GDPR AWARENESS RAISING CAMPAIGN FOR SMEs

Cofinanziato dall'Unione Europea

LE MISURE TECNICHE E ORGANIZZATIVE DI SICUREZZA
6 febbraio 2024

Fausto Cioffi
Dorotea Alessandra de Marco
Funzionari direttivi
Dipartimento tecnologie digitali e sicurezza informatica

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Agenda

- Principi
- Responsabilità
- Sicurezza del trattamento
- Data Protection by design & by default
- Misure di sicurezza
- Strumenti a supporto
- Qualche provvedimento

Art. 5 - Principi applicabili al trattamento di dati personali

- liceità, correttezza e trasparenza
- limitazione delle finalità
- minimizzazione dei dati
- esattezza
- limitazione della conservazione
- Integrità e riservatezza

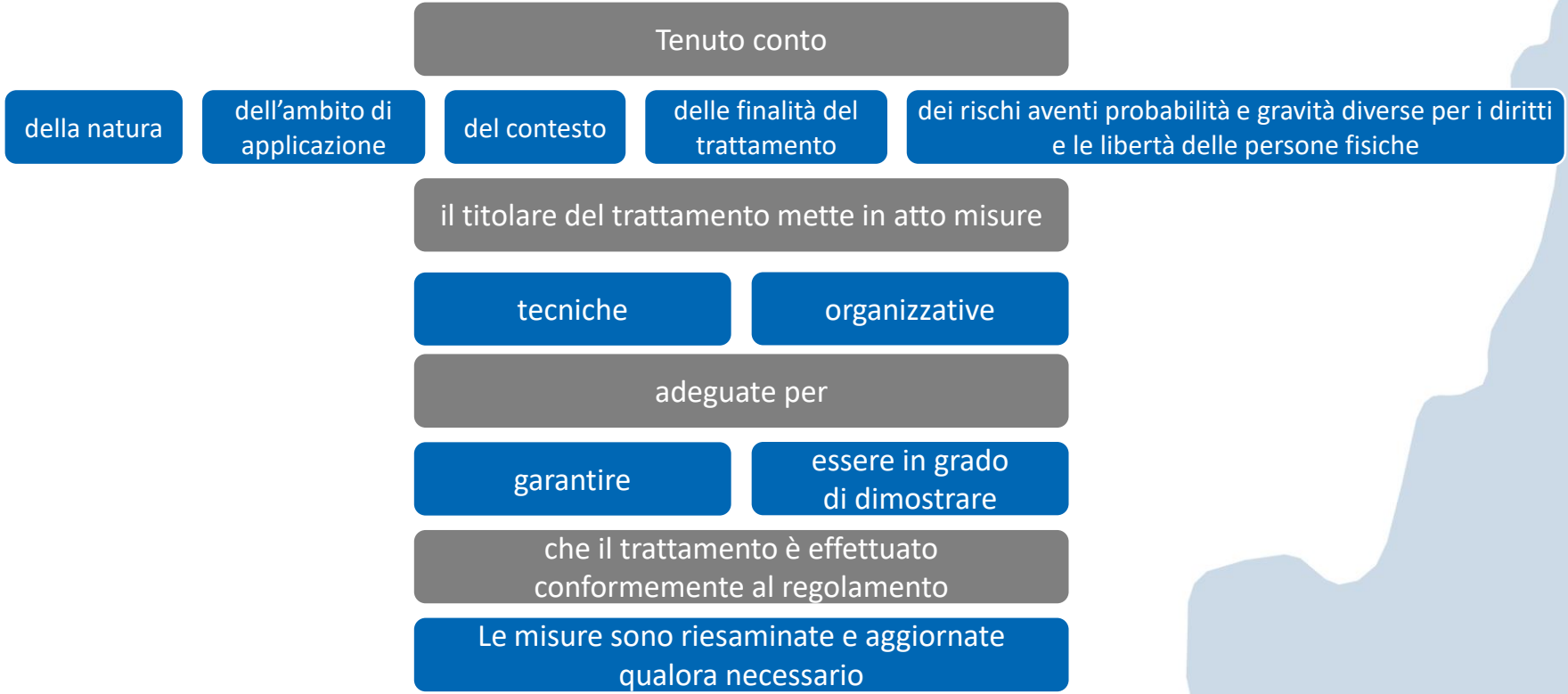
responsabilizzazione

I dati personali sono:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati
- esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati
- trattati in maniera da garantire **un'adeguata sicurezza** dei dati personali, compresa la protezione, **mediante misure tecniche e organizzative adeguate**, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali

Il titolare del trattamento è competente per il rispetto […] e in grado di **comprovarlo**

Art. 24 - Responsabilità del titolare del trattamento



Misure tecniche organizzative

Principi

Responsabilità

Misure tecniche organizzative

Art. 32 - Sicurezza del trattamento

Tenuto conto

dello stato dell'arte e dei costi di attuazione | della natura | dell'oggetto | del contesto | delle finalità del trattamento | del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche

il titolare del trattamento mette in atto misure

tecniche | organizzative

adeguate per

garantire

un livello di sicurezza adeguato al rischio

Art. 32 - Sicurezza del trattamento

Rischi da tenere in considerazione

Nel valutare l'adeguato livello di sicurezza

si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare

- distruzione
- perdita
- modifica
- divulgazione non autorizzata
- accesso, accidentale o illegale

a dati personali trasmessi, conservati o **comunque trattati**

Art. 32 - Sicurezza del trattamento

a) la **pseudonimizzazione** e la **cifratura** dei dati personali;

b) la capacità di assicurare su base permanente la **riservatezza**, **l'integrità**, la **disponibilità** e la **resilienza** dei sistemi e dei servizi di trattamento;

c) la capacità di **ripristinare** tempestivamente la **disponibilità** e **l'accesso** dei dati personali in caso di incidente fisico o tecnico;

d) una **procedura** per **testare, verificare e valutare regolarmente** l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento

Art. 32 - Sicurezza del trattamento

Art. 32, par. 1, lett. d), del Regolamento

Il titolare e il responsabile del trattamento devono adottare procedure «***per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento***»

- attività di audit e di penetration testing / vulnerability assessment
- costituire all'interno dell'organizzazione team dedicati alla verifica dell'efficacia delle misure di sicurezza adottate all'interno dell'organizzazione

Pseudonimizzazione

il trattamento dei dati personali in modo tale che i dati personali ***non possano 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;*

non è modificata l'associazione biunivoca tra dato e persona, consiste nel **sostituire un attributo, solitamente univoco, di un dato con un altro, ugualmente univoco e, solitamente, non immediatamente intellegibile**.

rimane **consentita l'identificazione**, anche se più complessa e con mezzi onerosi, poiché è **inalterato il quadro di certezze nella concatenazione dei passaggi necessari per l'attribuzione del dato pseudo-anonimo a quest'ultima**. (es. diritti di accesso sul dato).

risultato opposto a quello che si prefigge **l'anonimizzazione**

Pseudonimizzazione

riduce l'intellegibilità di un insieme di dati relativi a una persona interessata

misura di sicurezza non un metodo di anonimizzazione

garantisce la **confidenzialità** del dato, non più immediatamente intellegibile, ma anche, se utilizzate tecniche crittografiche, **l'integrità** contro manipolazioni anche accidentali

la **parte non pseudonimizzata del dato**, può presentare elementi identificativi tali da poter riferire ancora il dato alla persona specie se sono numerosi gli attributi che descrivono il dato (singolarità delle preferenze o dei gusti, delle relazioni interpersonali all'interno di una rete di contatti, dei movimenti, dell'unicità del carattere o del talento)

