Prima giornata del Tutorial Days CCR
Edizione 2021

Normativa di riferimento e definizioni

Nadina Foggetti

Fonti

Linee Guida OCSE 2015	• valutazione del rischio • modularità dell'implementazione
GDPR	• Art. 32 Sicurezza del trattamento • Accountability • Natura, oggetto, contesto, finalità del trattamento, valutazione del rischio, valutazione dei costi
Direttiva NIS 2016/1148	• Affidabilità e sicurezza • Operatori di servizi essenziali

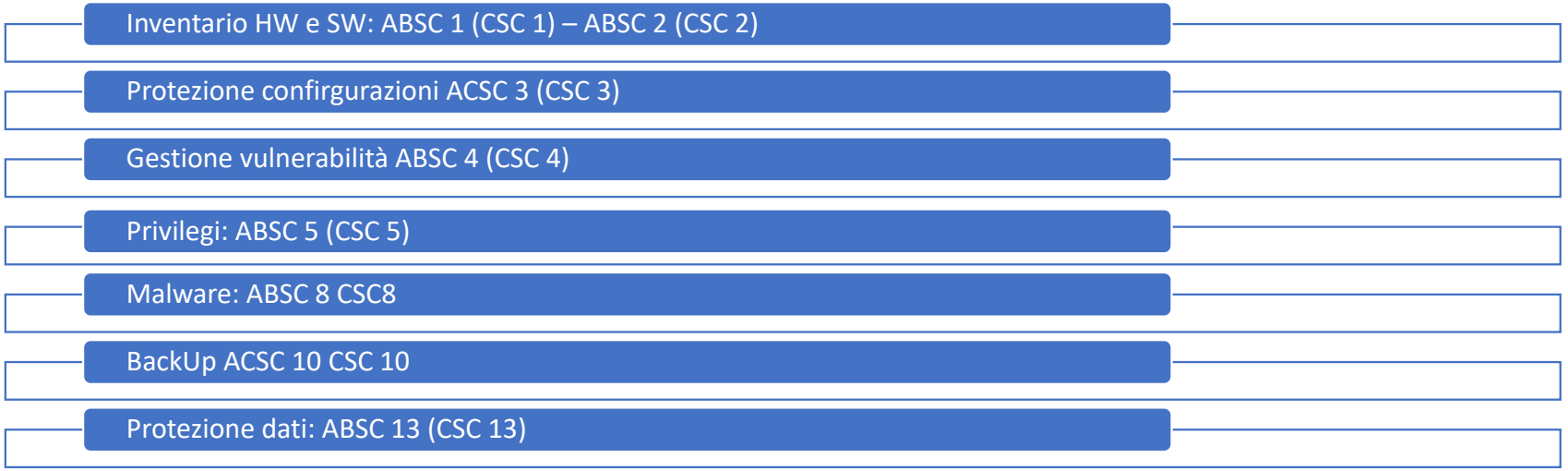
- **Misure minime di sicurezza AGID - Gazzetta Ufficiale (Serie Generale n.103 del 5-5-2017) della Circolare 18 aprile 2017, n. 2/2017,**

GDPR e Misure Minime AGID

- Valutazione del Rischio: misure idonee a garantire ed essere in grado di dimostrare, l'osservanza ai principi di protenzione dei dati personali, tenendo conto dei rischi aventi probabilità e gravità diverse per i diritti e libertà delle persone fisiche (Art. 24 GDPR) – DPIA;
- MMS-PA:ABSC (Agid Basic Security Controls)

- **I controlli individuati da Agid sono basati sui 20 CIS Critial Security Control Pubblicati dal Center for Internet Security noti come SANS 20**

Gli otto ambiti delle misure minime



- **I principi base sono sintetizzabili nella protezione della riservatezza, Integrità e Disponibilità (RID o CIA) delle informazione de dei dati. Le misure richieste sono collegate a questi aspetti.**

- Disponibilità: grado in cui le informazioni sono disponibili all’utente e al sistema nel momento in cui viene richiesto.
- Temporali: I sistemi informativi sono disponibili quando necessario:
- Continuità: il personale può continuar a lavorare in caso di guasto;
- Robustezza: vi è una capacità sufficiente per consentire a tutto il personale nel sistema di lavorare.

Obiettivi delle misure minime

- forniscono un riferimento operativo direttamente utilizzabile (checklist),
- stabiliscono una base comune di misure tecniche ed organizzative irrinunciabili;
- forniscono uno strumento utile a verificare lo stato di protezione contro le minacce informatiche e poter tracciare un percorso di miglioramento;
- responsabilizzano le Amministrazioni sulla necessità di migliorare e mantenere adeguato il proprio livello di protezione cibernetica.

