Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

GDPR e trattamento dei dati personali (privacy e cybersecurity)

Corso di formazione per neoassunti nelle attività di Computing

Silvia Arezzini

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

GDPR

Un termine comparso ieri!

In riferimento ad una serie di attività legate alla FISICA MEDICA

Ma non è l'unico ambito che ci riguarda...

In sintesi

Cosa è il GDPR

Privacy e Protezione dei Dati Personali

Perchè e come il GDPR riguarda la comunità del calcolo INFN (noi)

Privacy & Cybersecurity

Registro Trattamenti / Data Breach / DPIA

Le norme nell'INFN

I documenti che recepiscono la normativa

Centro di calcolo Pisa Tier2 CMS/Belle2
CCR AAI Formazione Harmony

Componente di un team

Evoluzione del concetto di privacy

Stefano Rodotà

«…dal diritto di essere lasciato solo, al diritto di mantenere il controllo sulle proprie informazioni…»

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

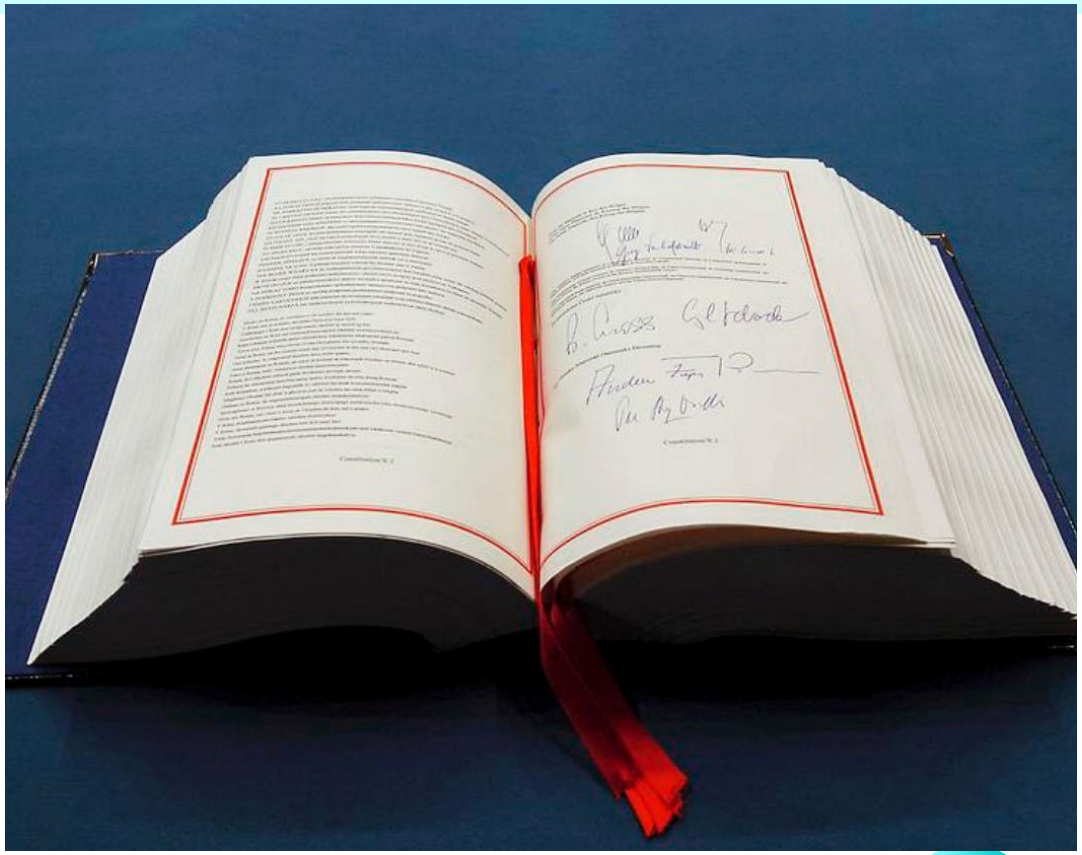
LA NORMATIVA COMUNITARIA

In prestito da E. Ronconi

Carta dei diritti fondamentali dell'Unione europea

(Nizza 7-12-2000)

Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano



Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

LA NORMATIVA COMUNITARIA

In prestito da E. Ronconi

REGOLAMENTO (UE) 2016/679

del 27 aprile 2016

relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati

(***in vigore dal 25.5.2018***)

In prestito da E. Ronconi

LA FINALITÀ

proteggere i dati personali

con una disciplina unica

e direttamente

applicabile in tutti gli Stati

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

LA NORMATIVA NAZIONALE

In prestito da E. Ronconi

Decreto Legislativo

del 30 giugno 2003 n. 196

(Codice in materia di protezione dei dati personali)

modificato dal

Decreto Legislativo

10 agosto 2018 n. 101

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

In prestito da E. Ronconi

LE DUE NORMATIVE

- **HANNO APPLICAZIONE DIRETTA,**
- **COESISTONO,**
- **VANNO CITATE ENTRAMBE.**

ai sensi del Regolamento UE 2016/679 e del D.Lgs. 30 giugno 2003 n. 196 e ss.mm.ii.

IL DATO E' ...

In prestito da E. Ronconi

qualsiasi **informazione** riguardante

una persona fisica identificata o identificabile

IL SOGGETTO TUTELATO

INTERESSATO

- *persona fisica*
- *identificata o identificabile,*
- *direttamente o indirettamente.*
- *Non le persone giuridiche*

ESCLUSIONE DAL GDPR

In prestito da E. Ronconi

DATI ANONIMI

- informazioni che non riguardano una persona identificata o identificabile

DATI ANONIMIZZATI

- trattamento volto a de-identificare **in maniera irreversibile** l'informazione dal soggetto cui si riferisce (tecniche di *randomizzazione* o di *generalizzazione*)

INCLUSIONE NEL GDPR

In prestito da E. Ronconi

DATI PSEUDONIMIZZATI

- i dati personali che non possono più essere attribuiti a un interessato specifico **senza l'utilizzo di informazioni aggiuntive**, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile - *cifratura*

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

CLASSIFICAZIONE DEI DATI

In prestito da E. Ronconi

DATO COMUNE	• permette l'identificazione diretta o indiretta di una persona
DATO PARTICOLARE	• rivela l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale.
DATO GIUDIZIARIO	• rivela l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale

QUALCHE ESEMPIO

In prestito da E. Ronconi

nome	numero di identificazione	dati relativi all'ubicazione	identificativo online (indirizzi IP)	identità fisica
identità fisiologica	identità psichica		identità genetica	dati biometrici
dati sulla salute	identità economica	identità culturale	identità sociale	

IL TRATTAMENTO E' ...

In prestito da E. Ronconi

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 ….

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

TIPOLOGIE DI TRATTAMENTO

In prestito da E. Ronconi

RACCOLTA	REGISTRAZIONE	ORGANIZZAZIONE	STRUTTURAZIONE	CONSERVAZIONE	ADATTAMENTO
MODIFICA	ESTRAZIONE	CONSULTAZIONE	USO	COMUNICAZIONE MEDIANTE TRASMISSIONE	DIFFUSIONE O QUALSIASI ALTRA FORMA DI MESSA A DISPOSIZIONE
RAFFRONTO	INTER CONNESSIONE	LIMITAZIONE	CANCELLAZIONE	DISTRUZIONE	

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

In prestito da E. Ronconi

E' NORMATIVA PERVASIVA DI OGNI ATTIVITA' DELL'INFN

10 ottobre 2023

In prestito da E. Ronconi

PRINCIPIO DELL'ACCOUNTABILITY
o della responsabilizzazione/rendicontazione

spetta titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, dimostrando e comprovando la conformità al GDPR

I soggetti del trattamento

chi protegge i dati dell'interessato?

In prestito da E. Bovo

TITOLARE: la persona fisica o giuridica o l'autorità pubblica che **determina le finalità e i mezzi del trattamento**

AUTORIZZATI: coloro che agiscono sotto l'autorità del Titolare

POSSONO AGGIUNGERSI

ALTRI TITOLARI AUTONOMI: persone fisiche o giuridiche la cui **attività** è **definita dettagliatamente da norme di legge** e per lo svolgimento della cui attività sono **specializzati e appositamente autorizzati**

RESPONSABILI DEL TRATTAMENTO: coloro che effettuano un trattamento **per conto** del Titolare

CONTITOLARI: le persone fisiche o giuridiche o autorità pubbliche che **determinano congiuntamente** le finalità e i mezzi del trattamento

E il DPO… Data Protection Officer o Responsabile della Protezione dei Dati (RPD)

PROMUOVERE LA CULTURA DELLA PROTEZIONE DEI DATI PERSONALI e contribuisce all'attuazione del GDPR

INFORMARE E FORNIRE CONSULENZA al titolare circa gli obblighi che derivano dalla normativa comunitaria e nazionale in materia

VIGILARE SULL'OSSERVANZA DEL GDPR nelle politiche del titolare in materia di trattamento

FORNIRE PARERI in merito alla valutazione di impatto

COOPERARE COL GARANTE

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

PRINCIPI DEL TRATTAMENTO

In prestito da E. Ronconi

LICEITÀ (avere corretta base giuridica), CORRETTEZZA (rispetto ai doveri di lealtà e buona fede) E TRASPARENZA (informare l'interessato)

del trattamento nei confronti dell'interessato;

LIMITAZIONE DELLA FINALITÀ

assicurarsi che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati;

MINIMIZZAZIONE DEI DATI:

i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento;

ESATTEZZA E AGGIORNAMENTO

compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;

LIMITAZIONE DELLA CONSERVAZIONE:

è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;

INTEGRITÀ E RISERVATEZZA:

occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento.