Pseudonimizzazione

risultato (pseudonimo) può essere indipendente dal dato iniziale (es. valore casuale assegnato a un attributo del dato) o può essere calcolato a partire dal valore originale di un attributo o insieme di attributi (es. applicazione di una tecnica crittografica).

il **dato pseudonimizzato**, una volta impiegato in combinazione con tutti i mezzi necessari per effettuare la sostituzione di attributi a ritroso, è **inequivocamente riferibile alla persona**

a seguito del processo di pseudonimizzazione, la **persona fisica potrebbe essere ancora identificata in maniera indiretta**

Pseudonimizzazione

Technique	Pseudonym Generator
Counter	Monotonic counter which starts at a certain value and is increased each time a new pseudonym is necessary
Random number	Random value extracted between a minimum and a maximum boundary each time a new pseudonym is necessary
Hash function	One-way (non-reversible) cryptographic function transforming input personal data in fixed-length values
Hash-based message authentication code (HMAC)	One-way (non-reversible) cryptographic function adding a key that makes it less predictable than a hash function
Encryption	Two-way (reversible) cryptographic function transforming an input personal data in values that can be re-transformed in its original format using a key

Anonimizzazione

dati anonimizzati: dati tali da **non consentire l'identificazione diretta o indiretta di una persona in relazione ai** mezzi (economici, informazioni, risorse tecnologiche, competenze, tempo disponibile) nella disponibilità di chi (titolare o altro soggetto) provi a utilizzare il dato anonimizzato per identificare la persona

pervenire ad una nuova rappresentazione del dato, il dato anonimizzato, che non è più un dato personale e, pertanto, non rientra nell'ambito di applicazione della disciplina di protezione dati

tutela volta a impedire, a meno di dover ricorrere a mezzi irragionevolmente utilizzabili, la riferibilità del dato a una persona (**misura di protezione della privacy**)

Anonimizzazione

mezzi “**ragionevolmente utilizzabili**”: elementi soggettivi (contesto), oggetto di un riesame periodico in ragione dei nuovi rischi connessi alla crescente disponibilità di mezzi tecnici a basso costo (es. cloud computing), all’accessibilità pubblica sempre maggiore di altre banche dati (es. Big Data), e alle competenze tecniche utilizzate.

mezzi idonei a disvelare l’identità della persona diventano “**irragionevolmente utilizzabili**” quanto minore sarà il numero di elementi potenzialmente identificativi presenti nel dato anonimizzato poiché tanto maggiore sarà lo sforzo necessario all’identificazione della persona per chi utilizza quel dato

Anonimizzazione

il livello di **motivazione** di eventuali soggetti interessati ad associare il dato anonimizzato ad una persona

natura dei dati originali (soprattutto se categorie particolari ex art. 9) e della riferibilità dei dati a specifiche tipologie di interessati, che per questa stessa caratteristica possono essere più facilmente identificabili

applicazione, da parte del titolare che effettua l'anonimizzazione, di idonee **misure di sicurezza**, o di **vincoli** contrattuali che possono limitare la "visibilità" dei dati anonimizzati, ad esempio a soli utilizzatori in possesso di specifiche credenziali di accesso e sulla base di riconosciute esigenze a conoscere il dato anonimizzato

Art. 28 - Responsabile del trattamento

1. *Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a* ***responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative*** *adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato*

[…]

3. *I trattamenti da parte di un responsabile del trattamento sono disciplinati* ***da un contratto o da altro atto giuridico*** *[…].* ***Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:*** *[…]*

- f) ***assista il titolare*** *del trattamento nel garantire il rispetto degli obblighi di cui agli* ***articoli da 32 a 36****, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento […]*

Art. 25 - Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

Efficacia nell'applicazione dei principi

- Liceità
- Trasparenza
- Esattezza
- Limitazione delle finalità
- Conservazione
- Integrità e riservatezza

Misure tecniche e organizzative

- Individuare dei KPI per l'applicazione dei principi
- Preoccuparsi di rispettare il requisito di stato dell'arte
- Attenzione ai costi

Art. 25 - Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

L'obbligo principale consiste nel predisporre misure adeguate e garanzie necessarie che permettano un'attuazione efficace dei principi della protezione dei dati e, di conseguenza, dei diritti e delle libertà degli interessati fin dalla progettazione e per impostazione predefinita. L'articolo 25 prescrive gli elementi, sia della progettazione che dell'impostazione predefinita, di cui occorre tenere conto

L'articolo 25, paragrafo 1, prevede che il titolare debba prendere in considerazione la DPbDD fin dalla pianificazione di un nuovo trattamento.

Art. 25 e Linee guida 4/2019

I titolari attuano la DPbDD prima del trattamento e poi costantemente durante il trattamento, **verificando regolarmente l'efficacia delle misure e delle garanzie individuate**

Standard, migliori prassi e codici di condotta riconosciuti da associazioni e da altri organismi che rappresentano categorie di titolari del trattamento possono essere utili ai fini della determinazione di misure adeguate. Tuttavia, il titolare deve verificare l'adeguatezza delle misure con riguardo allo specifico trattamento

Art. 25 e Linee guida 4/2019

Per garanzia e misura tecnica od organizzativa **s'intende tutto ciò che è compreso fra l'uso di soluzioni tecniche avanzate e la formazione di base del personale**.

esempi, a seconda del contesto e dei rischi associati al trattamento in questione,

- la pseudonimizzazione dei dati personali,
- la memorizzazione di dati personali in un formato strutturato, di uso comune e leggibile da dispositivo automatico,
- la possibilità per gli interessati di intervenire nel trattamento
- la fornitura di informazioni sulla conservazione dei dati personali, la disponibilità di sistemi di rilevamento di malware
- la formazione dei dipendenti sull'«igiene informatica» di base
- istituzione di sistemi di gestione della privacy e della sicurezza delle informazioni
- l'obbligo contrattuale per i responsabili del trattamento di attuare prassi specifiche di minimizzazione dei dati

Art. 25 e principio riservatezza

elementi principali della progettazione e dell'impostazione predefinita, relativi all'integrità e alla riservatezza, possono figurare:

- sistema di gestione della sicurezza delle informazioni – occorre disporre di uno strumento operativo per gestire le politiche e le procedure per la sicurezza delle informazioni;
- analisi del rischio – valutare i rischi per la sicurezza dei dati personali, considerando l'impatto sui diritti delle persone, e contrastare quelli identificati, nonché, ai fini dell'utilizzo nella valutazione dei rischi, sviluppare e gestire una «modellizzazione delle minacce» esaustiva, sistematica e realistica e un'analisi della superficie di attacco riferita al software specifico così da ridurre i vettori di attacco e le opportunità di sfruttare eventuali punti deboli e vulnerabilità;
- sicurezza fin dalla progettazione – tenere conto non appena possibile dei requisiti di sicurezza nella progettazione e nello sviluppo del sistema, integrando e svolgendo costantemente test pertinenti;

Art. 25 e principio riservatezza

elementi principali della progettazione e dell'impostazione predefinita, relativi all'integrità e alla riservatezza, possono figurare:

