

I dati personali: il GDPR

**TUTORIAL DAYS di CCR 2022:
CYBERSICUREZZA**

Silvia Arezzini



Data Protection Officer

Un team di aiuto, supporto, monitoring nell'ambito della protezione dei dati personali all'interno dell' Ente *Deliberazione n. 14734 del 27 Aprile 2018*

Istituito dal **REGOLAMENTO (UE) 2016/679 – GDPR**

in vigore dal 25.5.2018

recepito da INFN con la delibera n. 14844 del 27 Luglio 2018



Privacy & Cybersecurity

Un binomio indissolubile

La protezione dei dati personali può nascere solo dalla protezione più generale dell'infrastruttura digitale e delle sue componenti

Ma «privacy» è anche altro



Proteggere

Confidentiality (Riservatezza)

Integrity (Integrità)

Availability (Disponibilità)

Le parole della «CIA»

RISERVATEZZA: Solo chi ne ha diritto può accedere all'informazione

Identità, Autenticazione, Autorizzazione, protezione dei file, ruoli...

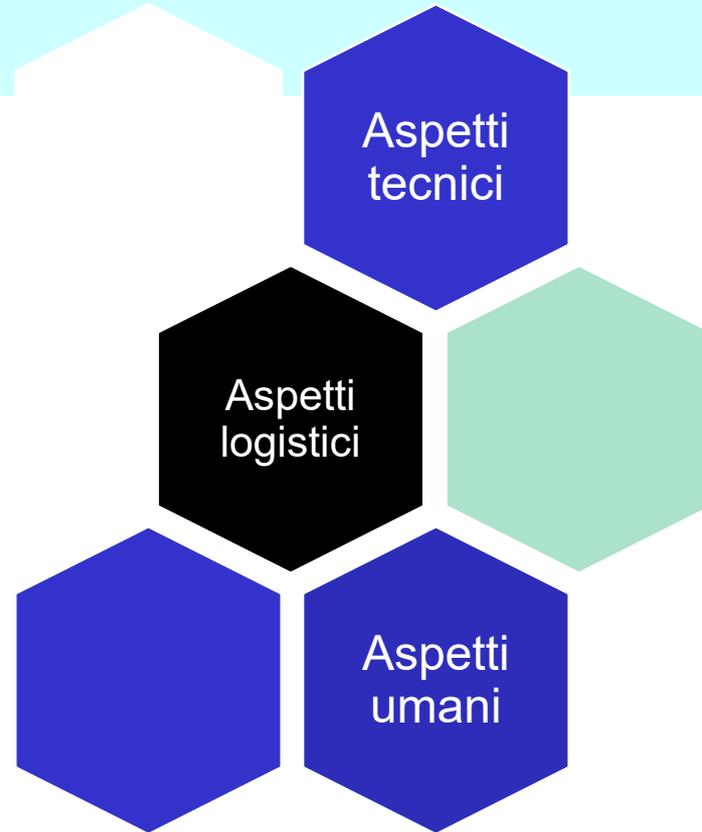
INTEGRITA': In ogni momento l'informazione è corretta e non ha subito modifiche.

LOG, non ripudiabilità...

DISPONIBILITA': L'informazione è disponibile quando richiesta.

DDOS, eventi fisici,...

AMMINISTRATORE di SISTEMA



ANALISI DEL RISCHIO

CYBERSECURITY

Non basta la tecnica...

Non basta
l'organizzazione...

Non dimenticare l'aspetto
umano

Minacce informatiche





**YOUR PERSONAL FILES
ARE ENCRYPTED**

Make payment or private key
will be destroyed in
12 Hours 01:34

Minacce informatiche

PROTEZIONE dei DATI PERSONALI

Le stesse considerazioni, declinate con grande attenzione perché stiamo **trattando dati che riguardano le persone.**

Il GDPR nei primi articoli richiama proprio l'importanza dei dati personali,

...e enuncia dei principi a cui riferirsi

DATA PROTECTION BY DESIGN

WIKIPEDIA: Privacy by design riguarda il principio di incorporazione della privacy a partire dalla progettazione di un processo aziendale con le relative applicazioni informatiche di supporto.

saper dimostrare che un trattamento è progettato e organizzato fin dall'inizio in maniera tale da offrire per l'intera gestione del ciclo di vita dei dati, le garanzie indispensabili a soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati.

DATA PROTECTION BY DEFAULT

per impostazione predefinita devono essere trattati solo i dati personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini.

PRINCIPIO DI MINIMIZZAZIONE

saper dimostrare che i dati trattati per impostazione predefinita (di default) sono solo quelli necessari per ogni specifica finalità del trattamento, evitando di acquisire informazioni eccedenti gli obiettivi dichiarati nell'informativa

PRINCIPIO DELL'ACCOUNTABILITY o della responsabilizzazione

dal Garante:

Il GDPR pone con forza l'accento sulla "responsabilizzazione" (accountability: **essere in grado di render conto**) di titolari e responsabili – ossia, sull'**adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento**. Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali – nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

Non è più la legge che mi dice cosa devo fare ma sono io che devo dimostrare cosa faccio per prevenire rischi sui diritti e le libertà delle persone



Diritti e libertà delle persone fisiche.

GDPR

il **GDPR** non è un insieme di norme precettive

E' invece una sorta di “**framework normativo**” disegnato con l'obiettivo sì di proteggere, ma anche di favorire la circolazione dei dati.

Dati all'estero!

coinvolgimento

Privacy & Consapevolezza

Di chi tratta i dati (autorizzati)

uffici di Direzione, del Personale, Amministrazioni Centrali e Locali, Uffici Fondi esterni, PI e responsabili di progetti,...

Di chi si occupa di security

Servizi Calcolo e Reti, CCR e gruppo Security, Sistema Informativo,...

Di chi si occupa di privacy

DPO, referenti privacy, CCR e gruppo Harmony

PER...

Progettare prodotti

Definire processi

SPORT di SQUADRA!



Thank You