BASI GIURIDICHE DEL TRATTAMENTO DEI DATI COMUNI

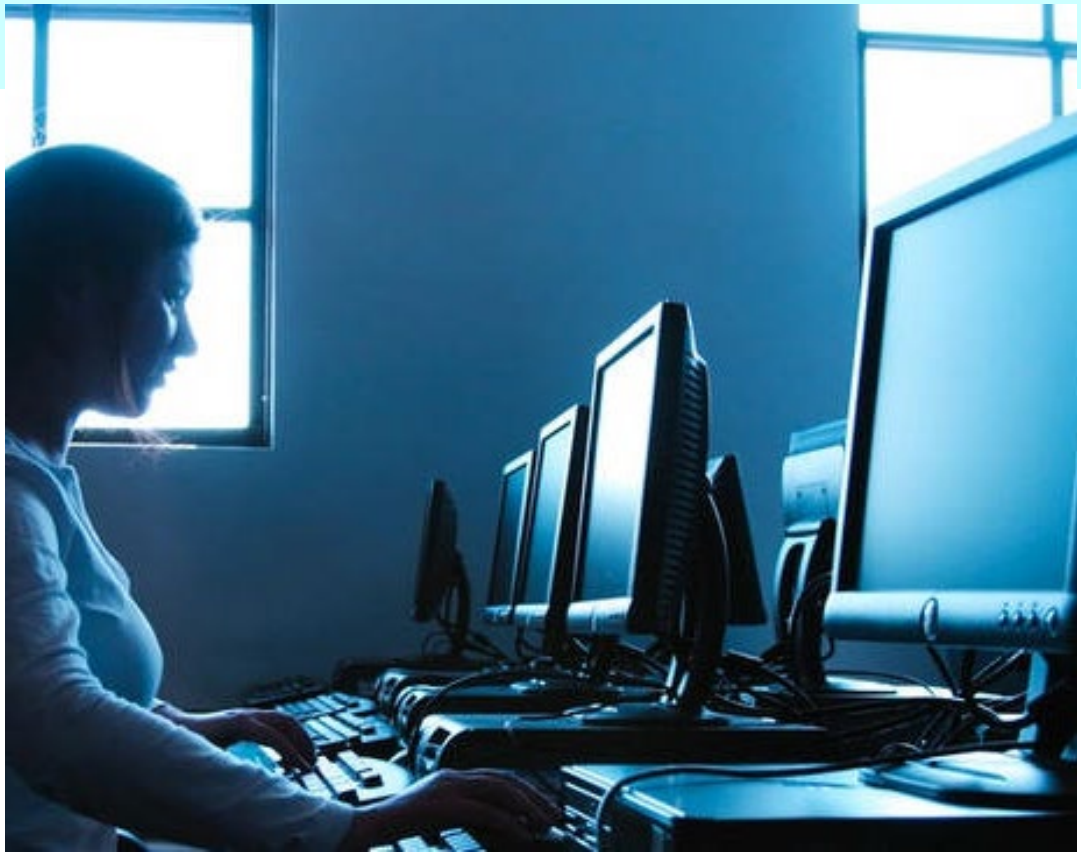
- CONSENSO *
- ADEMPIMENTO OBBLIGHI CONTRATTUALI
- INTERESSI VITALI DELLA PERSONA INTERESSATA O DI TERZI
- OBBLIGHI DI LEGGE CUI È SOGGETTO IL TITOLARE *
- INTERESSE PUBBLICO O ESERCIZIO DI PUBBLICI POTERI
- INTERESSE LEGITTIMO PREVALENTE DEL TITOLARE O DI TERZI CUI I DATI VENGONO COMUNICATI

In prestito da E. Ronconi

Chi tratta i dati nell'INFN?

coloro che operativamente trattano i dati personali secondo le istruzioni del Titolare sono

AUTORIZZATI



DESIGNAZIONE E ISTRUZIONI AGLI AUTORIZZATI

in: https//dpo.infn.it

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

In prestito da E. Ronconi

Istituto Nazionale di Fisica Nucleare

Designazioni delle persone autorizzate al trattamento dei dati personali

Il/La sottoscritto/a _____ in qualità di Direttore della Sez/Lab (oppure Direzione/Servizio AC) INFN di _____

DESIGNA

le persone sotto elencate quali **autorizzate al trattamento** dei dati personali da effettuarsi sia in modo cartaceo che elettronico, nell'ambito a ciascuno indicato e con accesso ai soli dati la cui conoscenza sia necessaria per adempiere ai compiti assegnati; consegna a ciascun incaricato le Norme per il trattamento dei dati personali prescrivendone l'osservanza.

Cognome	Nome	Ambito di trattamento[1]	Conferimento incarico e ricevute Norme per il Trattamento		Revoca incarico	
			Data	Firma	Data	Firma

Il Direttore

_____

[1] l'ambito del trattamento di ogni autorizzato è individuato in ragione dei compiti allo stesso assegnati che coinvolgono il trattamento di dati personali.

Istituto Nazionale di Fisica Nucleare
Responsabile Protezione Dati

Norme per il trattamento di dati personali nell'INFN

4 Dicembre 2018

Premessa

Questo documento contiene le istruzioni per il trattamento dei dati personali nell'Istituto Nazionale di Fisica Nucleare (di seguito anche INFN) in conformità a quanto disposto:

- dal Regolamento UE 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati (di seguito anche Regolamento);
- dal Codice in materia di trattamento dei dati personali di cui al D.Lgs. n. 196/2003 e ss.mm.ii. recante disposizioni per l'adeguamento nazionale al Regolamento UE n. 2016/679 (di seguito anche Codice).

Il personale dipendente ed associato, nonché tutti coloro che collaborano a qualunque titolo nelle attività dell'INFN che comportino il trattamento di dati personali, sono tenuti ad osservarle, conformando la propria condotta a criteri di diligenza e correttezza, al fine di assicurare la massima tutela ai dati trattati.

Definizioni

Si intende per

- **Dato Personale:** qualsiasi informazione riguardante una persona fisica («interessato») identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamen-

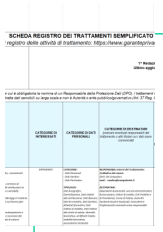
Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

GLI STRUMENTI PER DIMOSTRARE IL RISPETTO DEI PRINCIPI GENERALI

In prestito da E. Ronconi

INFORMATIVA

AUTORIZZATI



REGISTRO TRATTAMENTI

CONTRATTO RESPONSABILE

VALUTAZIONE D'IMPATTO

REGISTRO DATA BREACH

- DOVE
- COME
- QUANDO
- PERCHE'

incontriamo (o ci scontriamo...) con la PRIVACY?

Privacy?

- NORMATIVA PERVASIVA DI OGNI ATTIVITA' DELL'INFN quindi anche delle nostre attività:
  - Non solo perchè trattiamo dati che riguardano le attività di persone fisiche,
  - Ma anche e soprattutto perchè chi opera nelle attività di IT è chiamato a **proteggere** con idonee misure (cybersecurity) i dati personali trattati dall'Ente.

IT:
i due ambiti della privacy

- Problematiche di tutti i giorni dalla manipolazione dei dati personali vera e propria (log, file con username, database di utenti e asset, ticketing system ecc) al costruire un habitat protetto (privacy by design e by default) e ritagliato sulle caratteristiche della propria struttura alla condivisione di regole con tutta la comunità INFN…

- La cybersecurity…

GDPR (art.24)

misure tecniche ed organizzative adeguate a garantire, e se richiesto a dimostrare, che i dati personali vengono protetti a norma di regolamento.