- manutenzione – rivedere e verificare periodicamente il software, l'hardware, i sistemi e i servizi, ecc. per scoprire eventuali vulnerabilità dei sistemi di supporto del trattamento;
- gestione del controllo degli accessi – solo il personale autorizzato che ne ha necessità dovrebbe avere accesso ai dati personali necessari ai loro compiti di trattamento. Inoltre, il titolare dovrebbe differenziare i privilegi di accesso del personale autorizzato;
  - limitazione dell'accesso (agenti) – definire il trattamento dei dati in modo tale che un numero minimo di persone abbia bisogno di accedere ai dati personali per svolgere le proprie funzioni, e limitare l'accesso di conseguenza;
  - limitazione dell'accesso (contenuto) – nel contesto di ciascuna operazione di trattamento, limitare l'accesso per ogni set di dati ai soli attributi che sono necessari allo svolgimento di tale operazione. Limitare inoltre l'accesso ai dati relativi agli interessati di competenza del rispettivo dipendente;
  - segregazione dell'accesso – definire il trattamento dei dati in modo tale che nessuno necessiti di accedere a tutti i dati raccolti sull'interessato, tanto meno a tutti i dati personali di una categoria specifica di interessati;

Art. 25 e principio riservatezza

elementi principali della progettazione e dell'impostazione predefinita, relativi all'integrità e alla riservatezza, possono figurare:

- trasferimenti sicuri – i trasferimenti sono protetti da modifiche e accessi non autorizzati e accidentali
- conservazione sicura – la conservazione dei dati è protetta da modifiche e accessi non autorizzati. Dovrebbero essere previste procedure per valutare il rischio di conservazione centralizzata o decentrata, e le categorie di dati personali cui si applicano. Alcuni dati potrebbero richiedere misure di sicurezza supplementari rispetto ad altri o l'isolamento da questi ultimi;
- pseudonimizzazione – i dati personali e i backup/registri di eventi dovrebbero essere pseudonimizzati come misura di sicurezza per ridurre al minimo i rischi di potenziali violazioni dei dati, ad esempio utilizzando l'hashing o la cifratura;
- backup/registri di eventi – conservare backup e registri di eventi nella misura necessaria per la sicurezza delle informazioni, utilizzare registri delle attività (audit trails) e il monitoraggio degli eventi come controlli di sicurezza su base routinaria, proteggendoli da modifiche e accessi non autorizzati e accidentali e rivedendoli periodicamente, oltre a gestire in modo tempestivo eventuali incidenti;

Art. 25 e principio riservatezza

elementi principali della progettazione e dell'impostazione predefinita, relativi all'integrità e alla riservatezza, possono figurare:

- ripristino in caso di disastro (disaster recovery)/continuità operativa – soddisfare i requisiti per il ripristino del sistema informativo in caso di disastro e per la continuità operativa, al fine di ripristinare la disponibilità dei dati personali a seguito di incidenti rilevanti;
- protezione in base al rischio – tutte le categorie di dati personali dovrebbero essere protette con misure adeguate contro il rischio di violazioni della sicurezza. I dati che comportano rischi particolari dovrebbero, ove possibile, essere tenuti separati dagli altri dati personali;
- gestione della risposta in caso di incidenti legati alla sicurezza – occorre disporre di metodologie, procedure e risorse per rilevare, limitare, gestire e segnalare le violazioni dei dati e trarne insegnamenti;
- gestione degli incidenti – al fine di rendere più solido il sistema di trattamento, il titolare deve disporre di procedure per gestire violazioni e incidenti, ivi comprese procedure di notifica quali la gestione delle notifiche (per l'autorità di controllo) e delle informazioni (per gli interessati).

Pilastri della sicurezza delle informazioni

Riservatezza

informazioni accessibili solo al personale autorizzato

Integrità

protezione delle informazioni da modifiche indesiderate (solo chi è autorizzato può modificare le informazioni)

Disponibilità

informazioni/risorse disponibili solo a chi è autorizzato nei tempi e modi stabiliti

Violazione dei dati personali – *Personal Data breach*

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*

Violazione dei dati personali – *Personal Data breach*

Un *data breach* può essere classificato
in base ai tre principi della sicurezza delle informazioni

Violazione della riservatezza	Violazione dell'integrità	Violazione della disponibilità
divulgazione o accesso non autorizzati a dati personali	*modifica non autorizzata di dati personali*	*distruzione o perdita non autorizzate di dati personali*

Un *data breach* può anche riguardare contemporaneamente
la riservatezza, l'integrità e la disponibilità dei dati personali,
oppure una combinazione delle stesse

Artt. 33 e 34 - Notifica di una violazione dei dati personali all'autorità di controllo
Comunicazione di una violazione dei dati personali all'interessato

Il regolamento impone, tanto al titolare quanto al responsabile del trattamento, di disporre di **misure tecniche e organizzative adeguate per garantire un livello di sicurezza commisurato al rischio cui sono esposti i dati personali trattati**.

Un aspetto fondamentale di qualsiasi politica di sicurezza dei dati è la **capacità, ove possibile, di prevenire una violazione e, laddove essa si verifichi ciò nonostante, di reagire tempestivamente**

Violazione dei dati personali – *Personal Data breach*

C85 *«Una **violazione** dei dati personali **può**, se non affrontata in modo adeguato e tempestivo, **provocare danni fisici, materiali o immateriali alle persone fisiche**, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata* […]»

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Rilevamento del *data breach*

Contenimento del *data breach*

Valutazione del rischio

Notifica al Garante

Art. 33

Comunicazione agli interessati

Art. 34

C75 *«I **rischi per i diritti e le libertà delle persone fisiche**, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un **danno fisico, materiale o immateriale*** […]»

