Aggiornamenti sulla protezione dei dati

Norme per il trattamento di dati personali nell'INFN

Normativa di riferimento

Norme relative alla sicurezza informatica e al trattamento dei dati personali in ordine cronologico

- Disciplinare per l'uso delle risorse informatiche nell'INFN 10/3/2016 (link)
- Regolamento (UE) - GDPR 2016/679 (link) in vigore 28/5/18
- Circolare Agid Misure Minime di sicurezza informatica per le PA 18/4/2017 (link) in vigore 31/12/2017
- *D.Lgs. 196/2003* (Codice Privacy) integrato con le modifiche del *D.Lgs. 101/2018* (*link*)
- *Deliberazione INFN n. 14844 del 27 Luglio 2018* (link)
- *Norme per l'uso dei sistemi informatici destinati al trattamento di dati personali* (*link*)
- Norme per il trattamento dei dati personali nell'INFN 4/12/18 (link)

GDPR-FAQ

GDPR Regolamento a «tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati»

Perché?

Un regolamento che regola i diritti di tutti i cittadini residenti nell'UE riguardo al trattamento dei loro dati personali

Dove?

Ovunque. Sia per le organizzazioni con sede nell'UE che per tutte le organizzazioni straniere che elaborano i dati dei residenti nell'UE

Chi?

Chiunque tratti dati personali di cittadini UE

Come?

Facendo tutto il possibile per processare in modo sicuro i dati personali (By design e By default) implementando appropriati approcci tecnici ed organizzativi

https://www.garanteprivacy.it/documents/10160/0/Regolamento+UE+2016+679.+Una+sintesi+per+aziende+ed+enti

GDPR-Garante

https://dpo.infn.it/wp-content/uploads/2018/12/Norme_Trattamento_Dati_Personali_INFN.pdf

GDPR Definizioni

- **Dato Personale**: qualsiasi informazione riguardante una persona fisica («interessato») identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
- **Categorie particolari di dati personali**: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

https://dpo.infn.it/wp-content/uploads/2018/12/Norme_Trattamento_Dati_Personali_INFN.pdf

GDPR Definizioni

- **Dati relativi a condanne penali e reati**: dati relativi a vicende riguardanti persone fisiche disciplinate dalla legislazione penale, nonché la comminatoria di misure di sicurezza.
- **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, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

https://dpo.infn.it/wp-content/uploads/2018/12/Norme_Trattamento_Dati_Personali_INFN.pdf

GDPR Soggetti

I soggetti rilevanti nella disciplina in materia di trattamento dei dati personali sono:

- il Titolare
  - INFN e sue articolazioni descritte nelle Norme per il trattamento
- il Responsabile per la protezione dei dati personali,
  - DPO ufficio appositamente creato
- i Responsabili del trattamento (eventuali),
  - Eventuali soggetti esterni che trattano dati personali dei quali INFN e' titolare
- gli Autorizzati al trattamento
  - Sono tutti coloro che agiscono sotto l'autorità del Titolare e che hanno accesso ai dati personali
- gli Interessati al trattamento
  - Sono coloro cui si riferiscono i dati personali trattati

https://dpo.infn.it/wp-content/uploads/2018/12/Norme_Trattamento_Dati_Personali_INFN.pdf

GDPR Principi generali

Il trattamento di dati personali deve essere effettuato nel rispetto dei principi di:

- *liceità*, *correttezza* e *trasparenza*;
- *limitazione della finalità del trattamento*, assicurando che eventuali trattamenti successivi non siano incompatibili con le finalità per le quali i dati sono stati raccolti;
- *minimizzazione dei dati*, prestando cura che i dati siano adeguati, pertinenti e limitati a quanto necessario per raggiungere le finalità del trattamento;
- *esattezza e aggiornamento dei dati*, compresa la tempestiva cancellazione di quelli che risultino inesatti rispetto alle finalità del trattamento;
- *limitazione della conservazione*, limitando la conservazione dei dati a un periodo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
- *integrità e riservatezza*, qarantendo un'adeguata sicurezza dei dati personali oggetto del trattamento;

https://dpo.infn.it/we-content/uploads/2018/12/LNF_181128_Ronconi.pdf

GDPR Liceita'