File di LOG

- user names nei log files
- log di sistema con dati personali
- SIEM (Security Information and Event Management)

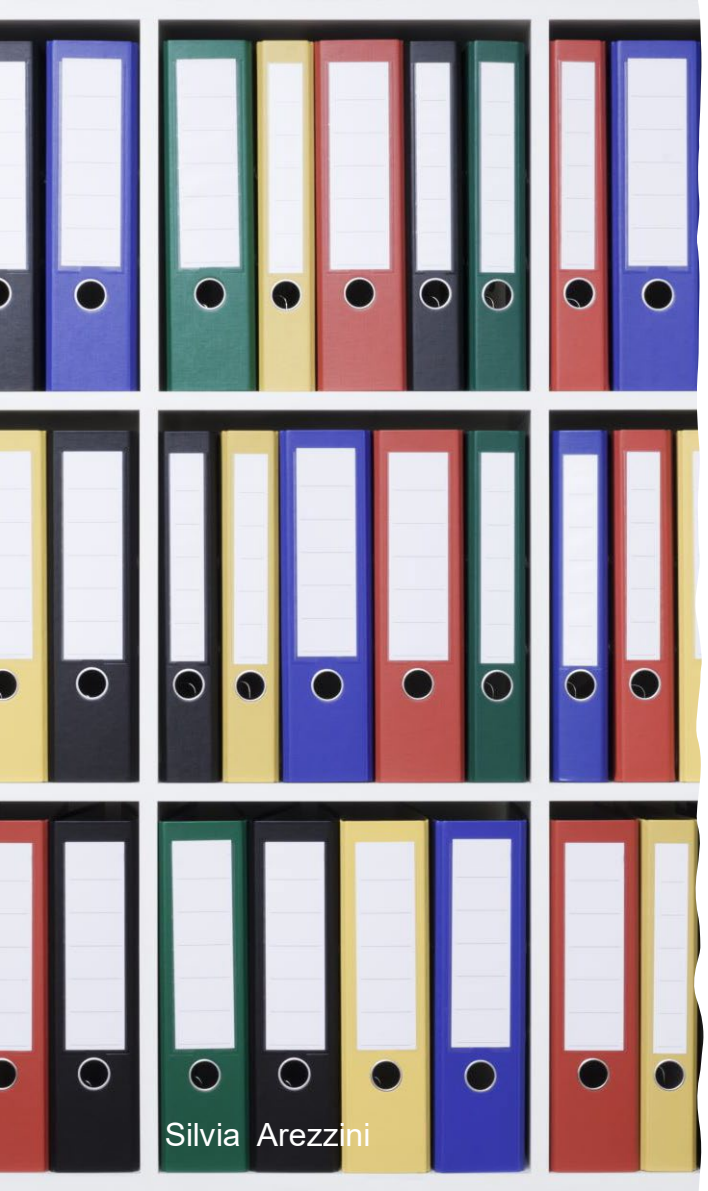
Il log file è il tipico file contenente dati personali che il sistemista è chiamato a trattare

Nomina a autorizzato al trattamento dei dati personali

La conservazione dei log è normata dal nostro disciplinare sull'uso delle risorse informatiche:

Tempo di conservazione un anno

- Non sono elencati tutti i tipi di log
- ma è sensato individuare in un anno il periodo tipico di conservazione



altri file
non esaustivo…

DataBase utenti

locali Directory Server di Domini Windows

etc/passwd etc/group

INFNwide ldap, GODiVA

DataBase degli asset, con associazione di utenti

Ticket system

E-mail

Tipica attività legata al trattamento di dati personali richiamata specificamente nel disciplinare risorse informatiche.

Servizio da proteggere (antivirus/antispam)

Un uso estremamente diffuso, eccessivamente diffuso…

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

problematiche e-mail

Dati personali che il singolo utente «scrive» nei suoi mail	La scrittura di un mail e la sua spedizione tramite il sistema di posta, generano dei dati personali che vengono registrati nel server di posta: mittente, destinatario, ora… Non confondiamoli con quanto di personale un utente scrive all'interno dei suoi messaggi
Dati personali riguardanti gli utenti che vengono trasferiti via mail	La posta elettronica non è più l'unico mezzo per trasferire dati personali nell'ambito lavorativo. •Aspetti organizzativi del lavoro d'ufficio e necessità di usare strumenti più appropriati •Pericoli legati alla posta elettronica
Posta elettronica usata per attività personali non lavorative	Il Disciplinare Risorse Informatiche prevede un uso modesto delle risorse dell'ente per usi personali.
Forward della casella di posta su un provider diverso…	Meglio di no…

Server WEB

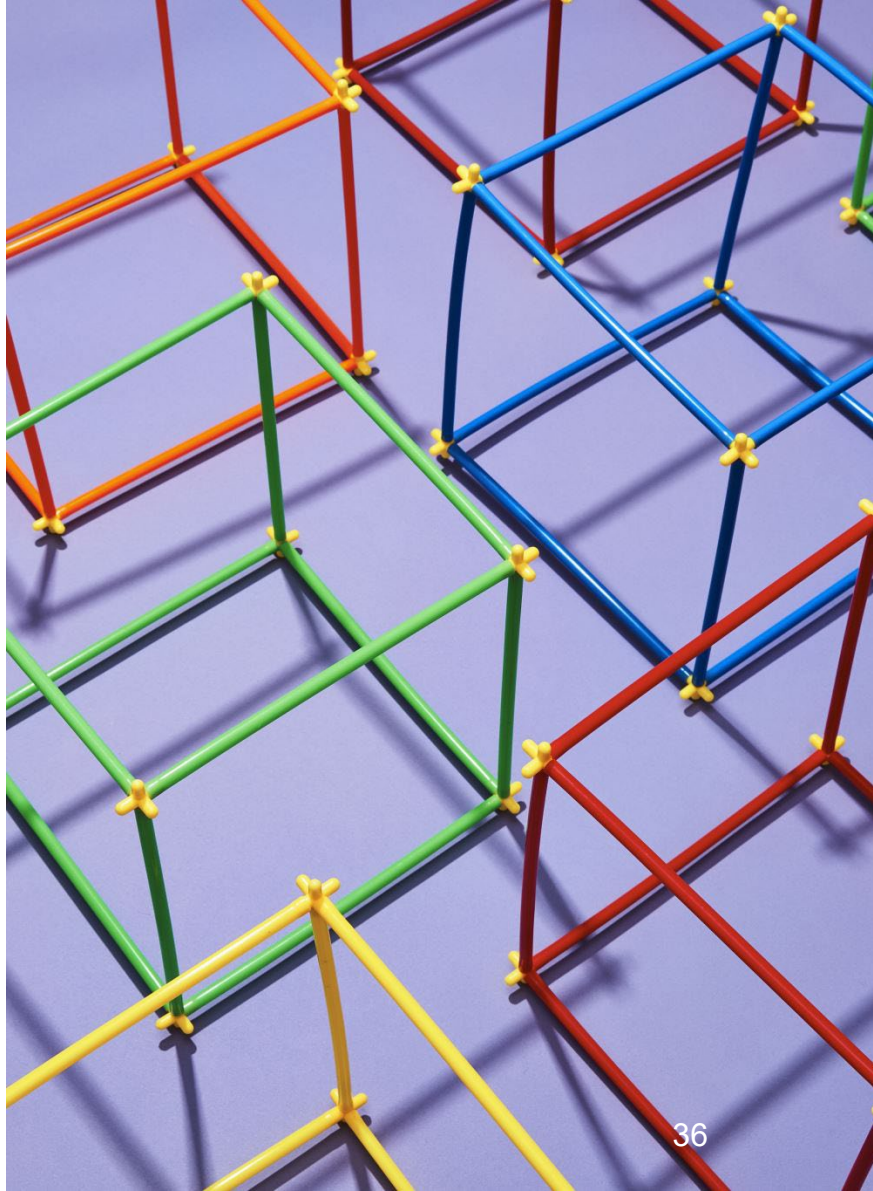
Gestione della privacy di un sito web istituzionale

Indicazioni standard.

E’ necessario fornire una informativa, accessibile da tutte le pagine del sito. L’informativa deve essere personalizzata e non può essere quella generica fornita dal DPO.

Occorre una indicazione specifica per i cookie, che quindi devono essere attentamente valutati. La problematica più significativa è quella dei cookie analitici, nel caso in cui siano presenti.

Google Analytics… recente richiamo del Garante Privacy



Organizzazione eventi fisici/virtuali

Eventi

iscrizioni

informazioni sulla salute per la predisposizione di cibi

acquisizione di materiale audio/video

registrazioni di presentazioni, foto e video ricordo ecc. utilizzabili eventualmente anche con scopi pubblicitari interni

INFORMATIVA sul sito DPO, da ADATTARE

CONSENSO uso di materiale audio/video/fotografico

& alla pubblicazione del nominativo tra l'elenco degli iscritti

sistemi automatizzati (come agenda/indico)

Particolare attenzione al mancato consenso per l'uso di immagini.

Elenco partecipanti

In caso di evento fisico appositi spazi video/foto free

FOTO e VIDEO

Foto di persone ben riconoscibili

Se l'identità non è chiara perché è oscurata o sfocata o perché il soggetto è ripreso in una modalità che ne impedisce il riconoscimento il problema non si pone .

(ed è questa lo modalità da usare in particolari contesti)

CONSENSO

INFORMATIVA

Esempi: formazione INFN

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

DROPBOX e gli altri???

Utilizzo di piattaforme esterne

Dal disciplinare sull'uso di risorse informatiche

il trattamento dei dati personali di qualunque tipo o di particolare rilevanza per l'Ente può essere effettuato mediante l'uso di servizi esterni, anche di tipo cloud, soltanto ove l'INFN abbia preventivamente verificato i rischi e i benefici connessi ai servizi offerti, i limiti nella circolazione e trasferimento dei dati, nonché l'affidabilità del fornitore, la sussistenza di garanzie e cautele per la conservazione, persistenza e confidenzialità dei dati oltre ai profili di responsabilità nel trattamento

O365 **un discorso un po' diverso**

RUP & Gare Commissari & Concorsi

La documentazione di gara deve essere trattata solo da personale incaricato del trattamento ed è quindi necessario che il RUP venga nominato tale dal Direttore.

Il RUP deve trattare convenientemente i dati. Per questo è ragionevole predisporre istruzioni che rimandino alle norme INFN e prevedere della formazione specifica.