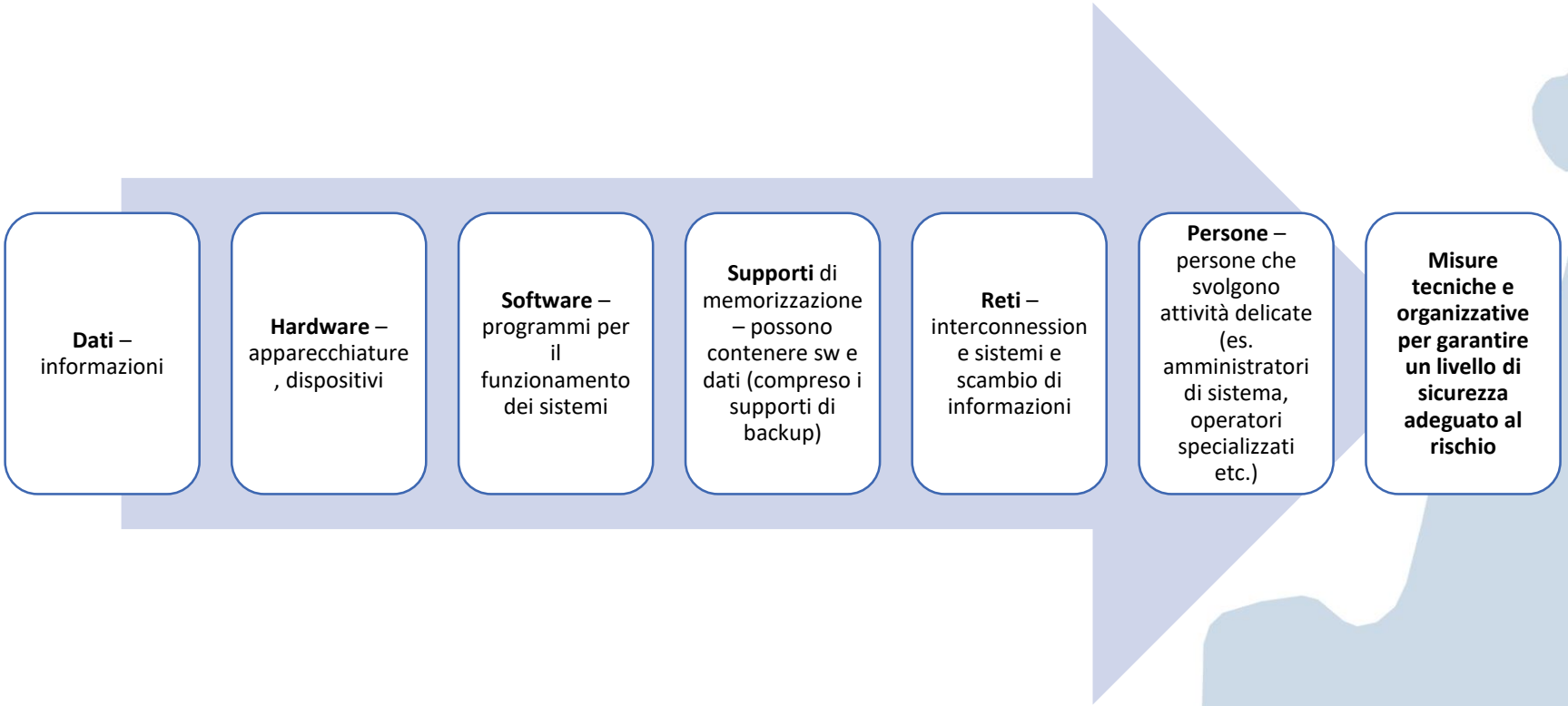
Art. 33, par. 5

C76 *«La **probabilità** e la **gravità** del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con … **natura**, all'**ambito** **applicazione**, al **contesto** e alle **finalità** del trattamento. Il rischio dovrebbe essere considerato in base a una **valutazione** … mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato»*

"Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679" (WP250 rev.01)

"Linee-guida 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali"

Asset da proteggere



Misure organizzative

Applicazione del **principio del *need to know* e *segregation of duty***, (indispensabilità e necessità, separazione)

politiche di sicurezza (es. IAA, accessi, meccanismi di protezione dell'integrità dei dati, procedure di *back u*p, procedure di *disaster recovery*, procedure in caso di incidenti)

verifiche periodiche (*audit* interni o terza parte) per **processo continuo di miglioramento** per la verifica dell'adeguatezza delle misure di sicurezza tecnico organizzative e la loro rispondenza alle disposizioni vigenti (*compliance*)

formazione e sensibilizzazione del personale

Procedure di *back up*

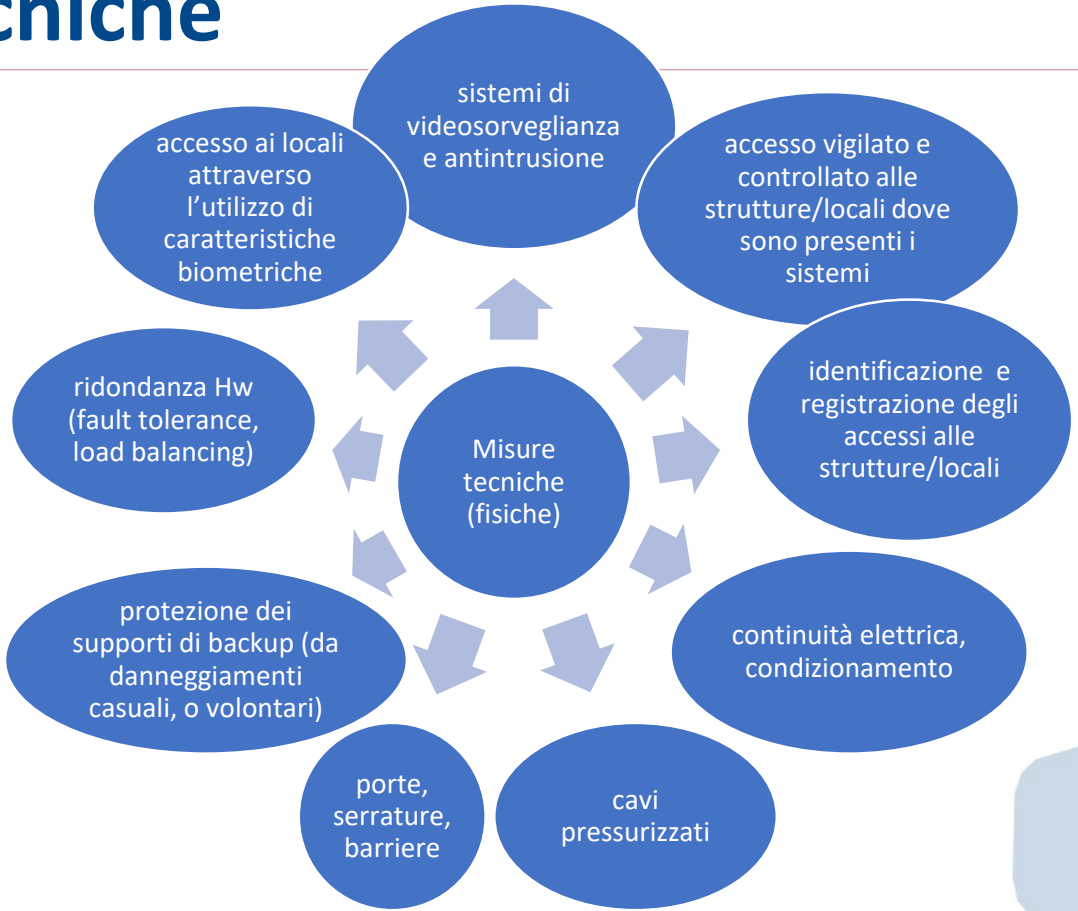
documentazione (procedure, *policy*, decisioni, audit/verifiche, etc)