- Liceità del trattamento dati personali (per le PA)
  - OBBLIGHI DI LEGGE
  - OBBLIGHI DI CONTRATTO
  - CONSENSO
  - COMPITI DI INTERESSE PUBBLICO O ESERCIZIO DI PUBBLICO POTERE
- Liceità del trattamento dati personali particolari (per le PA)
  - CONSENSO ESPLICITO PER FINALITA' DETERMINATE
  - ESERCIZIO DI OBBLIGHI E DIRITTI IN MATERIA DI : LAVORO, SICUREZZA E PROTEZIONE SOCIALE, MEDICINA DEL LAVORO

https://dpo.infn.it/wp-content/uploads/2018/12/Norme_Trattamento_Dati_Personali_INFN.pdf

GDPR Informativa

- Per adempiere agli obblighi di informazione sul trattamento di cui all'art. 13 del Regolamento, devono essere utilizzati gli schemi di informative disponibili al sito web del DPO dell'INFN
- È necessario pertanto aver cura che all'avvio di ogni procedimento amministrativo o di qualunque altra attività che coinvolga il trattamento di dati personali sia fornita agli interessati, per iscritto e preferibilmente in formato elettronico, l'informazione preventiva circa:
  - il Titolare del trattamento ed i relativi dati di contatto,
  - i dati di contatto del Responsabile della Protezione dei dati,
  - le finalità e modalità del trattamento,
  - i legittimi interessi perseguiti dal Titolare,
  - gli eventuali destinatari dei dati,
  - l'eventuale trasferimento dei dati in un paese terzo o un'organizzazione internazionale,
  - la natura obbligatoria o facoltativa del conferimento dei dati, con indica zione delle conseguenze di un eventuale rifiuto del conferimento stesso,
  - il periodo di conservazione dei dati,
  - il diritto di chiedere al Titolare l'accesso, la rettifica, o la cancellazione dei dati o la limitazione del trattamento, oltre il diritto di opporsi al loro trattamento,
  - l'esistenza eventuale di processi decisionali automatizzati o di proflazione,
  - il diritto di presentare un reclamo al Garante per la tutela dei dati personali.

https://dpo.infn.it/wp-content/uploads/2019/01/Informativa_generale_INFN_181204.pdf

https://dpo.infn.it/we-content/uploads/2018/12/LNF_181128_Ronconi.pdf

GDPR Consenso

Nel caso tra i requisiti di liceità sia necessario acquisire il consenso esso deve possedere le seguenti caratteristiche

- INFORMATO (preceduto da un'informativa)
- LIBERO (senza condizionamenti o vincoli)
- SPECIFICO (riferito ad ogni finalità)
- INEQUIVOCABILE (certezza che sia stato prestato)
- ESPRESSO (non tacito o passivo)

https://dpo.infn.it/wp-content/uploads/2018/10/Privacy_policy_web_INFN.pdf

https://dpo.infn.it/wp-content/uploads/2019/01/Modello_informativa_eventi_181204-1.pdf

https://dpo.infn.it/wp-content/uploads/2018/12/Norme_Trattamento_Dati_Personali_INFN.pdf

GDPR Diffusione e comunicazione

- La comunicazione dei dati personali ad un altro soggetto pubblico può essere effettuata quando è prevista da una norma di legge o di regolamento o, in mancanza, se necessaria per lo svolgimento di compiti di interesse pubblico o di funzioni istituzionali, decorsi quarantacinque giorni dalla relativa comunicazione al Garante senza che lo stesso abbia adottato una diversa determinazione delle misure da adottarsi a garanzia degli interessati.
- L'art. 100 del Codice consente alle università e gli enti di ricerca, al fine di promuovere e sostenere la ricerca e la collaborazione in campo scientifico e tecnologico, di adottare autonome determinazioni con le quali disporre la comunicazione o diffusione, anche a privati e per via telematica, di dati relativi ad attività di studio e di ricerca, a laureati, dottori di ricerca, tecnici, tecnologi, ricercatori, docenti, esperti e studiosi, con esclusione di quelli di cui agli articoli 9 e 10 del Regolamento *(dati personali particolari e dati giudiziari)*

https://dpo.infn.it/wp-content/uploads/2019/01/Violazione_dati_personali_181204.pdf