Può essere certo fonte di preoccupazione sapere che i RUP conservano sui loro computer personali molti dei dati relativi alle gare. Per questo è raccomandabile il ricorso a spazi condivisi centralizzati, in grado di fornire la possibilità di archiviazione remota su server ben protetti. E' chiaro però che l'eventuale trasferimento su sistemi personali rientra nella facoltà del RUP che deve per questo essere conscio delle responsabilità collegate a questa operazione.

Analoghe considerazioni valgono per i commissari di concorso nel momento in cui decidono di trasferire sui loro sistemi i dati personali relativi ai concorrenti.

anonimizzare / pseudonimizzare

Progetti «salute»

Le problematiche di anonimizzazione/pseudonimizzazione di dati non sono in generale presenti nelle attività standard del sistemista INFN. Esse possono presentarsi in situazioni particolari ad esempio nel caso di progetti in cui siano presenti dati sanitari. In questo caso, se l'INFN è chiamato a trattare questo tipo di dati occorre prevedere misure specifiche. Esiste una indicazione ad hoc del garante

La problematica dei dati biologici in generale attiene a specifici progetti con entità esterne. In più occasioni il DPO ha avuto modo di dare indicazioni considerato anche che esistono specifiche raccomandazioni del Garante.

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Attenzione…
Privacy e accesso a dati personali

E’ una preoccupazione frequente dei sistemisti:

Nel corso del mio lavoro può capitare di «vedere» dati personali degli utenti

Qui non si tratta di applicare le norme sulla privacy, ma quelle sulla deontologia professionale

Cybersecurity

PROTEGGERE cosa?

C.I.A.

Confidentiality (Riservatezza)
Integrity (Integrità)
Availability (Disponibilità)

Documenti protetti, come?

Backup / protezione fisica / cifratura

I documenti che predisponiamo rimangano inalterati nel tempo (non ripudiabilità).

Credenziali / ACL / ruoli

Che i documenti non siano accessibili a chi non ne ha diritto (e siano invece accessibili a chi deve lavorare con essi).

Organizzazione / permessi/ ruoli

Che i documenti risultino sempre disponibili quando devono essere utilizzati.

INTEGRITA' Impedire che possano avvenire cancellazioni o modifiche a causa di interventi non autorizzati o a causa di eventi non facilmente controllabili (incendi, allagamenti…):

modifiche non autorizzate anche accidentali

RISERVATEZZA Impedire che qualcuno possa volontariamente o involontariamente accedere all'informazione senza essere autorizzato:

furti, smarrimenti, accesso da non autorizzati

DISPONIBILITA': Far sì che non venga impedito l'accesso all'informazione a chi ne ha invece l'autorizzazione:

cause accidentali anche fisiche, virus, malware

strumenti

Antivirus

Antispam

Controllo degli accessi

- IAM *Identity & Access Management*
- AAI *Authentication & Authorization Infrasctructure*

Cifratura

Controllo fisico (Sala Calcolo)

Backup

Protezioni dei file

Applicativi di condivisione controllati

IAM & AAI & GODIVA

Accountability

- Organizzazione
- Credenziali
- Ruoli (organigrammi)
- Minimo privilegio

Privacy by design e by default

Minimizzazione

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!***

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

coinvolgimento

Privacy & Consapevolezza

FATTORE UMANO

Di chi tratta i dati (autorizzati)

uffici di Direzione, del Personale, Amministrazioni Centrali e Locali, Uffci 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!

Ma… va sempre tutto liscio?

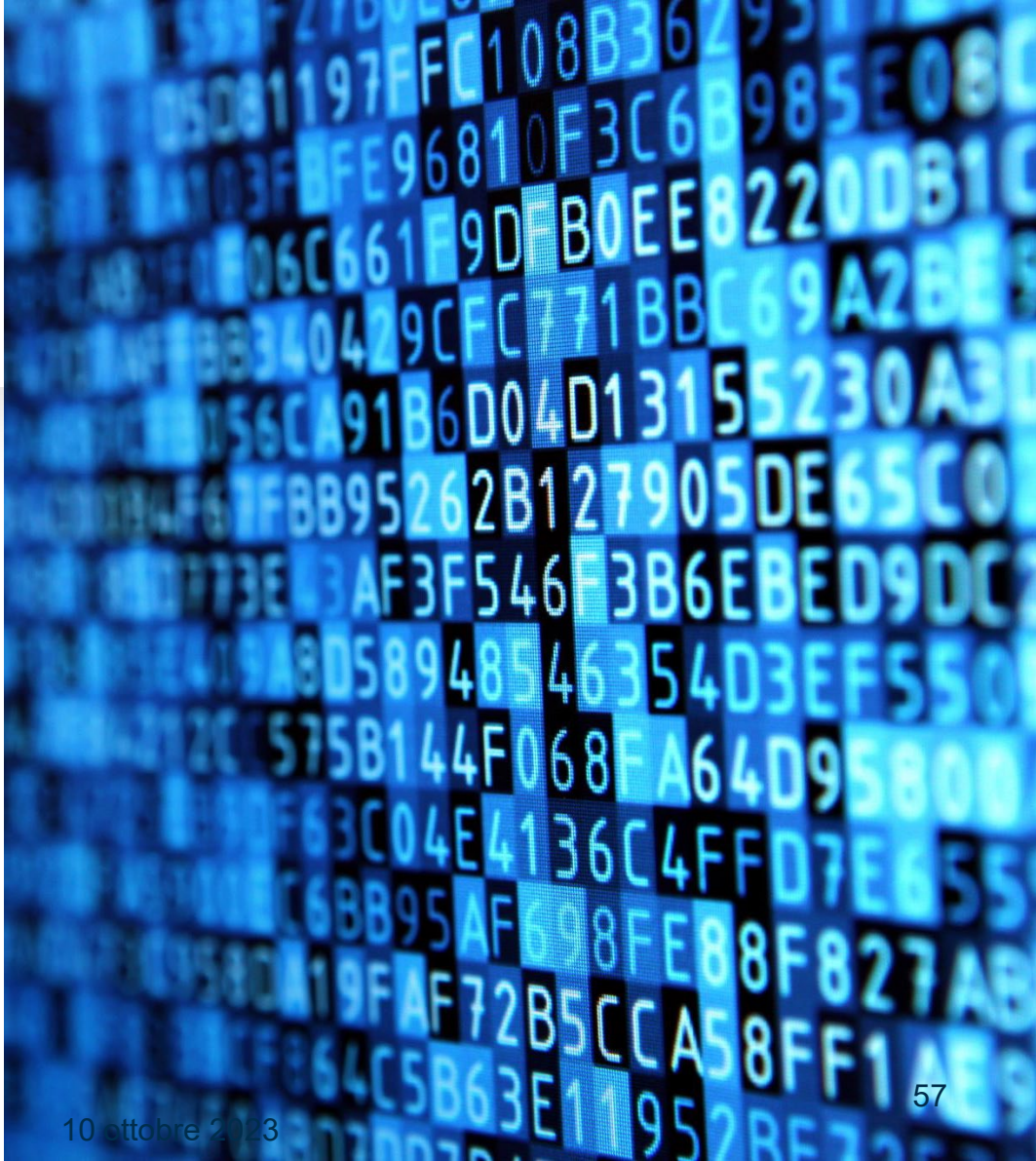
Pericoli e incidenti informatici…

Perdita di disponibilità, integrità e riservatezza

Nel caso di dati personali si parla di DataBreach

Data breach (GDPR, Art. 4.12)

Violazione di sicurezza che comporta 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.



Obblighi del titolare…

… quindi dell' INFN e quindi del Direttore

- Documentare ogni Data Breach (Registro a cura del DPO)
- Notificare ogni Data Breach entro 72 ore. A chi?
  - Al DPO, sempre
  - Al GARANTE PRIVACY se presumiamo possa avere effetti avversi significativi sulle persone coinvolte causando danni (fisici, materiali o immateriali)
  - Agli interessati se presumiamo sussista un rischio elevato ai diritti alla libertà delle persone

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Esempi di “effetti avversi significativi”

- Perdita del controllo sui propri dati personali,
- discriminazione,
- furto d'identità o il rischio di frode,
- perdita di riservatezza di dati personali protetti dal segreto professionale,
- perdita finanziaria,
- danno alla reputazione.

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Strumento di autovalutazione

In prestito da R. Cecchini

Aiuta ad individuare le eventuali azioni da intraprendere:

- notifica all'autorità di controllo,
- comunicazione agli interessati.

https://servizi.gpdp.it/databreach/s/self-assessment

La comunicazione al DPO è sempre obbligatoria.

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Dati inviati per errore

In prestito da R. Cecchini

Un elenco di dipendenti con numeri di telefono e indirizzi di email viene inviato per errore a un altro destinatario.

Il destinatario dichiara di aver cancellato il messaggio.

Nessuna notifica al Garante

Nessuna comunicazione agli interessati

Compromissione di un database

In prestito da R. Cecchini

Sito web compromesso via vulnerabilità SQL. Scaricate alcune centinaia di password, nomi e indirizzi di email.

Notifica al Garante.

Comunicazione agli interessati.

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Compromissione account di posta

In prestito da R. Cecchini

Un utente rivela la password del proprio account di posta che viene usato per spedire un grande numero di mail di spam. Dai log non risulta che siano state fatte altre azioni.