Livelli di attuazione

- Le misure consistono in controlli di natura tecnologica, organizzativa e procedurale e utili alle Amministrazioni per valutare il proprio livello di sicurezza informatica.

  - Minimo: è quello al quale ogni Pubblica Amministrazione, indipendentemente dalla sua natura e dimensione, deve necessariamente essere o rendersi conforme.

  - Standard: è il livello, superiore al livello minimo, che ogni amministrazione deve considerare come base di riferimento in termini di sicurezza e rappresenta la maggior parte delle realtà della PA italiana.

  - Avanzato: deve essere adottato dalle organizzazioni maggiormente esposte a rischi (ad esempio per la criticità delle informazioni trattate o dei servizi erogati), ma anche visto come obiettivo di miglioramento da parte di tutte le altre organizzazioni.

Le misure minime Agid

- Non Rappresentano tutto ciò che è necessario fare per garatnire la cybersecurity

Il GDPR: principi fondamentali in materia di tutela dei dati personali

Principio di liceità, correttezza e trasparenza

- Art. 5 par. 1, lett a) GDPR: “I dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell’interessato”.
- Lecito: base giuridica!
- Necessario: ingerenza proporzionata
- Correttezza: norme etiche e deontologiche
- Trasparente:

- **Mettere a disposizione del pubblico l’informativa sulla privacy, ossia un documento che spiega in maniera chiara, concisa ma completa le finalità della raccolta dei dati e come si intende usarli.**
- **Modelli predisposti da INFN Cloud**

Il principio di limitazione della finalità

- Art. 5 par. 1, lett. B): “I dati devono essere raccolti per le finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con le finalità; un unterorire trattamento dei dati personali ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storia o af ini statistici non è consentito”.

- **Concetto di compatibilità;**
- **Base guidica aggiuntiva**

Il principio di minimizzazzione

- Art. 5 paragrafo 1, lettera c): “adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati”.
- Quantità minima di dati personali
- Portata minima del trattamento dei dati personali.
- Privacy by desing

- **Es: utente chiamato a compilare più volte sul sito web form online**
- **Es: pseudonimizzazione**

Il principio di esattezza, integrità e riservatezza dei dati

- I dati personali devono essere esatti e, se necessario, aggioranti”
- Adeguata sicurezza compresa la protezione da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale, mediante misure tecniche ed organizzative adeguate.

- **Non c’è un decalogo:**
- **Misure pseduonimizzazione e di cifratura dei dati;**
- **Misure atte ad assicurare su base permanente la riservatezza, l’integrità e la disponibilità dei dati, la resilienza dei sistemi e dei servizi di trattamento**
- **Misure per rispristinare tempestivamente la disponibilità dei dati in caso di incidente**

Principio di limitazione della conservazione

- Art. 5 par. 1 lett. E) GDPR: tutti i dati devono essere conservati in una forma che consenta l'identificazione degli interessanti per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.
- Cancellazione dei dati
- Conservazione vs necessario
- Esempio: File di log
- **Eccezioni: ricerca scientifica**

Accountability

- Principio di responsabilizzazione:
- Misure atte a garantire che le norme siano rispettate (es. Policy);
- Disporre documentazione atta a dimostrare agli interessati e alle utorità di controllo le misure adottate (Incident team; documentazione per l'uso delle risorse, ToU);

- **IMP: DPIA definire I rischi e le misure adottate (Cfr. Provvedimento 20 dicembre 2018).**

Consenso

- Art. 4 par. 11 GDPR:
- Qualsiasi manifestazione di volontà libera, specifica e informata e inequivocabile dell'interessato;
- Esplicito:
  - art. 9 (Categorie particolari di dati);
  - art. 49 (trasferimento verso Paesi terzi);
  - Art. 22 (processi decisionali automatizzati);
  - Linee Guida: confermato in una dichiarazione scritta e sottoscritta da parte dell'interessato.
  - Modalità elettroniche

- **Informativa sui dati**

Il GDPR: gli attori

Il titolare del trattamento

- Responsabile:
  - Correttezza e trasparenza del trattamento dei dati
  - Rispetto delle finalità
  - Esattezza
  - Riservatezza durante il trattamento
- Obblighi:
  - Lo sviluppo del registro dei trattamenti
  - La valutazione dei rischi privacy
  - L'eventuale valutazione di impatto
  - La consultazione preventiva con il Garante
  - L'implementazione delle misure tecniche ed organizzative
  - La nomina dei responsabili esterni
  - L'individuazione degli autorizzati al trattamento di dati personali
  - L'eventuale nomina del DPO (Responsabile della protezione dei dati)
  - L'emissione delle informative
  - La raccolta del consenso, ove necessario
  - L'implementazione della procedura di data breach
  - La formazione degli autorizzati al trattamento
  - La nomina dell'amministratore di sistema, ove necessario
  - La redazione del capitolato della video sorveglianza (ove presente)
  - La gestione del riscontro verso le istanze degli interessati
  - La gestione della contitolarità