GDPR
Data Breach

- l Regolamento definisce violazione dei dati personali la 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 (art. 4, punto 12)
- Il Gruppo di lavoro europeo sulla protezione dei dati personali – Working Party art. 29 o WP29 ha individuato tre categorie di violazioni:
  - violazione della confidenzialità del dato: nel caso in cui vi sia una divulgazione o un accesso ai dati personali, accidentale o non autorizzata;
  - violazione dell'integrità del dato: in caso di alterazione accidentale o non autorizzata di dati personali;
  - violazione della disponibilità del dato: nel caso di perdita di accesso o distruzione di dati, accidentale o non autorizzata.
- A seconda delle circostanze, una violazione può riguardare singolarmente o contemporaneamente la confidenzialità, l'integrità o la disponibilità di dati o combinazioni di esse.

https://dpo.infn.it/wp-content/uploads/2019/01/Violazione_dati_personali_181204.pdf

GDPR
Data Breach

- Il Regolamento dispone all'art. 33 che le violazioni dei dati personali debbano essere notificate dal Titolare del trattamento al Garante entro 72 ore dal momento in cui ne sia venuto a conoscenza, a meno che risulti improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche.
- In attuazione di quanto disposto dalla deliberazione del Consiglio Direttivo INFN n. 14844 del 27 luglio 2018, il compito di provvedere alla notifica della violazione è attribuito ai Direttori delle Strutture, nonché ai Direttori delle articolazioni dell'Amministrazione Centrale ed ai Responsabili del Servizio di Presidenza e dell'Ufficio Comunicazione dell'INFN

https://dpo.infn.it/wp-content/uploads/2019/01/Modello_notifica_data_breach_181204.pdf

https://dpo.infn.it/wp-content/uploads/2019/01/Violazione_dati_personali_181204.pdf

GDPR
Data Breach

- Il Regolamento all'art. 34 dispone che "Quando la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento comunica la violazione all'interessato senza giustificato ritardo"
- .È sempre dovuta la notificazione al Garante della violazione dei dati personali se dalla violazione possa derivare un rischio per i diritti e le libertà delle persone; quando tale rischio sia qualificabile come elevato, la violazione deve essere comunicata anche agli interessati (cioè ai soggetti a cui i dati si riferiscono)

https://dpo.infn.it/wp-content/uploads/2019/01/Modello_comunicazione_data_breach_181204.pdf


GDPR
DON'T
PANIC


GDPR
SAFET
MANU
SECURITY

https://dpo.infn.it/wp-content/uploads/2018/10/Deliberazione_CD_14844.pdf

GDPR Adempimenti del Titolare

- a) **designano le persone autorizzate al trattamento dei dati personali nell'ambito della articolazione che dirigono**; garantiscono che le stesse siano state **preliminarmente istruite** per il trattamento e si siano impegnate alla riservatezza; **verificano l'osservanza delle istruzioni** che sono state impartite per il trattamento, e, ove ne sussistano le condizioni, l'osservanza di obblighi legali di riservatezza;
- b) **assicurano che l'informativa sul trattamento dei dati sia fornita all'interessato e, nei casi previsti, ne acquisiscono il consenso**;
- c) danno seguito alle eventuali richieste degli interessati per l'esercizio dei diritti loro garantiti dal Capo IV del Regolamento;
- d) **implementano il Registro del trattamento dei dati personali**, comunicando al DPO i nuovi trattamenti in uso presso la Struttura o l'articolazione che dirigono o di cui hanno la responsabilità
- e) **notificano al Garante** della protezione dei dati personali **le violazioni dei dati personali (data breach)**; provvedono alla comunicazione della violazione agli interessati, ai sensi degli articoli 33 e 34 del Regolamento, e ne danno informativa al Direttore Generale e al DPO;

https://dpo.infn.it/wp-content/uploads/2018/10/Deliberazione_CD_14844.pdf

GDPR Adempimenti del Titolare

- f) **effettuano**, quando sia necessaria e sentito il DPO, una **valutazione dell'impatto dei trattamenti** previsti sulla protezione dei dati personali;
- g) mettono a disposizione tutte le informazioni necessarie per dimostrare il rispetto degli obblighi richiesti dal Regolamento; consentono e contribuiscono alle attività di revisione e di ispezione;
- h) informano immediatamente il Direttore Generale e il DPO in ogni circostanza in cui ritengono che un'istruzione relativa al trattamento dei dati violi il Regolamento o altre disposizioni relative alla protezione dei dati;
- i) **designano quali Responsabili esterni al trattamento** i soggetti che trattano dati personali per conto dell'INFN nell'ambito di convenzioni o contratti che hanno potere a sottoscrivere, nell'ambito delle competenze per valore e materia previste dagli atti interni dell'INFN;
- j) **individuano un referente locale** quale punto di contatto con il DPO e supporto alle attività di gestione degli adempimenti connessi alla protezione dei dati.