Nessuna notifica al Garante.

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Furto di materiale con dati non cifrati

In prestito da R. Cecchini

Un portatile con dati dei candidati a un concorso viene rubato.

I dati non erano cifrati e alcuni sono particolari.

Notifica al Garante / Comunicazione agli interessati.

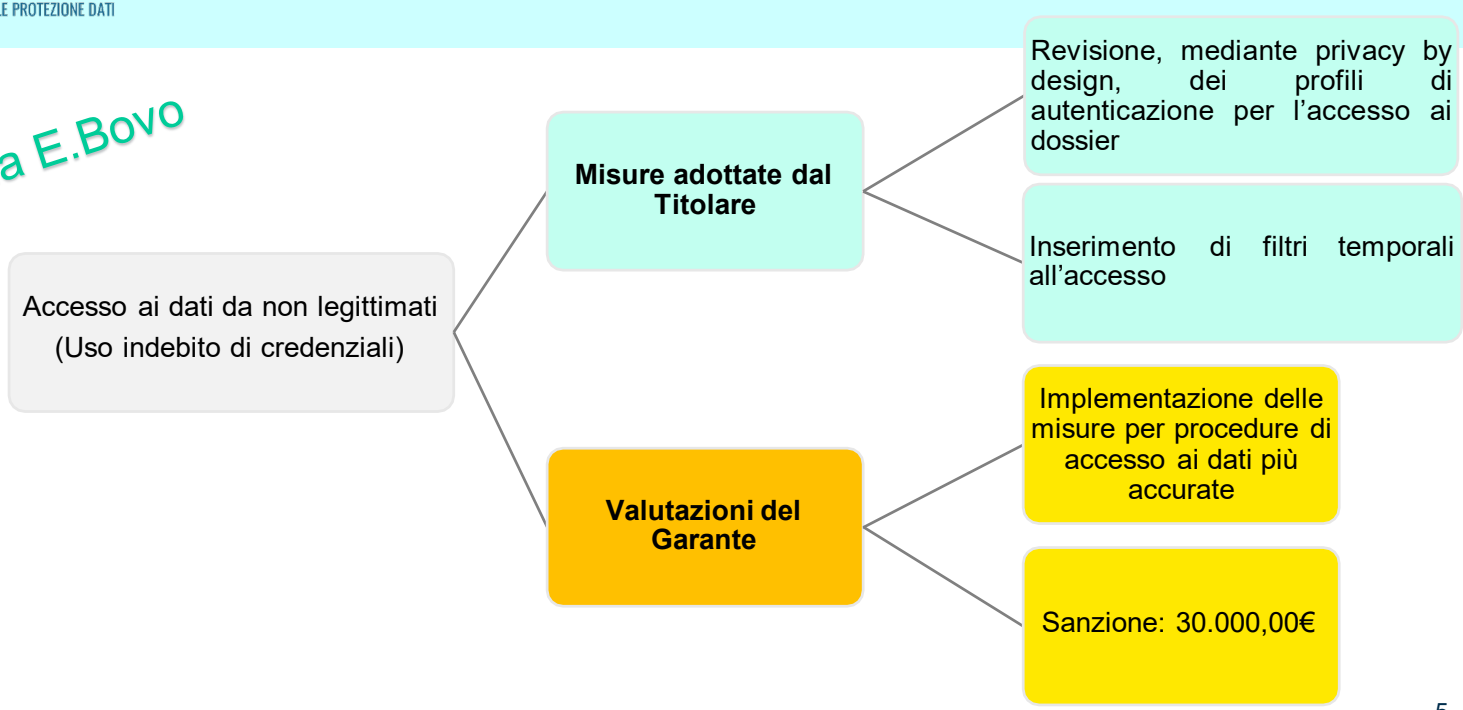
Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Alcuni esempi di data breach sanzionati dal GARANTE PRIVACY

Attenzione a ciò che SEGNALA e SANZIONA il Garante!

Conseguenze delle violazioni

In prestito da E.Bovo



In prestito da E.Bovo

Conseguenze delle violazioni

Visualizzazione indebita di dati (Interferenza tra Piattaforma e Applicativo)

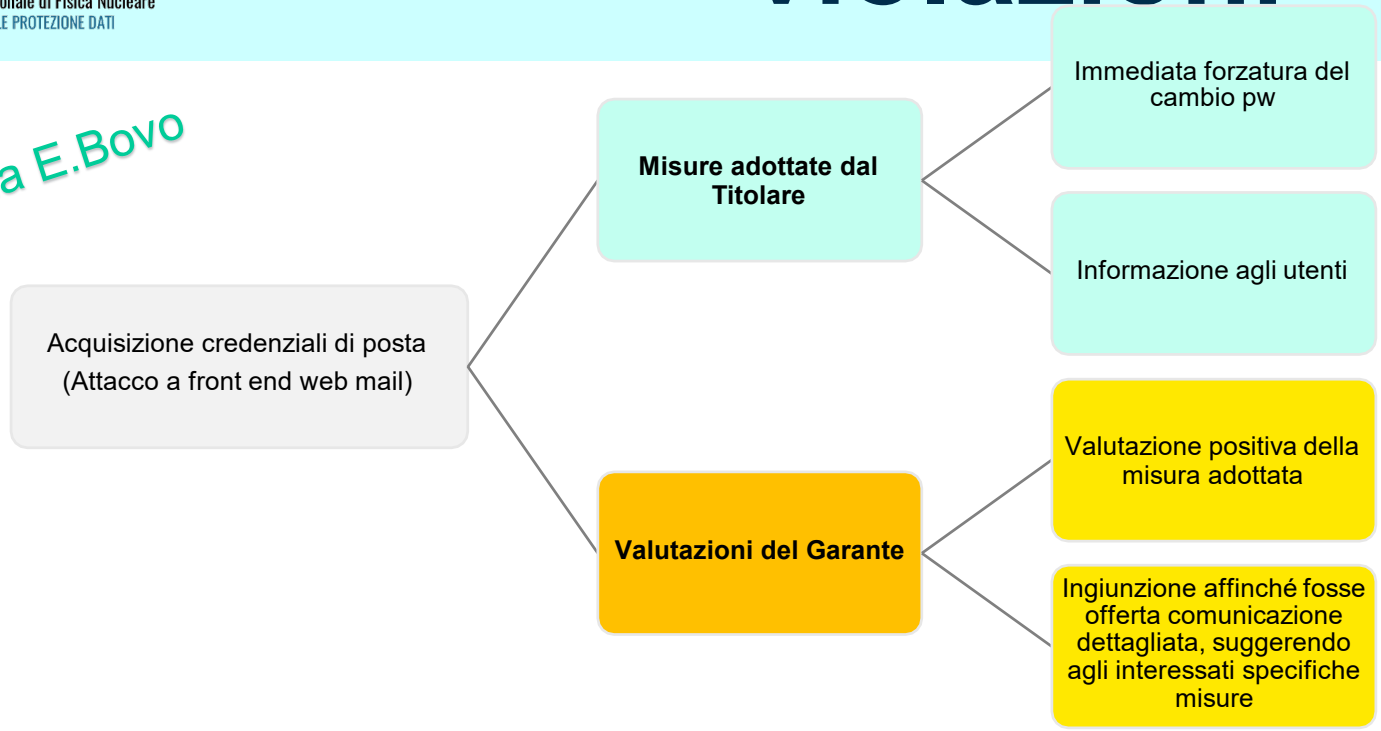
- **Misure adottate dal Titolare**
  - Comunicazione della violazione agli utenti
  - Sospensione dell'applicativo e oscuramento della pagina
  - Analisi dei risultati indicizzati da Google e richiesta rimozione dei contenuti
- **Valutazioni del Garante**
  - Il Titolare è tenuto ad adottare procedure per *"testare, verificare e valutare regolarmente l'efficacia delle misure per garantire la sicurezza"*.
  - Sanzione: 30.000,00 €

Istituto Nazionale di Fisic
RESPONSABILE PROTEZIONE
dpo@infn.it

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Conseguenze delle violazioni

In prestito da E.Bovo



Ma cosa si può fare per evitare i data breach?

Concetto di RISCHIO

Non completamente annullabile ma… governabile ad esempio con un altro strumento di cui ci parle il GDPR: la DPIA

Data Protection Impact Assessment

DPIA

Un trattamento di dati personali in cui oltre alla descrizione si effettua una valutazione della necessità di quel trattamento, della proporzionalità e dei rischi, con in mente l'idea di predisporre misure idonee ad affrontarli.

Aiuta il titolare a rispettare le norme GDPR e a dimostrare che sono state messe in pratica misure appropriate per garantirne il rispetto.

Si realizza quando il trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Da fare prima che inizi il trattamento e da mantenere aggiornata!

La si può evitare…

Se il trattamento non presenta rischio elevato per i diritti e le libertà delle persone fisiche.

Se il trattamento è molto simile ad un altro per cui è già stata fatta una DPIA.

Se il trattamento fa riferimento a norme o regolamenti per la cui definizione è stata condotta una DPIA.

