Normativa

Corso locale della sezione di Bologna

«INFN Cloud : Funzionalita', sicurezza e privacy»

23/06/2021

Gianluca Peco, Paolo Veronesi

Modalità di registrazione identita' digitale

Per poter utilizzare le risorse di INFN Cloud, anche quelle istanziate da altri, devono essere soddisfatte le seguenti condizioni obbligatorie :

1. possedere una identita'digitale verificata (LoA2) su INFN AAI :
   - Se non si possiede ancora tale identita' occorre connettersi a https://signup.app.infn.it/ per effettuare la auto registrazione ed ottenere un account su INFN-AAI. La documentazione e' disponibile qui.
   - Fatto questo occorre connettersi al portale utente di INFN-AAI https://userportal.app.infn.it/ utilizzando l'account appena ottenuto, per completare la registrazione. Durante questo processo occorrera'scegliere in quale sito INFN ci si vuole identificare e la persona che dovra'approvare la richiesta. La documentazione e' disponibile qui. A questo punto verrete contattati dalla segreteria competente per l'identificazione.
2. avere seguito e superato il "Corso di Sicurezza Informatica - BASE". Per effettuare il corso utilizzare questo link.
3. dichiarare di aver letto ed accettato I regolamenti INFN in materia di utilizzo delle risorse informatiche:
   - Rules for the processing of personal data
   - Disciplinary for the use of INFN IT resources

Modalita' di registrazione IAM di INFN Cloud

Occorre richiedere un account per lo IAM di INFN Cloud solo se e' necessario istanziare servizi sull'infrastruttura INFN Cloud

- In questo caso e' necessario ricevere la "Nomina ad Amministratore di sistema" da parte del Direttore della sezione o Laboratorio, menzionando come ambito di utilizzo: "INFN-CLOUD (come utente amministratore)
- La procedura necessaria da seguire e' disponibile qui.
- Nel caso in cui non sia possibile ottenere questa “nomina ad amministratore di sistema”, si puo'utilizzare INFN Cloud accedendo ad un servizio creato, e amministrato, da un'altra persona, che è stata nominata amministratore di sistema. Questa persona può appartenere a qualsiasi Sezione o Laboratorio dell'INFN.
- Per registrarsi allo IAM di INFN Cloud https://iam.cloud.infn.it/

Modulo nomina 1

Designazione alla funzione di Amministratore di sistema

Il sottoscritto ……., in qualità di Direttore del …….

DESIGNA

(nome-cognome) ……. quale Amministratore dei sistemi impiegati, anche per il trattamento di dati personali (ove presenti), nel seguente ambito di operatività: INFN-CLOUD (quale utente amministratore)

COMUNICA

1. che la designazione ha durata quadriennale salvo revoca espressa: la cessazione del rapporto di lavoro o di collaborazione con l'INFN e la variazione dell'ambito di operatività sopra descritto determinano la decadenza dalla funzione assegnata;
2. che gli amministratori di sistema, in conformità a quanto disposto dalla legge e dai regolamenti dell'INFN, sono tenuti all'osservanza di tutte le disposizioni contenute nel Disciplinare per l'uso delle risorse informatiche dell'INFN, e in particolare a:
   - mantenere i sistemi al livello di sicurezza appropriato al loro uso;
   - verificare con regolarità l'integrità dei sistemi;
   - controllare e conservare i log di sistema per il tempo necessario a verificare la conservazione degli standard di sicurezza;
   - segnalare immediatamente all'INFN-Cloud security incident team sospetti abusi e violazioni della sicurezza e partecipare alla loro gestione;
   - installare e mantenere aggiornati programmi antivirus per i sistemi operativi che lo prevedono
   - 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;
   - in caso di interventi di manutenzione, impedire, per quanto possibile, l'accesso alle informazioni e ai dati personali presenti nei sistemi;
   - seguire le attività formative in materie tecnico-gestionali e di sicurezza delle reti, nonché in tema di protezione dei dati personali e di segretezza della corrispondenza.