https://dpo.infn.it/wp-content/uploads/2018/12/Norme_Trattamento_Dati_Personali_INFN.pdf

GDPR Adempimenti dei soggetti autorizzati

I soggetti autorizzati al trattamento devono:

- predisporre la modulistica per la raccolta dei dati personali avendo cura di chiedere agli interessati soltanto i dati necessari e pertinenti alla finalità per le quali sono raccolti;
- accertarsi che la raccolta dei dati personali sia giustificata da una effettiva base giuridica o comunque sia necessaria per eseguire compiti di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è titolare l'INFN;
- nel caso in cui il dato che si intende raccogliere non sia giustificato da una effettiva base giuridica o non sia strettamente necessario per il raggiungimento di compiti di interesse pubblico, far sottoscrivere all'interessato una dichiarazione di consenso al trattamento;
- fornire agli interessati l'informativa sul trattamento in tutte le circostanze in cui procedono alla raccolta di dati personali;
- verificare l'esattezza della scritturazione o digitazione dei dati nelle operazioni di registrazione dei dati personali raccolti;
- utilizzare i dati personali in base al principio del "need to know" ed evitare di condividerli o comunicarli a persone che non ne hanno bisogno per lo svolgimento delle proprie mansioni lavorative;

https://dpo.infn.it/wp-content/uploads/2018/12/Norme_Trattamento_Dati_Personali_INFN.pdf

GDPR Adempimenti dei soggetti autorizzati

- non trasmettere all'esterno o a soggetti terzi informazioni circa i dati personali conosciuti in ragione della propria attività, salvo che si tratti di comunicazione funzionale allo svolgimento dei propri compiti;
- conservare la riservatezza dei dati personali conosciuti nello svolgimento dell'attività lavorativa anche successivamente al trasferimento ad altra attività o nel periodo successivo alla cessazione del rapporto di lavoro;
- accertarsi dell'identità dell'interessato al momento della raccolta dei dati o prima di fornire informazioni circa i dati personali di altri interessati, anche ove la richiesta sia presentata nell'esercizio del diritto di accesso;
- nei casi in cui è ammessa la consultazione di dati personali e in particolare nei procedimenti di accesso a dati personali, verificare che i documenti oggetto di accesso non riportino dati particolari o dati relativi a condanne penali: in tal caso procedere all'oscuramento di tali informazioni (p. es. mediante omissis), salvo che non vi sia una base giuridica che autorizzi la conoscibilità anche di tale tipologia di dati
- aver cura di non rendere conoscibili, neppure accidentalmente, a soggetti non autorizzati i dati personali contenuti in atti o documenti: a tal fine non lasciare in evidenza documenti quando si ricevono soggetti non autorizzati a conoscere tali dati o non lasciare aperto ed incustodito l'ufficio.

https://dpo.infn.it/wp-content/uploads/2018/12/Norme_Trattamento_Dati_Personali_INFN.pdf

GDPR Adempimenti nell' utilizzo di risorse informatiche

UTILIZZO DEI SISTEMI INFORMATICI

Una buona attenzione alle regole elementari di sicurezza fisica è la base su cui poggiano tutte le altre regole. Per tale motivo è necessario osservare il Disciplinare per l'uso delle risorse informatiche dell'INFN ed in particolare aver cura di:

- accedere ai sistemi di gestione documentale informatizzata e alle banche dati contenenti dati personali soltanto attraverso le credenziali di accesso concesse dall'INFN e nei limiti delle abilitazioni operative consentite dall'Istituto;
- non utilizzare servizi cloud per il trattamento dei dati personali se non espressamente autorizzati dall'INFN;
- se si ha il sospetto che si sia verificato un accesso non autorizzato ai dati personali, segnalare immediatamente l'incidente al Direttore di Struttura o, per l'Amministrazione Centrale, al Direttore di Direzione, Divisione o Servizio di appartenenza;

https://dpo.infn.it/wp-content/uploads/2018/12/Norme_Trattamento_Dati_Personali_INFN.pdf