decalogo uso strumenti

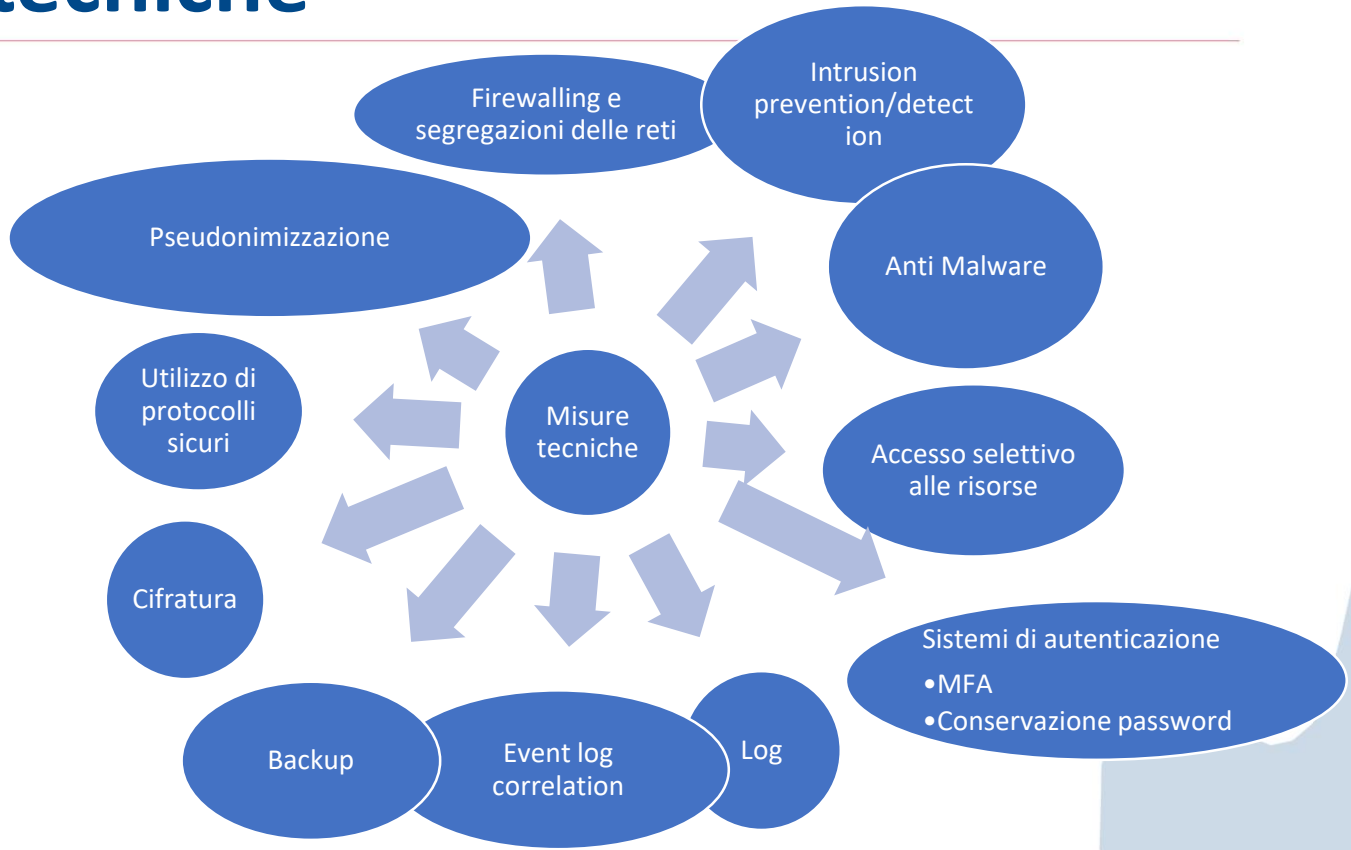
Policy

controllo degli accessi	classificazione e gestione delle informazioni (categorie e misure da applicare quali pseudonimizzazione, crittografia etc)	utilizzo dei sistemi, servizi e delle applicazioni aziendali (include email, di Internet e dei social media policy)	utilizzo dei sistemi in mobilità
utilizzo dei supporti di memorizzazione rimovibili	“clean desk” and “clear screen”	backup e ripristino dati	gestione degli incidenti che comportano violazioni di dati personali

Misure tecniche



Misure tecniche



Linee Guida Funzioni Crittografiche – Conservazione delle Password

Provvedimento del 7 dicembre 2023 [doc. web n. 9962283]

misure di attuazione dei principi di limitazione della conservazione e di integrità e riservatezza, nonché degli obblighi in materia di sicurezza del trattamento (artt. 5, par. 1, lett. e) e f), e 32 del Regolamento)

indicazioni sulle modalità e sui tempi di conservazione delle *password* impostate dagli utenti

Linee Guida Funzioni Crittografiche – Conservazione delle Password

soggetti destinatari

- titolari e i responsabili del trattamento, che devono adottare misure tecniche in grado di garantire un livello di sicurezza adeguato ai rischi presentati dal trattamento, proteggendo in modo efficace le *password* degli utenti che sono conservate nell'ambito di sistemi di autenticazione informatica o di altri sistemi
- produttori di prodotti, servizi e applicazioni, che sono invitati a tener conto delle indicazioni fornite dal Garante nella progettazione e nello sviluppo di prodotti, servizi e applicazioni al fine di consentire a titolari e responsabili del trattamento di utilizzare sistemi e tecnologie che integrano i principi di protezione dei dati

Linee Guida Funzioni Crittografiche – Conservazione delle Password

soggetti tenuti ad adottare adeguate misure tecniche di protezione delle *password*

- l'adozione delle linee guida risulta necessaria qualora sia soddisfatta una o più delle seguenti condizioni:
  - il trattamento riguarda le *password* di un numero significativo di utenti (es. un numero elevato di soggetti in termini assoluti oppure espressi in percentuale della popolazione di riferimento a livello locale, regionale e nazionale)
  - il trattamento riguarda le *password* di utenti che possono accedere a banche di dati di particolare rilevanza o dimensioni (es. dipendenti di pubbliche amministrazioni)
  - il trattamento riguarda le *password* di specifiche tipologie di utenti che sistematicamente trattano, con l'ausilio di strumenti informatici, dati appartenenti a categorie particolari o relativi a condanne penali e reati di cui agli artt. 9 e 10 del Regolamento (UE) 2016/679 (es. professionisti sanitari, avvocati, magistrati)

Linee Guida Funzioni Crittografiche – Conservazione delle Password

Cancellazione delle *password* degli utenti

- obsolescenza delle misure adottate per proteggere le *password* o compromissione dell'efficacia
- le *password* possono essere conservate anche per garantire la sicurezza delle procedure di autenticazione informatica, es. per impedire il riuso da parte dell'utente delle precedenti *password* (c.d. *password history*) o per assicurare il ripristino del sistema di autenticazione informatica in caso di incidente (copie di *backup*).
- cancellazione tempestiva, anche in modo automatico, in caso di
  - cessazione o dismissione dei sistemi informatici o servizi *online* a cui le credenziali di autenticazione consentivano l'accesso;
  - disattivazione o revoca delle credenziali di autenticazione di un utente che non ha più necessità di accedere a un sistema informatico o un servizio *online* o che non ha più i requisiti che ne hanno determinato l'abilitazione.