Modulo nomina 2

INVITA

A prendere visione dei seguenti documenti:

- Norme per il trattamento dei dati personali

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

- Disciplinare per l'uso delle risorse informatiche dell'INFN

  https://web.infn.it/CCR/images/stories/upload_file/sicurezza_informatica/Sicurezza_Informatica_aggiornata/Disciplinare_2020_IT.pdf

Data:

Il Direttore

Firma per presa visione e accettazione

.....

Normativa di riferimento

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

- Circolare Agid Misure Minime di sicurezza informatica per le PA 18/4/2017 (link) in vigore 31/12/2017
- Regolamento (UE) - GDPR 2016/679 (link) in vigore 28/5/18
- *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)
- Disciplinare per l'uso delle risorse informatiche nell'INFN 24/1/2020 (ITA ENG)

Informativa DG trattamento dati personali https://dpo.infn.it/documenti-interni-infn/

Documenti INFN

Deliberazioni

Nomina del DPO: *Deliberazione n. 14734 del 27 Aprile 2018*

Deliberazione n. 14844 del 27 Luglio 2018 e in allegato *Norme per l'uso dei sistemi informatici destinati al trattamento di dati personali nell'INFN*

Lettere di trasmissione

Lettera di trasmissione del Direttore Generale del 15/11/2018: *Documento informativa cookie e adempimenti deliberazione CD 14844*

Lettera di trasmissione del Direttore Generale del 20/12/2018: *Trasmissione modulo designazione incaricati trattamento dati personali e relative istruzioni*

Lettera di trasmissione del Direttore Generale del 3/1/2019: *Trasmissione modelli di informativa per il trattamento dati personali e relative istruzioni*

Lettera di trasmissione del Direttore Generale del 3/1/2019: *Adempimenti in caso di violazione dati personali e trasmissione modelli per le relative comunicazioni*

Lettera di trasmissione del Direttore Generale del 11/3/2019: *contratto per la designazione del responsabile del trattamento dei dati personali*

Lettera di trasmissione del Direttore Generale del 23/7/2019: *procedura di gestione data breach*

Lettera di trasmissione del Direttore Generale del 19/9/2019: *prescrizioni sul trattamento dei dati particolari nel rapporto di lavoro*

Deliberazione 14844 e Norme per l'uso di sistemi destinati al trattamento dei dati personali

Visualizzazione norme d'uso GDPR

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

Disciplinare INFN per l'utilizzo delle risorse informatiche

Visualizzazione disciplinare

http://www.infn.it/disciplinareRisorseInformatiche/documents/it_disciplinare_2020.pdf

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*, garantendo 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/2018/10/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/2018/10/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