GDPR Adempimenti nell' utilizzo di risorse informatiche

- fare attenzione, nel caso in cui si utilizzino fotocopiatrici, stampanti o fax condivisi a non lasciare incustodito l'apparecchio con il quale vengono stampati, duplicati o ricevuti documenti contenenti dati personali e rimuovere immediatamente i documenti prodotti;
- nel caso in cui la stampante o la fotocopiatrice diano segnali di malfunzionamento provvedere a cancellare i lavori in coda, evitando che, a seguito di interventi di manutenzione, il macchinario proceda incustodito alla stampa di documenti contenenti dati personali;
- chiudere le applicazioni che si stavano usando, o attivare il salvaschermo protetto da password, quando si lascia la postazione di lavoro;
- se si trasferiscono dati personali su dispositivi rimovibili (p.e. chiavetta usb), avere cura di cancellarli al termine delle attività di trattamento

https://dpo.infn.it/wp-content/uploads/2018/12/Norme_Trattamento_Dati_Personali_INFN.pdf

GDPR Adempimenti nell' utilizzo di risorse informatiche

CONFIGURAZIONI DEL SISTEMA

Le impostazioni del sistema fatte dal Servizio Calcolo non devono essere modificate senza un'autorizzazione preventiva. In particolare è necessario aver cura di:

- non permettere l'esecuzione automatica dei contenuti al momento dell'inserimento di un dispositivo rimovibile;
- attivare l'esecuzione delle macro eventualmente presenti nei file Office solo caso per caso, dopo aver verificato la loro indispensabilità;
- non attivare l'apertura automatica dei link esterni e degli allegati nei messaggi di posta elettronica;
- non attivare l'anteprima automatica dei contenuti dei file;
- non disattivare la scansione automatica anti-malware dei dispositivi rimovibili alla connessione

https://dpo.infn.it/wp-content/uploads/2018/12/Norme_Trattamento_Dati_Personali_INFN.pdf

GDPR Adempimenti nell' utilizzo di risorse informatiche

PASSWORD

- La corretta individuazione, custodia e gestione delle password consente all'utente di tutelarsi rispetto ad eventuali attività non corrette o addirittura illecite effettuate da altri soggetti tramite il computer a lui assegnato.
- La password è personale e l'utente è responsabile della corretta conservazione e gestione della stessa. Non deve essere comunicata ad altri né scritta su supporti facilmente accessibili a terzi. Nella sua scelta devono essere evitati riferimenti personali (nome e/o cognome proprio o di familiari, indirizzo ecc…), e preferite sequenze miste di caratteri e numeri.
- I soggetti autorizzati al trattamento dei dati personali devono aver cura, inoltre, di non impiegare la stessa password per i diversi sistemi utilizzati e di non rendere note quelle non più in uso, perché potrebbero permettere l'individuazione delle regole adottate per la loro generazione.

https://dpo.infn.it/wp-content/uploads/2018/12/Norme_Trattamento_Dati_Personali_INFN.pdf

GDPR Adempimenti nell' utilizzo di risorse informatiche

POSTA ELETTRONICA

I soggetti autorizzati al trattamento dei dati personali non devono mai fornire

- dati riservati via e-mail (ad es. password). I messaggi in cui vengono richieste informazioni di questo tipo, ad es. tramite un link ad una pagina, anche apparentemente legittima, sono sicuramente dei tentativi di phishing e vanno immediatamente segnalati al Servizio Calcolo.
- Prima di aprire un link presente in un messaggio di posta elettronica, verificare con attenzione la sua legittimità, controllando ad esempio l'indirizzo visibile con quello che appare, di solito nella parte inferiore della finestra, quando vi si posiziona sopra il cursore.

https://dpo.infn.it/wp-content/uploads/2018/12/Norme_Trattamento_Dati_Personali_INFN.pdf

GDPR Responsabilita' e sanzioni

È riconosciuto il diritto al risarcimento a chiunque subisca un danno materiale o immateriale causato dalla violazione delle norme del Regolamento. Sebbene il risarcimento sia posto a carico del Titolare, questi può esercitare un'azione di rivalsa nei confronti dell'autore del danno, secondo i termini e le modalità previste dalle norme in materia di responsabilità amministrativa.