Il Responsabile del trattamento

- **il responsabile del trattamento non è affatto una figura interna all'organizzazione ma è una persona fisica o giuridica che tratta i dati personali degli interessati per conto del titolare all'esterno dell'organizzazione**

- **Accordo/contratto per la nomina**

Data Protection Officer (DPO)

- E’ **una figura specializzata nella protezione dei dati personali attraverso l’applicazione delle misure tecniche ed organizzative (art. 37 GDPR).**

- **Il ruolo del DPO è di tutelare i dati personali, non gli interessi del titolare del trattamento.** E ciò appare ovvio soprattutto nell'ambito degli enti pubblici e delle aziende che effettuano un monitoraggio su larga scala degli individui. Il DPO deve, infatti, possedere un'adeguata conoscenza delle normative e delle prassi di gestione dei dati personali, e **deve adempiere alle proprie funzioni in piena autonomia ed indipendenza, e in assenza di conflitti di interesse**.

- **Il provvedimento del Garante sloveno del 24 marzo 2021 segnala l'incompatibilità delle posizione di alta dirigenza e altri ruoli subordinati nell'organizzazione aziendale, qualora tali incarichi o ruoli portino alla determinazione delle finalità e dei mezzi del trattamento.**
- **Principio di indipendenza DPO**

L’incaricato

- **Si tratta della persona fisica che, all’interno dell’Organizzazione, opera trattando i dati personali degli interessati.**

- **Apposita nomina!**

L’amministratore di sistema

- *Provvedimento del Garante* **27 novembre 2008 Amministratori di sistema :** Con la definizione di "amministratore di sistema" si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del presente provvedimento vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi *software* complessi
- *RegoleAGID* 18a prile 2017, n.**2/2017**.
- DisciplinareINFN

- **Vigilare**
- **Attuare misure di sicurezza**
- **Gestire gli accessi ai database e le operazioni che vengono effettuate sui dati personali**
- **Stretta relazione con il titolare del trattamento**

Tipologie di Dati

Dato personale

- Dato vs informazione
- Dato personale è qualsiasi informazione (es. nome) concernente una **persona fisica identificata o identificabile** (art. 4 GDPR) **anche indirettamente**, oppure informazioni (es. codice fiscale, impronta digitale, traffico telefonico, immagine, voce) riguardanti una persona la cui identità può comunque essere accertata mediante informazioni supplementari.
- **il dato personale è un concetto dinamico, che va sempre riferito al contesto**,

- La **CEDU:** non esiste una netta separazione tra **vita privata e vita professionale** per quanto riguarda i dati personali, per cui anche le informazioni riguardanti la vita professionale e pubblica di una persona sono considerate dati personali.

Dati identificativi

- Le informazioni di identificazione personale (**PII, Personally identifiable information**) sono dati che consentono l'identificazione diretta dell'interessato, tra i quali abbiamo (anche considerando la definizione dell'Istituto nazionale degli standard e della tecnologia, NIST):

- nome e cognome
- indirizzo di casa
- indirizzo email
- numero identificativo nazionale
- numero di passaporto
- indirizzo IP (quando collegato ad altri dati)
- numero di targa del veicolo
- numero di patente
- volto, impronte digitali o calligrafia
- numeri di carta di credito
- identità digitale
- data di nascita
- luogo di nascita
- informazioni genetiche
- numero di telefono
- account name o nickname;
- dati di localizzazione e mobilità (GPS).

Categorie particolari di dati

- **L'articolo 9 del GDPR sancisce un generale divieto di trattare alcuni tipi di dati, cioè quelli che rivelino:**

  - l'origine razziale o etnica;

  - le opinioni politiche;
  - le convinzioni religiose o filosofiche;
  - l'appartenenza sindacale;
  - i dati genetici,(Garante autorizzazione generale del 15 dicembre 2016);
  - dati biometrici intesi a identificare in modo univoco una persona fisica;
  - dati relativi alla salute (vedi la sentenza della Corte di giustizia europea del 6 novembre 2003, C 101/01, Rs Lindqvist, punto 50 f);
  - dati relativi alla vita sessuale o all'orientamento sessuale della persona;
  - dati relativi a condanne penali e reati, il cui trattamento è consentito solo se autorizzato da norma di legge o di regolamento.

Presupposti del trattamento

- Esplicito consenso dell'interessato;
- lI trattamento è necessario per **finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali;**
- il trattamento è necessario per **motivi di interesse pubblico nel settore della sanità pubblica**,
- il trattamento è necessario a f**ini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici**.