 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 al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
- ove possibile, i **termini ultimi previsti per la cancellazione** delle diverse categorie di dati;
- ove possibile, una **descrizione generale delle misure di sicurezza tecniche e organizzative** di cui all'articolo 32, paragrafo 1.

Gli obblighi in termini di protezione dei dati personali si possono ricondurre ai seguenti due articoli nell'ambito della gestione del rischio:

Art. 32 – Sicurezza del Trattamento

Art 35 - Valutazione d'impatto sulla protezione dei dati

Art. 32 – Sicurezza del Trattamento

Tenendo conto

- dello **stato dell'arte** e
- dei **costi di attuazione**,

nonché

- della **natura**,
- dell'**oggetto**,
- del **contesto**
- delle **finalità del trattamento**,
- come anche del **rischio** di varia **probabilità** e **gravità** per i **diritti e le libertà delle persone fisiche**

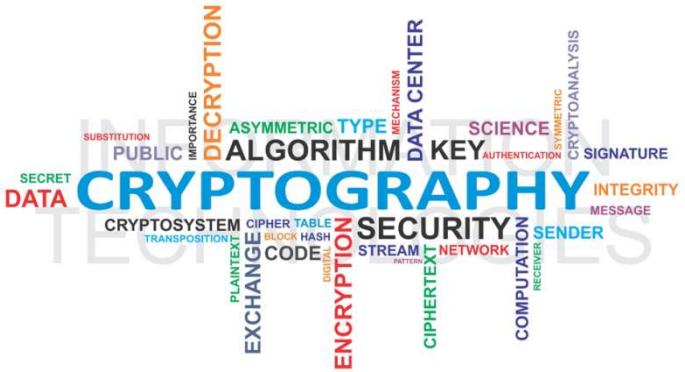
il **titolare** del trattamento e il **responsabile** del trattamento mettono in atto **misure tecniche e organizzative idonee a garantire un livello di sicurezza ADEGUATO al rischio**

Art. 32 – Sicurezza del Trattamento (II) – Misure

… comprendono, tra le altre, se del caso:

- **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**.

Comprendere le proprie responsabilità

Il lavoratore, soggetto autorizzato al trattamento dei dati personali, gioca un ruolo chiave nell'assicurare che l'insieme dei computer e le reti siano sicure e funzionanti ogni giorno.

Perché?

<u>i lavoratori sono coloro che usano questi strumenti ogni giorno</u>

- una ***distrazione*** o l'***uso scorretto*** di tali strumenti (→ l'**incipit** per una falla)
- in quanto essere umano → **debolezze**.

(Fattore umano = vettore di attacco)

Comprendere le proprie responsabilità

- Il suo **comportamento**
- l'**attenersi** a quanto stabilito dal regolamento informatico aziendale
- la **prontezza** nell'**identificare** un' ipotetica minaccia
- la conseguente **segnalazione**

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

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

Comprendere le proprie responsabilità

Il lavoratore in quanto soggetto che ha un contatto diretto con i sistemi e le reti aziendali, ogni sua azione determina una diretta conseguenza all'interno dell'infrastruttura.

Qual è uno dei focus dell' **ATTACCANTE**?

Perché?

- detenere le credenziali di accesso all'infrastruttura informatica
- essere indotto erroneamente ad aprire un file
- ricattato, e quindi costretto, ad effettuare determinate azioni
- detenere informazioni utili a comprendere il contesto della società