Nel caso in cui il Titolare dovesse essere assoggettato a sanzioni amministrative è previsto l'accertamento di eventuali responsabilità commesse dal personale autorizzato al trattamento di dati personali.

Per le sanzioni conseguenti a illeciti penali si rinvia all'art. 167 del Codice.

È fatta salva in ogni caso le responsabilità disciplinare eventualmente emergente dalla condotta che ha determinato l'assoggettamento a risarcimento o a sanzione.

https://dpo.infn.it/wp-content/uploads/2018/10/Norme_uso_sistemi_informatici.pdf

Norme d'uso obbligatorie per sistemi informatici destinati al trattamento di dati personali

- Questa documento riporta le norme tecniche e organizzative, relative ai sistemi in uso nell'INFN (Windows, Linux e macOS), ritenute adeguate a garantire la sicurezza dei dati personali trattati, compresa la loro protezione da trattamenti non autorizzati o illeciti e dalla loro perdita, distruzione o danno accidentale, secondo quando indicato nell'Art. 5 del Regolamento UE N. 2016/679 (Regolamento).
- Al fine di proporre norme precise e non ridondanti, utili a tradursi in effettive misure di sicurezza per i sistemi interessati, è stata presa attentamente in esame la recente disciplina AgID: Circolare AgID 18/04/2017, n. 2/2017, GU Serie Generale n.103 del 05/05/2017 (Circolare), di cui si riporta in Appendice la tabella riassuntiva delle misure obbligatorie previste. Allo stato attuale, si ritiene che l'attuazione di quanto richiesto nella Circolare soddisfi, almeno per la gran parte dei casi, quei requisiti di sicurezza che il Regolamento impone.

https://dpo.infn.it/wp-content/uploads/2018/10/Norme_uso_sistemi_informatici.pdf

Norme d'uso obbligatorie per sistemi informatici destinati al trattamento di dati personali

Le «misure minime» rappresentano un framework operativo per l'implementazione di misure che garantiscano un livello minimo di sicurezza al fine di realizzare Disponibilità Integrità e Confidenzialità dei sistemi e dei dati che utilizzano. Si articolano in 8 Capitoli ognuno con specifici paragrafi.

- ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI
- ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI
- ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER
- ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ
- ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE
- ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE
- ABSC 10 (CSC 10): COPIE DI SICUREZZA
- ABSC 13 (CSC 13): PROTEZIONE DEI DATI

https://dpo.infn.it/wp-content/uploads/2018/10/Norme_uso_sistemi_informatici.pdf

Norme d'uso obbligatorie per sistemi informatici destinati al trattamento di dati personali