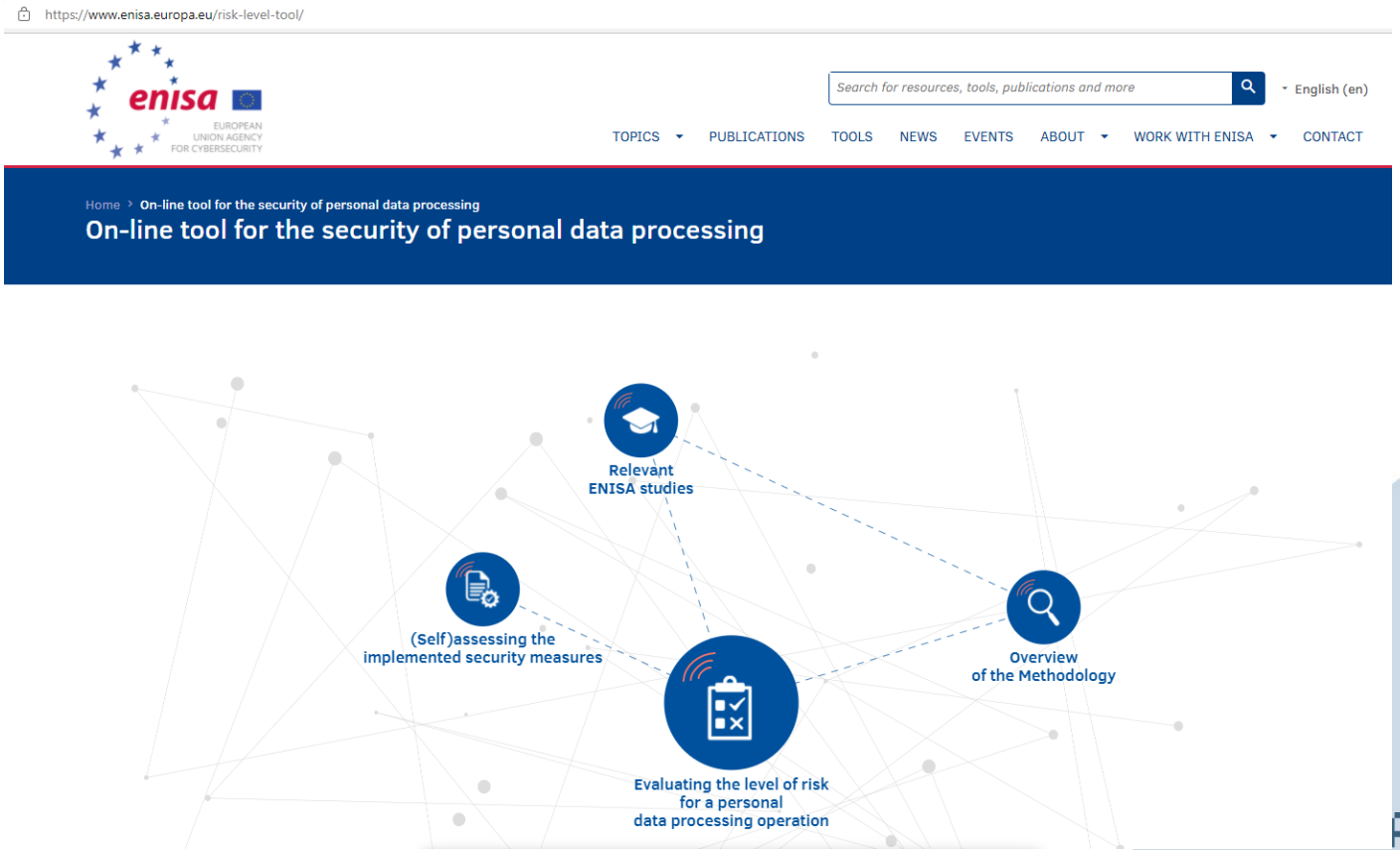
Art. 83 - Condizioni generali per infliggere sanzioni amministrative pecuniarie

Al momento di decidere se infliggere una ***sanzione amministrativa*** *pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi*

le ***misure adottate*** *dal titolare del trattamento o dal responsabile del trattamento* ***per attenuare il danno subito dagli interessati****;*

il grado di responsabilità del titolare del trattamento *o del responsabile del trattamento* ***tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32****;*

Tools a supporto dell'articolo 32 – ENISA



Tools a supporto dell'articolo 32 – ENISA

(Self)assessing the implemented security measures

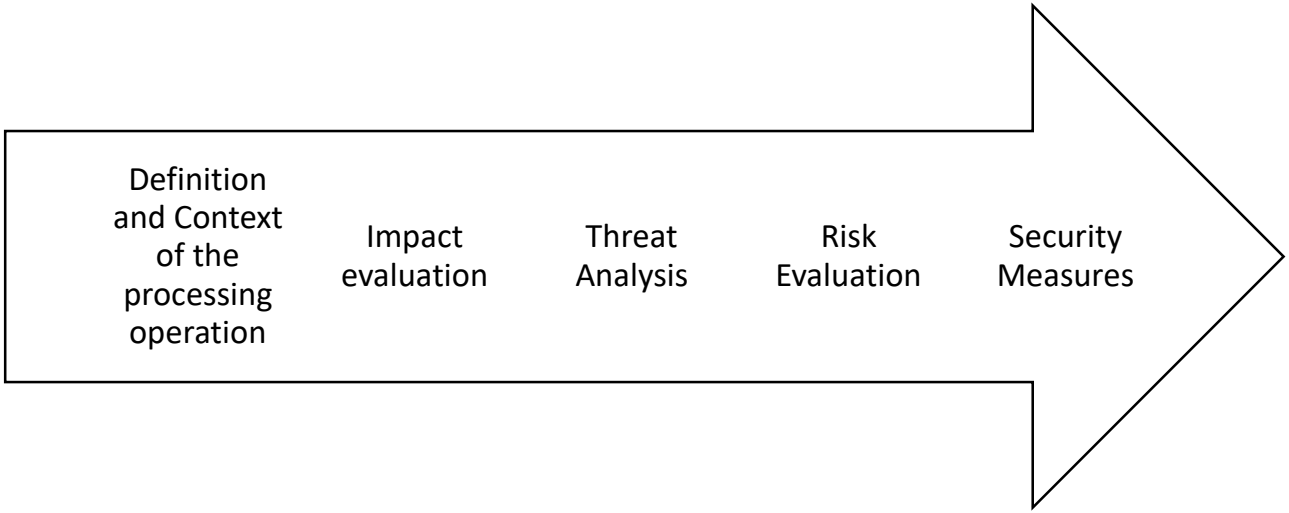
- Risk
- Processing

click the checkbox for each of the security measures that you are already implementing (20 categorie)

- Security policy and procedures for the protection of personal data (Related to ISO 27001:2013 - A.6.1.1 Information security roles and responsibilities)
- Roles and responsibilities
- Access control policy
- ….

Export

Tools a supporto dell'articolo 32 – ENISA



Tools a supporto dell'articolo 32 – ENISA

Step 1
Definition of the processing operation and its context

- Types of personal data
- Categories of data subjects
- Means of processing
- Recipients

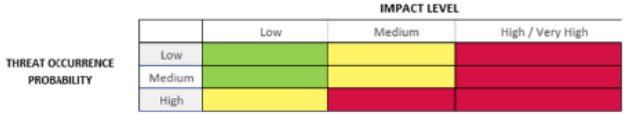
Step 2
Understanding and evaluation of impact

- Confidentiality
- Integrity
- Availability

Step 3
Definition of possible threats and evaluation of their likelihood

- Network and technical resources
- Processes/procedures related to the data processing operation
- Different parties and people involved in the data processing operation
- Business sector and scale of processing

Step 4
Evaluation of risk



Step 5
Selection of security measures

Tools a supporto dell'articolo 32 – ENISA

	Question	Purpose
1.	What is the personal data processing operation?	To realise if different risk assessment processes should run for different data processing operations.
2.	What are the types of personal data processed?	To understand the types of operations based on the data types; to get an indication of potential risk levels (as regards the types of data).
3.	What is the purpose of the processing?	To understand the limits of the data processing operation (as regards the purpose).
4.	What are the means used for the processing of personal data?	To define the means used for the data processing operations and their different types (in house resources, outsourced tools, etc.).
5.	Where does the processing of personal data take place?	To determine the location of the personal data processing.
6.	Which are the categories of data subjects?	To define the types of data subjects (clients, customers, etc.) involved in the data processing operation.
7.	Which are the recipients of the data?	To define the recipients of the data for capturing the authorized transfers of these data and the conditions of these transfers.

Tools a supporto dell'articolo 32 – ENISA

Level of Impact	Description
Low	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc.).
Very High	Individuals may encounter significant or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Tools a supporto dell'articolo 32 – ENISA

A. Network and technical resources (hardware and software)	
1.	Is any part of the processing of personal data performed through the internet?
2.	Is it possible to provide access to an internal personal data processing system through the internet (e.g. for certain users or groups of users)?
3.	Is the personal data processing system interconnected to another external or internal (to your organisation) IT system or service?
4.	Can unauthorized individuals easily access the data processing environment?
5.	Is the personal data processing system designed, implemented or maintained without following relevant best practices?