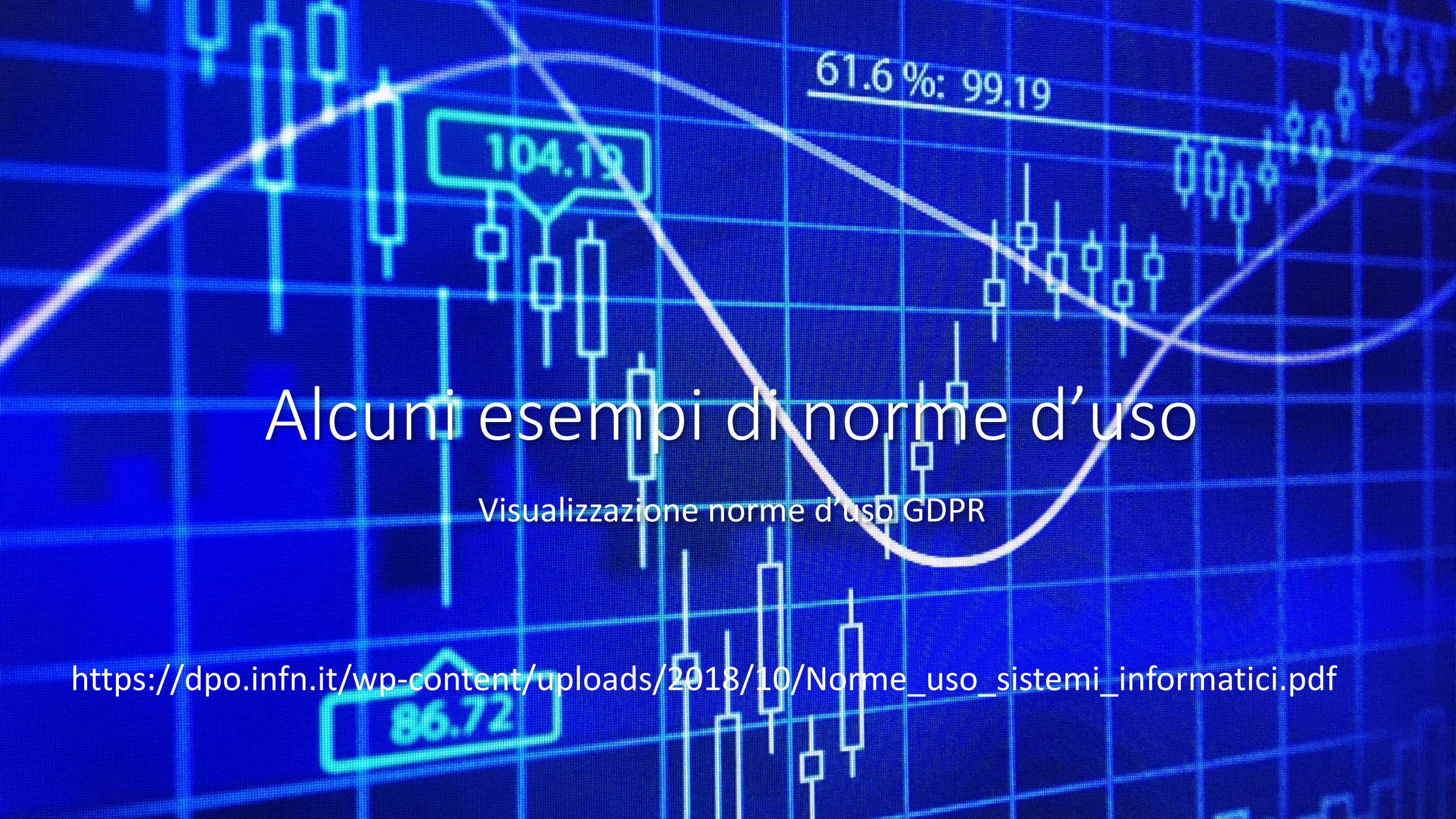
Norme d'uso obbligatorie per sistemi informatici destinati al trattamento di dati personali

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



Alcuni esempi di norme d’uso

Visualizzazione norme d’uso GDPR

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

Ripasso delle responsabilità di un utente di dispositivi TS (Tecnico Scientifici) in ambito INFN

- I sistemi detti Tecnico Scientifici sono quelli che hanno un solo utente (ad uso personale) e non trattano dati personali o considerati critici. (macchine per il calcolo single user, macchine per lo sviluppo, laptop e desktop personali, etc.)
- In questo caso occorre rispettare il disciplinare per l'uso delle risorse informatiche ed impegnarsi ad applicare le buone pratiche consigliate da CCR che derivano dall' applicazione della direttiva AGID dette "misure minime di sicurezza informatica
- https://docs.infn.it/share/page/site/ccr/document-details?nodeRef=workspace://SpacesStore/240e0dbe-0f14-4abf-8cab-d785da8dcc50
- https://docs.infn.it/share/page/site/ccr/document-details?nodeRef=workspace://SpacesStore/882245d9-9042-4f21-a52d-2e969990b3b9
- Ovviamente occore rispettare tutte le leggi e I regolamenti esistenti di carattere generale, i termini delle licenze d'uso e la disciplina sulla violazione della proprieta' intellettuale. !! Leggiamo sempre cio' che accettiamo !!

Differenze tra lavorare sul proprio laptop/desktop e lavorare su ambiente INFN-CLOUD

- Un Firewall perimetrale che blocca il traffico non esplicitamente richiesto
- Un sistema di Intrusion detection and prevention che individua prontamente eventuali minacce
- Un sistema antimalware che riduce il rischio di attacchi informatici
- Tali dispositivi di sicurezza non sono completamente disponibili nelle risorse di INFN Cloud o non sono disponibili I meccanismi per poterle gestire in autonomia. (almeno per ora)
- Questo rende tali risorse, se non adeguatamente gestite potenzialmente piu' vulnerabili ad attacchi informatici e al rischio data breach.