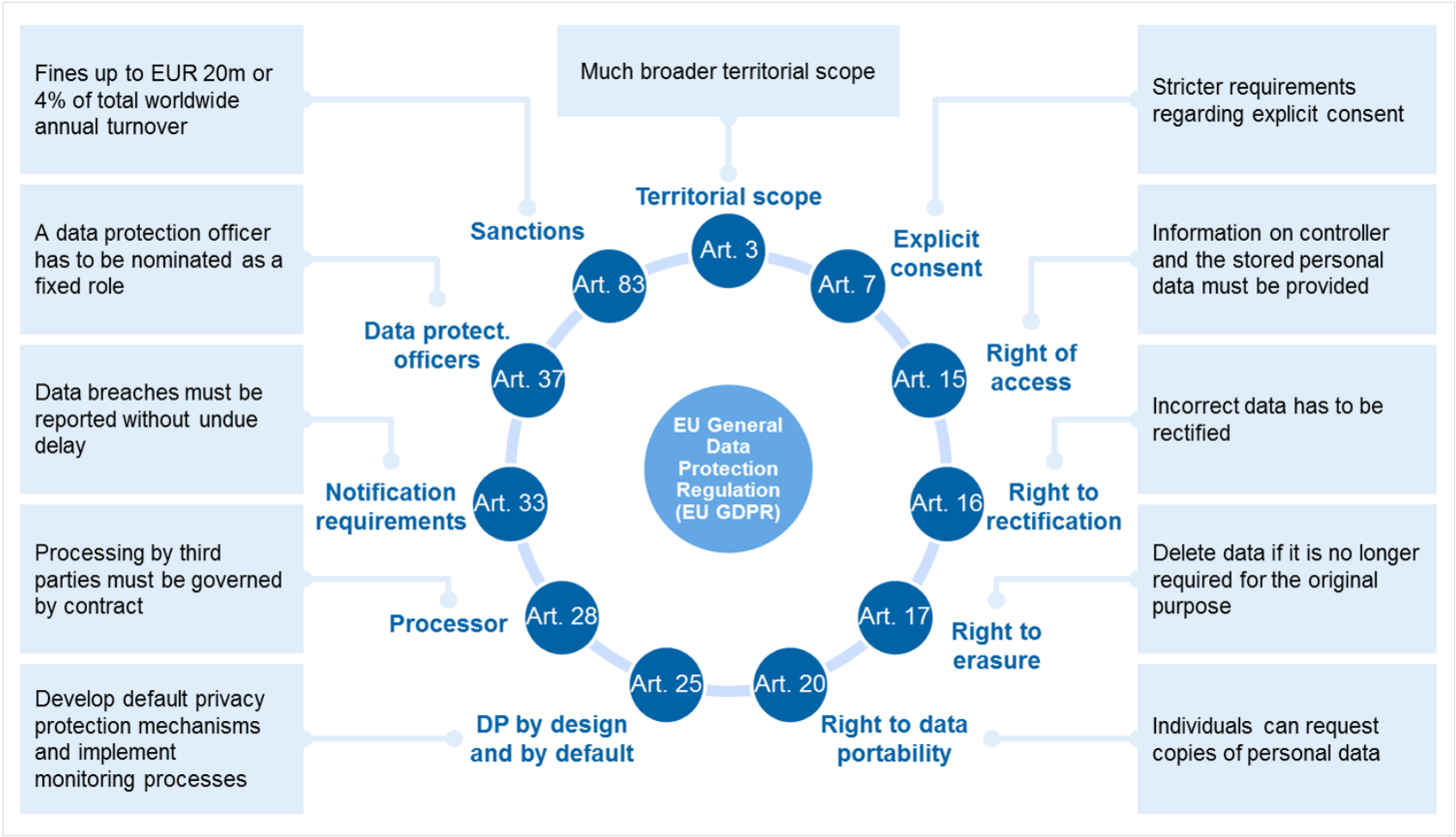
Gli amministratori di sistema di dispositivi che operano trattamento di dati personali DEVONO seguire la guida operativa che deriva dall'implementazione delle misure minime per i sistemi operativi in uso presso INFN e accettarla per presa visione

Contengono implementazioni obbligatorie e suggerimenti facoltativi ma vivamente consigliati

Entrano nel dettaglio implementativo e richiedono un livello medio di conoscenza sistemistica

Il Servizio di Calcolo e Reti è a disposizione per eventuali chiarimenti e disponibile ad eventuali suggerimenti in relazione agli argomenti trattati che possono essere riferiti ai competenti organi (DPO,CCR) per eventuali revisioni

Ci piacerebbe avere un riassunto conciso per sapere cosa fare ma… non si trova facilmente



Questo e' il massimo che sono riuscito a trovare

LINK

Link

- https://dpo.infn.it/wp-content/uploads/2018/10/Regolamento_UE_2016_679_Arricchito_e_Aggiornato_Gazzetta_23_Maggio.pdf
- https://dpo.infn.it/wp-content/uploads/2018/10/Codice-in-materia-di-protezione-dei-dati-personali-Testo-coordinato-2018.pdf
- https://www.garanteprivacy.it/documents/10160/0/Guida+all+applicazione+del+Regolamento+UE+2016+679.pdf
- https://www.ac.infn.it/normativa/Disciplinare_per_l'uso_della_risorse_informatiche.pdf
- https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict
- https://dpo.infn.it/wp-content/uploads/2018/12/LNF_181128_Ronconi.pdf
- https://dpo.infn.it/wp-content/uploads/2018/10/Deliberazione_CD_14844.pdf
- https://dpo.infn.it/wp-content/uploads/2018/12/Norme_Trattamento_Dati_Personali_INFN.pdf