Scrivania = Vettore d'attacco

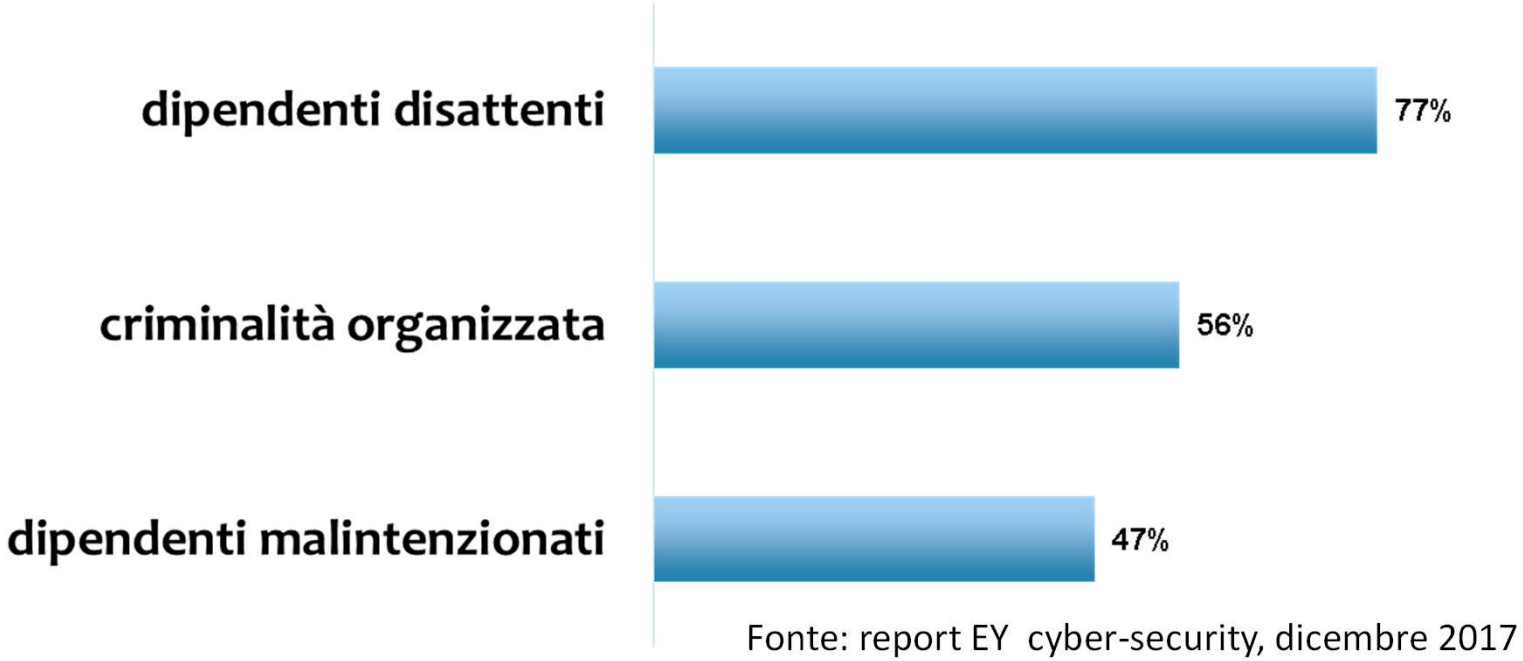
Scrivania a norma GDPR

GUIDA GDPR

In collaborazione con Ufficio Privacy e D.P.O. - Dott. Giovanni Modesti

Le minacce non sono solo esterne…

Le cause principali della vulnerabilità informatica sono:



Fonte: report EY cyber-security, dicembre 2017

Le minacce non sono solo esterne…

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

Alcune potenziali conseguenze

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 spiega perché l'impegno dell'Azienda nel redigere regolamenti sia in termini di sicurezza fisica che informatica.

Perché prevenire i rischi di attacchi cyber?

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

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 e cd inseriti

Alcune minacce

- **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

Cosa si potrebbe fare?

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 lavoratore** effettua al Responsabile della UO.

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

A chi deve essere inviata la segnalazione di Data Breach?

- Al Team di Valutazione dei Data Breach, che:
- 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

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.

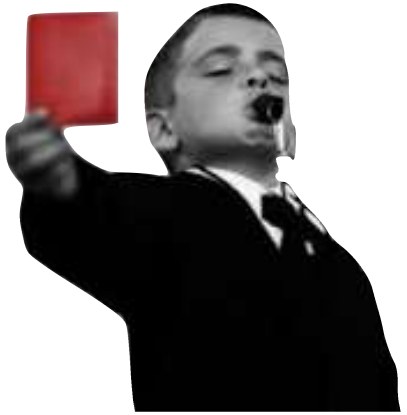
Esonerati soltanto

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

Art. 83 LE SANZIONI

Le sanzioni devono essere in ogni singolo caso:

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



Parametri di riferimento:

- ➢ 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

Regime Sanzionatorio

Fino a **10 milioni di Euro** o, per le imprese, fino al **2% 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**

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:

- **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)**

In collaborazione con Ufficio Privacy e D.P.O. - Dott. Giovanni Modesti

GRAZIE PER L'ATTENZIONE

Ufficio Privacy
D.ssa G. Chieffo
Dott. Gaspare Staniscia
ufficio.privacy@asl2abruzzo.it

DPO
Dott. Giovanni Modesti
dpo@asl2abruzzo.it