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Trattamenti da sottoporre a DPIA

In prestito da R. Cecchini

- Sorveglianza di una zona accessibile al pubblico.
- ✓ Uso di tecnologie innovative (p.e. IoT, AI).
- ✓ Trattamenti di dati particolari o giudiziari.
- ✓ Trattamenti sistematici [larga scala] di dati biometrici o genetici.
- ✓ Trasferimenti di dati verso paesi terzi.
- ✓ Impiego di servizi cloud da parte della PA.

In prestito da R. Cecchini

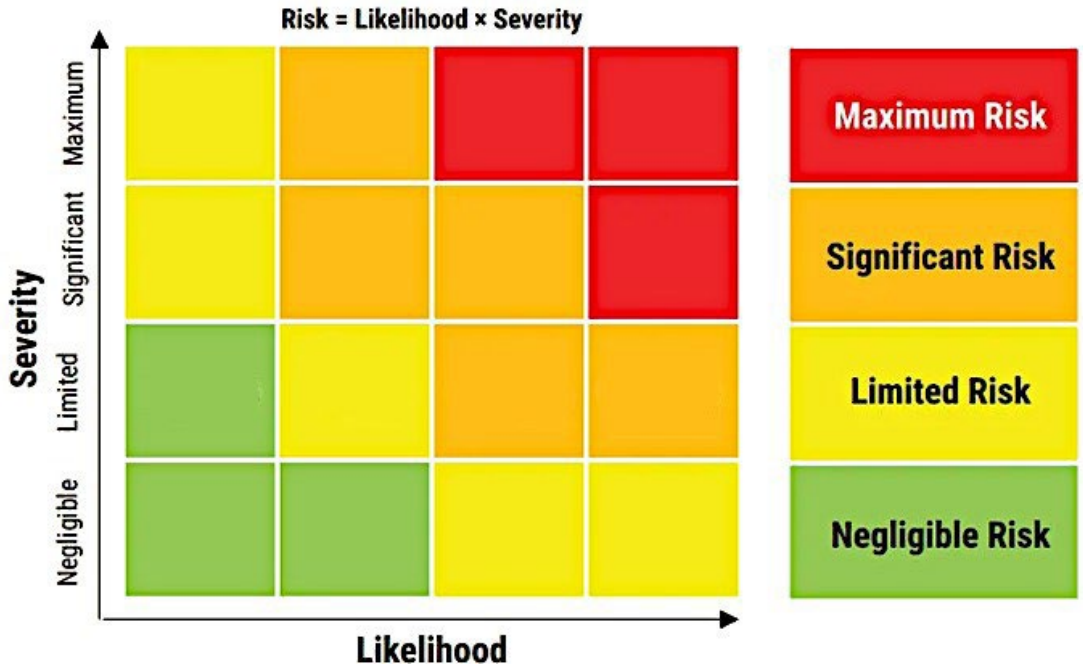
LA DPIA

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Rischio

In prestito da R. Cecchini

Il rischio è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità **per i diritti e le libertà delle persone**.



Esempi di rischi

- Perdita di apparecchiature elettroniche.
- Dati resi anonimi in modo non corretto.
- Dati utilizzati in modi non previsti a causa dell'evoluzione del progetto.
- Dati utilizzati in modi diversi da quanto spiegato ai soggetti.
- Dati trattenuti più del necessario.
- Dati in eccesso rispetto alle necessità.
- Dati trasferiti in paesi senza garanzie adeguate.

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Valutazione

In prestito da R. Cecchini

La valutazione deve riguardare non solo la **sicurezza** del trattamento (la triade D, I & R), ma anche gli **effetti complessivi** del trattamento.

Il rischio si riferisce al soggetto interessato, NON al titolare!

Conoscere i trattamenti…

E sapere quali sono quelli più standard e quelli più pericolosi….

Registro dei Trattamenti

RATP

(Registro Attività di Trattamento dati Personali)

Applicazione in fase avanzata di realizzazione da parte del Sistema Informativo

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Registro dei trattamenti dati personali

GDPR: ai fini dell'accountability

E' un obbligo del titolare che il DPO supporta in fase di realizzazione

DPO successivamente lo usa nelle attività di monitoraggio

In cosa consiste?

Chi lo deve «fare»?

- Servizi che tipicamente trattano dati personali (Direzione/Personale, Amministrazione, Radioprotezione, RSPP, Calcolo e Reti)
- Progetti (Horizon EU, PON, POR, TT, terza missione)

Il Registro per l' INFN

- **Una breve storia**
  - **Registro di trattamenti AC con schede in formato word conservate e indicizzate su Alfresco**
- **Deve essere una fotografia sempre aggiornata: per questo occorre uno strumento informatico**
- **Collaborazione con DSI**
  - **Realizzazione di un mockup, di una prima versione e di alcuni aggiornamenti. Lavori in corso…**

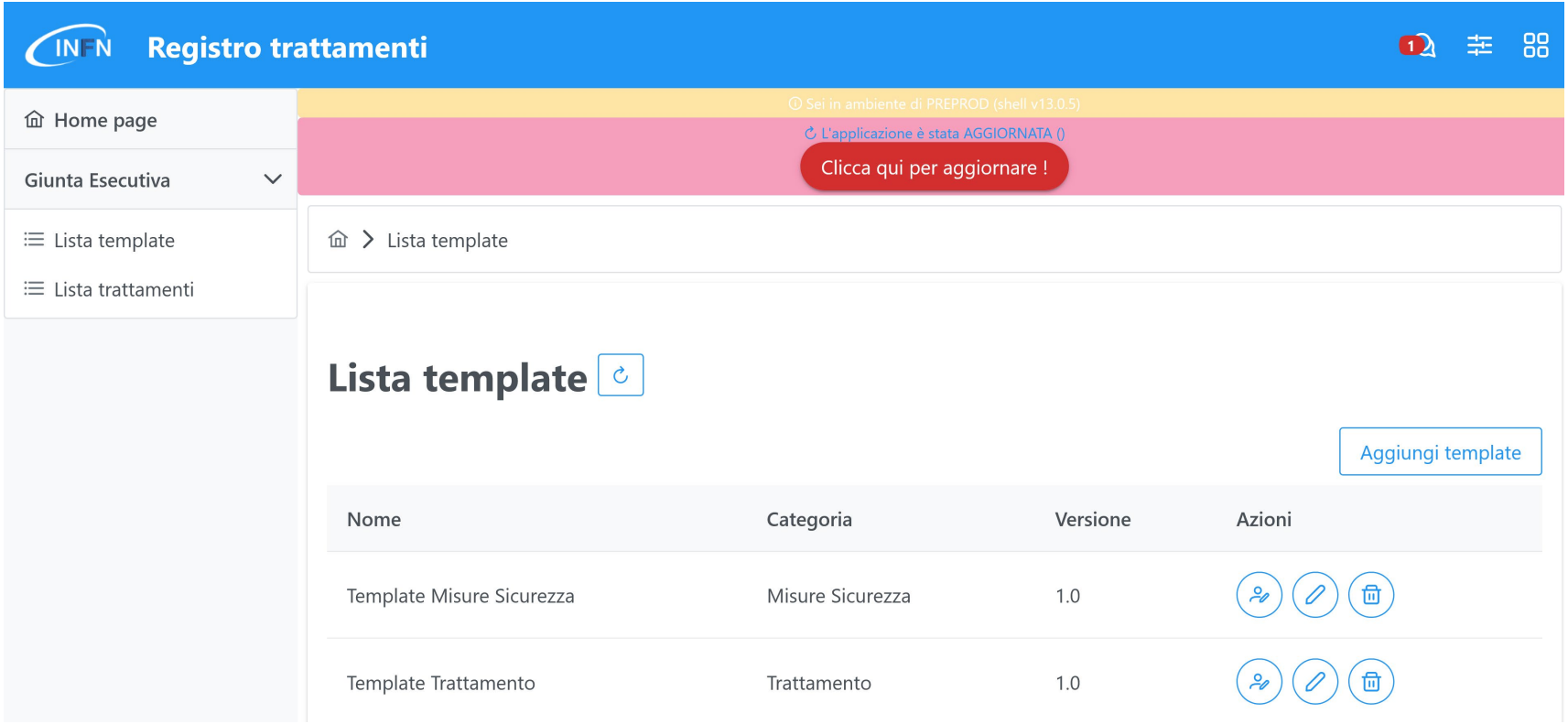
Ma cosa va scritto nel Registro?