Tools a supporto dell'articolo 32 – ENISA

B. Processes/procedures related to the data processing operation	
6.	Are the roles and responsibilities with regard to personal data processing vague or not clearly defined?
7.	Is the acceptable use of the network, system and physical resources within the organisation ambiguous or not clearly defined?
8.	Are the employees allowed to bring and use their own devices to connect to the personal data processing system?
9.	Are employees allowed to transfer, store or otherwise process personal data outside the premises of the organisation?
10.	Can personal data processing activities be carried out without log files being created?

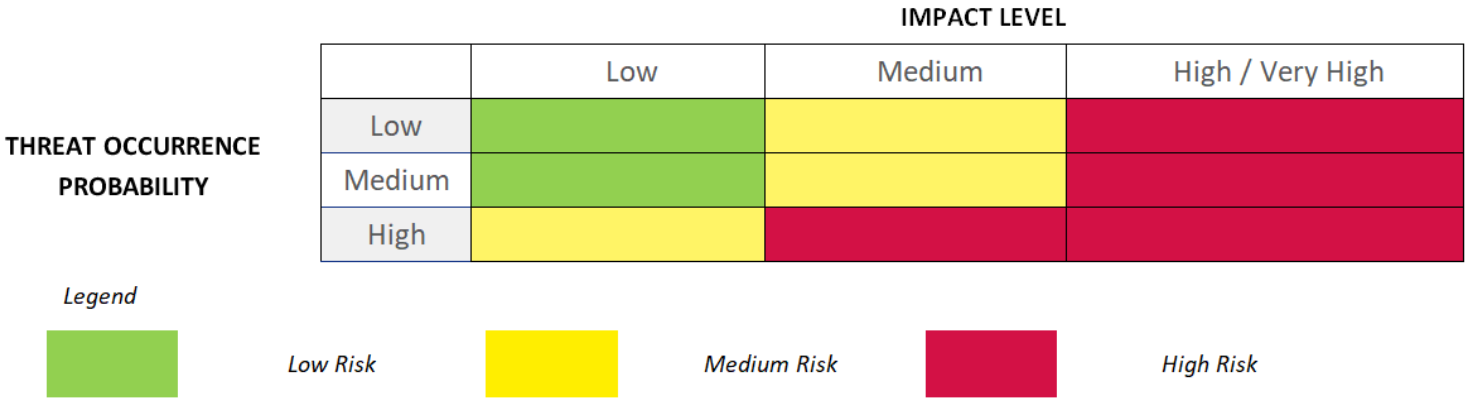
Tools a supporto dell'articolo 32 – ENISA

C. Different parties and people involved in the processing operation	
11.	Is the processing of personal data performed by a non-defined number of employees?
12.	Is any part of the data processing operation performed by a contractor/third party (data processor)?
13.	Are the obligations of the parties/persons involved in personal data processing ambiguous or not clearly stated?
14.	Is personnel involved in the processing of personal data unfamiliar with information security matters?
15.	Do persons/parties involved in the data processing operation neglect to securely store and/or destroy personal data?

Tools a supporto dell'articolo 32 – ENISA

D. Business sector and scale of the processing	
16.	Do you consider your business sector as being prone to cyberattacks?
17.	Has your organisation suffered any cyberattack or other type of security breach over the last two years?
18.	Have you received any notifications and/or complaints with regard to the security of the IT system (used for the processing of personal data) over the last year?
19.	Does a processing operation concern a large volume of individuals and/or personal data?
20.	Are there any security best practices specific to your business sector that have not been adequately followed?

Tools a supporto dell’articolo 32 - ENISA



Tools a supporto dell'articolo 32 – ENISA

Livello di rischio modificabile (particolari circostanze, giustificazione)

STEP 5: SELECTION OF APPROPRIATE SECURITY MEASURES

2 macro categorie

- Organizzative
- Tecniche
- Categorie specifiche (ISO/IEC 27001:2013 Annex A and ISO/IEC 27002:2013)

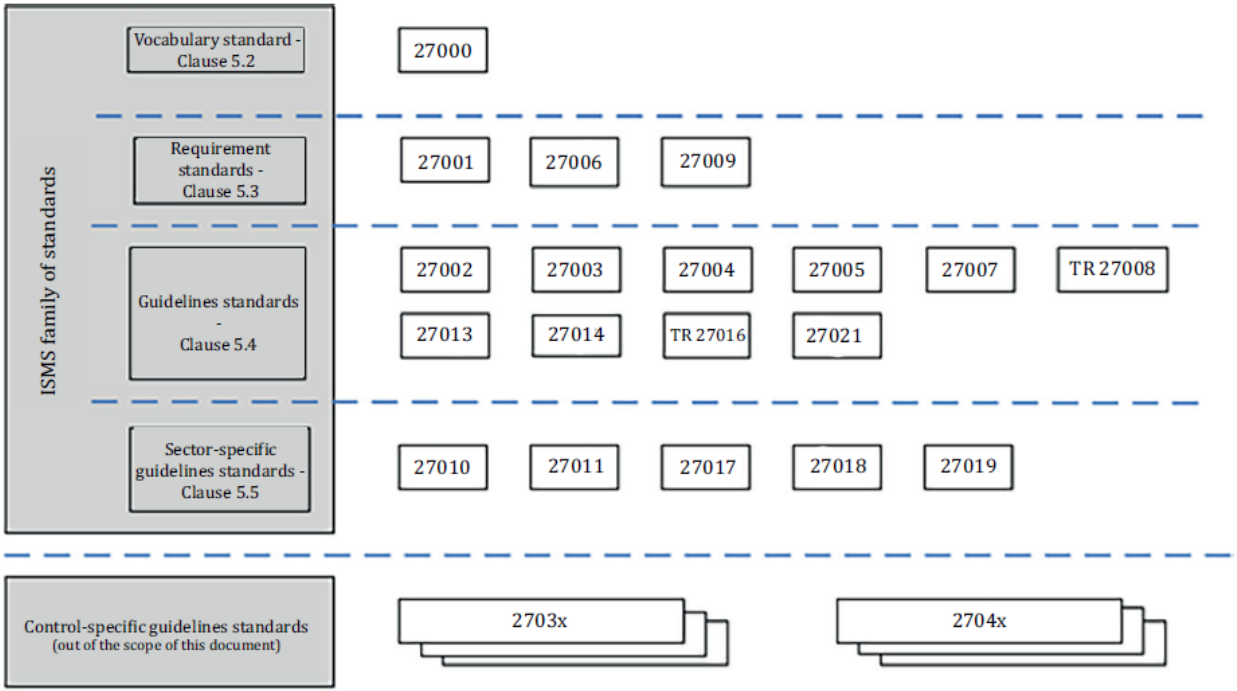
Tools a supporto dell'articolo 32 – ENISA

Organisational Security Measures Categories	Technical Security Measures Categories
Security management	**Access control and authentication**
• Security policy and procedures for the protection of personal data	**Logging and monitoring**
• Roles and responsibilities	**Security of data at rest**
• Access control policy	• Server/Database security
• Resource/asset management	• Workstation security
• Change management	**Network/Communication security**
• Data processors	**Back-ups**
Incident response and business continuity	**Mobile/Portable devices**
• Incidents handling / Personal data breaches	**Application lifecycle security**
• Business continuity	**Data deletion/disposal**
Human Resources	**Physical security**
• Confidentiality of personnel	
• Training	