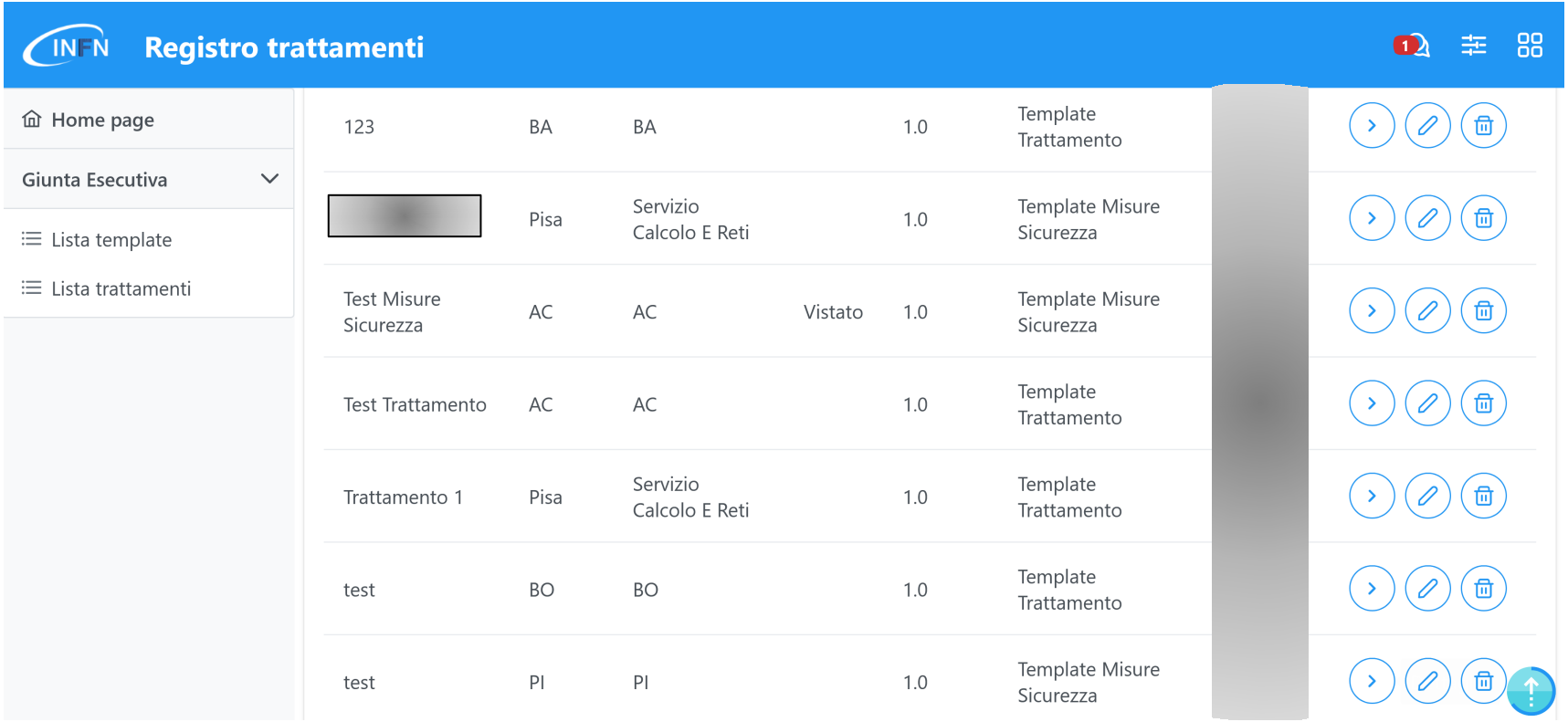
Più difficile a raccontarsi che a farsi

- **L'obbligo legale è la base giuridica a fondamento della quasi totalità dei nostri trattamenti perché tipicamente agiamo seguendo specifiche normative**
  - **Realizzare un elenco delle attività tipiche di un ufficio,**
  - **Identificare le attività che riguardano il trattamento di dati personali (dati anagrafici fondamentalmente)**

    &
  - **Raggruppare le famiglie simili di queste attività**

    (per evitare eccessive frammentazioni)


Registro trattamenti
1
Home page
Giunta Esecutiva
Lista template
Lista trattamenti
Sei in ambiente di PREPROD (shell v13.0.5)
L'applicazione è stata AGGIORNATA ()
Clicca qui per aggiornare !
Lista template
Lista template
Aggiungi template
Nome
Categoria
Versione
Azioni
Template Misure Sicurezza
Misure Sicurezza
1.0
Template Trattamento
Trattamento
1.0


Registro trattamenti
1
Home page
Giunta Esecutiva
Lista template
Lista trattamenti
123 BA BA 1.0 Template Trattamento
Pisa Servizio Calcolo E Reti 1.0 Template Misure Sicurezza
Test Misure Sicurezza AC AC Vistato 1.0 Template Misure Sicurezza
Test Trattamento AC AC 1.0 Template Trattamento
Trattamento 1 Pisa Servizio Calcolo E Reti 1.0 Template Trattamento
test BO BO 1.0 Template Trattamento
test PI PI 1.0 Template Misure Sicurezza

E come facciamo a ricordare cosa si deve fare per essere GDPR compliant, rispettare la privacy, proteggere i dati personali?

4 Documenti da tenere presenti

- Disciplinare uso risorse informatiche
- Misure Minime
- Norme privacy
  - per l'uso dei sistemi informatici destinati al trattamento di dati personali
  - per il trattamento di dati personali

Pochi documenti, ma importanti

Disciplinare uso risorse informatiche (a)

Delibera CD 15442 - 28/2/2020 *(anche CORSO SICUREZZA)*

L'INFN si dota di un DISCIPLINARE per:

«Salvaguardare la sicurezza del proprio sistema informatico e tutelare la riservatezza, l'integrità e la disponibilità delle informazioni e dei dati, anche personali, da questo prodotti, raccolti o comunque trattati.»

Nel disciplinare vengono date indicazioni all'AMMINISTRATORE DI SISTEMA

Chi è l'amministratore di sistema?

figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati, anche personali, compresi i sistemi di gestione delle basi di dati, le reti locali e gli apparati di sicurezza

Disciplinare uso risorse informatiche (b)

1. mantenere i sistemi al livello di sicurezza appropriato al loro uso;

2. verificare con regolarità l'integrità dei sistemi;

3. controllare e conservare i log di sistema per il tempo necessario a verificare la conservazione degli standard di sicurezza;

4. segnalare immediatamente al Servizio di Calcolo e Reti incidenti, sospetti abusi e violazioni della sicurezza e partecipare alla loro gestione;

5. installare e mantenere aggiornati programmi antivirus per i sistemi operativi che lo prevedono;

6. non visionare i dati personali e della corrispondenza di cui dovessero venire a conoscenza e comunque a considerarli strettamente riservati e a non riferire, né duplicare o cedere a persone non autorizzate informazioni sull'esistenza o sul contenuto degli stessi;

7. in caso di interventi di manutenzione, impedire, per quanto possibile, l'accesso alle informazioni e ai dati personali presenti nei sistemi amministrati;

8. seguire attività formative in materie tecnico-gestionali e di sicurezza delle reti, nonché in tema di protezione dei dati personali e di segretezza della corrispondenza.

Disciplinare uso risorse informatiche (c)

Al fine di assicurare la funzionalità, disponibilità, ottimizzazione, sicurezza ed integrità dei sistemi informativi e prevenire utilizzazioni indebite, l'INFN adotta misure che consentono la verifica di comportamenti anomali o delle condotte non previste dal presente Disciplinare nel rispetto dei principi generali di necessità, pertinenza e non eccedenza sopra richiamati. A tal fine il Servizio di Calcolo e Reti può eseguire elaborazioni sui dati registrati dirette ad evidenziare anomalie nel traffico di rete o condotte non consentite dal presente Disciplinare.

MISURE MINIME(a)

il documento che definisce le

Misure minime di sicurezza ICT per le pubbliche amministrazioni

https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict

(Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015) pubblicata sulla GU del 5-5-2017

"Modulo di implementazione delle misure minime di sicurezza nell'Istituto Nazionale di Fisica Nucleare" Documento in data certa depositato dalla Presidenza il 20/12/2017 (modulo_implementazione_mm_v4.pdf)

Note redatte in ambito CCR: Implementazione Misure Minime.pdf

MISURE MINIME(b)

Le misure minime in parte sono già previste nel disciplinare, ma sono più dettagliate negli aspetti tecnici.

Misure: MINIME, STANDARD, ADVANCED

Non solo un obbligo, ma una guida.

MISURE MINIME(c)

Una lettura ragionata del Modulo di Implementazione delle Misure Minime: un framewok di security per gli amministratori di sistema (seguono alcune slide con le misure da implementare)

ABSC: Agid Basic Security Control(s) ispirati a:

CSC: Critical Security Control(s) for Effective Cyber Defense, pubblicati da:

CIS, Center for Internet Security e originariamente noti come SANS 20

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	
1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositi almeno l'indirizzo IP.	
1	4	2	S	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	
1	4	3	A	Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione.	
1	5	1	A	Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati.	
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	

MM 1

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
2	1	1	M	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.	
2	2	1	S	Implementare una "whitelist" delle applicazioni autorizzate, bloccando l'esecuzione del software non incluso nella lista. La "whitelist" può essere molto ampia per includere i software più diffusi.	
2	2	2	S	Per sistemi con funzioni specifiche (che richiedono solo un piccolo numero di programmi per funzionare), la "whitelist" può essere più mirata. Quando si proteggono i sistemi con software personalizzati che può essere difficile inserire nella "whitelist", ricorrere al punto ABSC 2.4.1 (isolando il software personalizzato in un sistema operativo virtuale).	
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	
2	3	2	S	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.	
2	3	3	A	Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch.	
2	4	1	A	Utilizzare macchine virtuali e/o sistemi air-gapped per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete.	

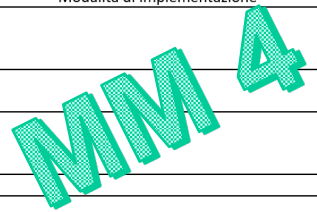
MM 2

ABSC_ID			Livello	Descrizione	Modalità di implementazione
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	
3	1	2	S	Le configurazioni sicure standard devono corrispondere alle versioni "hardened" del sistema operativo e delle applicazioni installate. La procedura di hardening comprende tipicamente: eliminazione degli account non necessari (compresi gli account di servizio), disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate.	
3	1	3	A	Assicurare con regolarità la validazione e l'aggiornamento delle immagini d'installazione nella loro configurazione di sicurezza anche in considerazione delle più recenti vulnerabilità e vettori di attacco.	
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	
3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	
3	4	1	M	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	
3	5	1	S	Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.	
3	5	2	A	Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento automatico, per qualunque alterazione di tali file deve essere generato un alert.	
3	5	3	A	Per il supporto alle analisi, il sistema di segnalazione deve essere in grado di mostrare la cronologia dei cambiamenti della configurazione nel tempo e identificare chi ha eseguito ciascuna modifica.	
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	
3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	

MM 3

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

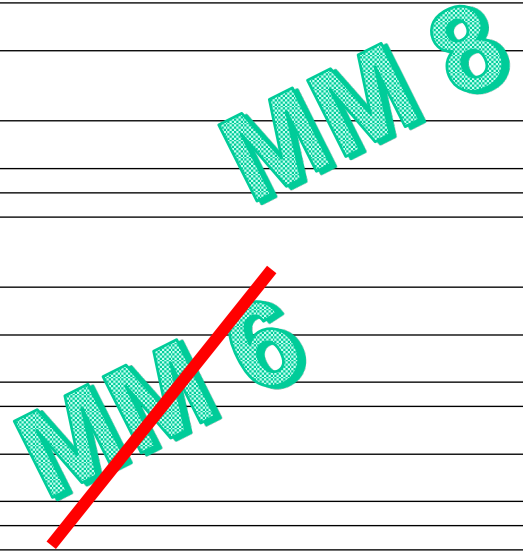
ABSC_ID			Livello	Descrizione	Modalità di implementazione
4	1	1	M	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	
4	1	3	A	Usare uno SCAP (Security Content Automation Protocol) di validazione della vulnerabilità che rilevi sia le vulnerabilità basate sul codice (come quelle descritte dalle voci Common Vulnerabilities ed Exposures) che quelle basate sulla configurazione (come elencate nel Common Configuration Enumeration Project).	
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	
4	3	1	S	Eseguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto, utilizzando un account dedicato che non deve essere usato per nessun'altra attività di amministrazione.	
4	3	2	S	Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.	
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	
4	4	2	S	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione	
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	
4	5	2	M	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	
4	6	1	S	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.	
4	7	1	M	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.	
4	7	2	S	Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio.	
4	8	1	M	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).	
4	8	2	M	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.	
4	9	1	S	Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione.	
4	10	1	S	Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.	



ABSC_ID			Livello	Descrizione	Modalità di implementazione
5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	
5	6	1	A	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.	
5	7	1	M	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	
5	8	1	S	Non consentire l'accesso diretto ai sistemi con le utenze amministrative, obbligando gli amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi.	
5	9	1	S	Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.	
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	
5	10	3	M	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	
5	10	4	S	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
8	1	1	M	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	
8	2	1	S	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.	
8	2	2	S	È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi anti-malware installati su ciascun dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale.	
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	
8	4	1	S	Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.	
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	
8	5	1	S	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	
8	9	1	M	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	
8	9	2	M	Filtrare il contenuto del traffico web.	
8	9	3	M	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).	
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	
8	11	1	S	Implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate.	



ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione	Modalità di implementazione
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	
10	1	2	A	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.	
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	
10	3	1	M	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.	
10	4	1	M	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	

MM 10

ABSC_ID			Livello	Descrizione	Modalità di implementazione
13	1	1	M	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica	
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	
13	3	1	A	Utilizzare sul perimetro della rete strumenti automatici per bloccare, limitare ovvero monitorare in maniera puntuale, sul traffico uscente dalla propria rete, l'impiego di crittografia non autorizzata o l'accesso a siti che consentano lo scambio e la potenziale esfiltrazione di informazioni.	
13	4	1	A	Effettuare periodiche scansioni, attraverso sistemi automatizzati, in grado di rilevare sui server la presenza di specifici "data pattern", significativi per l'Amministrazione, al fine di evidenziare l'esistenza di dati rilevanti in chiaro.	
13	5	1	A	Nel caso in cui non sia strettamente necessario l'utilizzo di dispositivi esterni, implementare sistemi/configurazioni che impediscano la scrittura di dati su tali supporti.	
13	5	2	A	Utilizzare strumenti software centralizzati atti a gestire il collegamento alle workstation/server dei soli dispositivi esterni autorizzati (in base a numero seriale o altre proprietà univoche) cifrando i relativi dati. Mantenere una lista aggiornata di tali dispositivi.	
13	6	1	A	Implementare strumenti DLP (Data Loss Prevention) di rete per monitorare e controllare i flussi di dati all'interno della rete in maniera da evidenziare eventuali anomalie.	
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	
13	9	1	A	Assicurare che la copia di un file fatta in modo autorizzato mantenga le limitazioni di accesso della sorgente, ad esempio attraverso sistemi che implementino le regole di controllo degli accessi (e.g. Access Control List) anche quando i dati sono trasferiti al di fuori del loro repository.	

MM 13

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Norme privacy (a)

GDPR (Regolamento 2016/679) chiede: **misure adeguate** a proteggere i dati

INFN sceglie di considerare «adeguate» le Misure Minime,

da accrescere, se necessario.

1 delibera CD e 2 documenti da non dimenticare:

Delibera *n. 14844 del 27 Luglio 2018* : Figure e ruoli legati alla privacy

Documento1: Norme per l'uso dei sistemi informatici destinati al trattamento di dati personali nell'INFN (allegato alla delibera)

Documento 2: Norme per il trattamento di dati personali nell'INFN (*dicembre 2018*)

PRIVACY

Norme privacy (b)

Norme per l'uso dei sistemi informatici destinati al trattamento di dati personali nell'INFN (allegato alla delibera)

Indicazioni e approfondimenti sull'applicazione misure minime:

sistemi LINUX

sistemi MAC-OS

Sistemi WINDOWS

PRIVACY

L'attuazione delle presenti norme dovrà pertanto essere valutata in ciascuna Struttura ed eventualmente adattata alle particolari situazioni locali, *documentando con chiarezza* il motivo delle scelte fatte.

Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it

Norme privacy (c)

Norme per il trattamento di dati personali nell'INFN

Una raccolta dei principali aspetti normativi

Individuazione delle figure rilevanti in ambito privacy INFN

Indicazioni anche pratiche per il trattamento di dati sia in forma cartacea che elettronica

Una guida che aiuti tutti gli autorizzati al trattamento

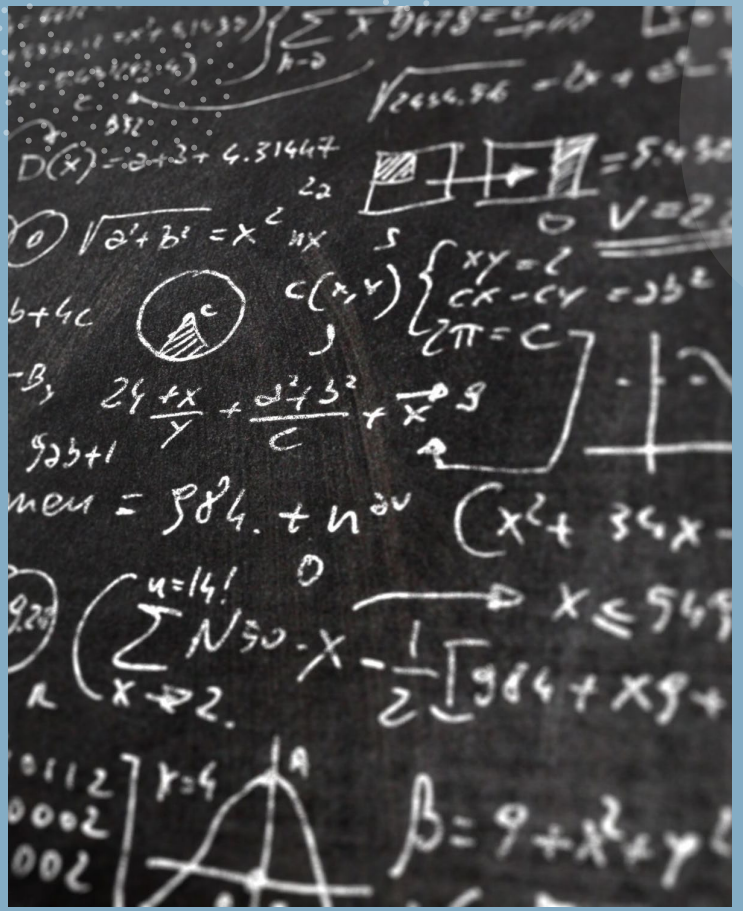
PRIVACY

Collocare la privacy nel giusto contesto…

Consapevolezza & attenzione

Referenti locali privacy & DPO

cultura della privacy!



Istituto Nazionale di Fisica Nucleare
RESPONSABILE PROTEZIONE DATI
dpo@infn.it