Tools a supporto dell'articolo 32 – ENISA

RISK ASSESSMENT AND SECURITY MEASURE FOR PERSONAL DATA PROCESSING

Standard ISO/IEC



Standard ISO/IEC 27001

approccio PDCA

basato sul processo di gestione del rischio relativo alla sicurezza delle informazioni (riferimento ISO 31000 e ISO 27005)

il trattamento del rischio prevede diverse opzioni fra cui la mitigazione/riduzione che si realizza adottando delle **misure tecnico organizzative** (controlli) di cui la ISO 27002 può essere considerata un catalogo

SGSI

- insieme di procedure che un'organizzazione deve seguire per raggiungere i suoi obiettivi.
- comprende la struttura, i ruoli, le responsabilità, la pianificazione e la gestione dell'organizzazione
- l'ambito (scope) di un sistema di gestione può comprendere tutta l'organizzazione oppure specifiche funzioni

Standard ISO/IEC 27002:2013

Standard ISO/IEC 27002:2022

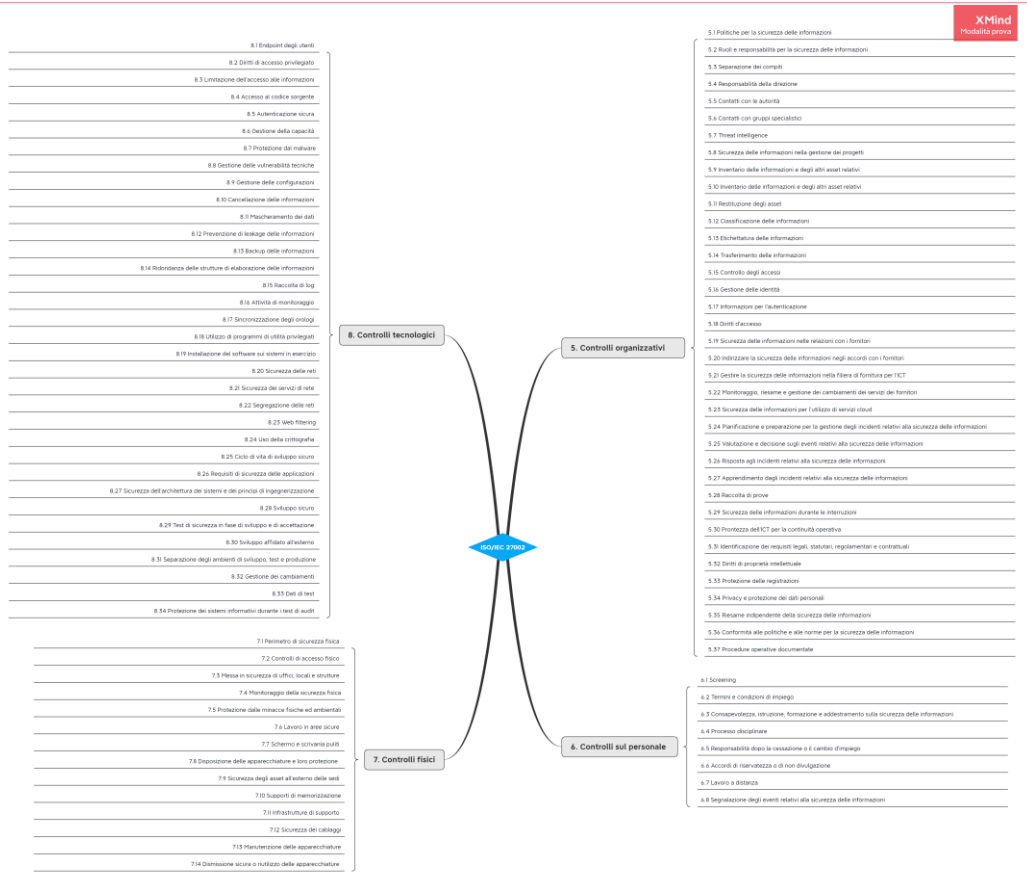
Quattro capitoli (non più 14) per i controlli:

- controlli **organizzativi**;
- controlli relativi alle **persone**;
- controlli di tipo **fisico**;
- controlli di tipo **tecnologico**

Attributi - etichette utili a selezionare i controlli:

- **tipologia di controllo**: preventivo, di rilevazione, correttivo;
- **proprietà di sicurezza**: riservatezza, integrità, disponibilità;
- **concetti di sicurezza cyber**: identificare, proteggere, rilevare, rispondere, ripristinare.
- **dominio di sicurezza**: governance ed ecosistema, protezione, difesa, resilienza
- **capacità operativa**: governance, gestione degli asset, protezione delle informazioni, sicurezza delle risorse umane, sicurezza fisica, sicurezza di sistemi e reti, sicurezza delle applicazioni, configurazione sicura, gestione di identità ed accessi, gestione di minacce e vulnerabilità, continuità, sicurezza nei rapport con i fornitori, legale e conformità, gestione degli eventi relative alla sicurezza delle informazioni, garanzie in tema di sicurezza delle informazioni

Standard ISO/IEC 27002:2022



Standard ISO/IEC 27035

ISO 27035 – 1:2023 - Principles of incident management

- Plan and prepare: policy, Incident Response Team etc.
- Detection and reporting: rilevare e riferire
- Assessment and decision: valutare l'evento e decidere se incidente
- Responses: contenimento dell'incidente
- Lessons learned: miglioramento continuo e sistematico.

ISO 27035 – 2:2023 - Guidelines to plan and prepare for incident response

- Organizzazione è pronta a rispondere in caso di incidente?
- information security and risk management Policy
- information security incident management plan
- Incident Response Team [CERT or CSIRT]
- Supporto tecnico o di altro tipo
- Consapevolezza e training
- Verifiche esercitazioni del piano
- Lesson learned

Standard ISO/IEC 27035

ISO 27035 – 3:2020 - Guidelines for incident response operations

Processi per essere pronti e rispondere a eventi e incidenti di sicurezza in ambito IT

- Common types of attacks
- Incident detection operations
- Incident notification operations
- Incident triage operations
- Incident analysis operations
- Incident containment, eradication and recovery operations
- Incident reporting operations

ISO 27035 – 4 (FDIS) - Coordination

- Coordination Team
- Principles of coordination
- Coordinated incident management process
- Guidelines for key activities of coordinated incident management
- Annex A (informative) Examples of information security incident management coordination

Qualche provvedimento

Fondazione – esfiltrazione sistema diagnostica per immagini radiografiche da gruppo hacker

- Titolare - violazione artt. 5, par. 1, lett. f) - 30.000
- Responsabile - violazione art. 32 par. 1, lett. a) – 7.000
- utilizzo di protocolli di rete non sicuri (http)
- mancata definizione di password policy (admin admin)

Comune - accesso non autorizzato portale multe

- Responsabile - violazione art. 32 par. 1, lett. a) – 10.000
- *password attribuite ad alcuni soggetti autorizzati non sottoposte a nessun controllo automatico di qualità che impedisse l'utilizzo di password "deboli" né dovevano essere obbligatoriamente modificate al primo utilizzo*
- *servizio disponibile anche su protocollo http, ossia tramite un protocollo di rete che non garantisce una comunicazione sicura sia in termini di riservatezza e integrità dei dati scambiati che di autenticità del sito web visualizzato*

Qualche provvedimento

Azienda Sanitaria - malware di tipo ransomware con esfiltrazione

- violazione artt. 5, par. 1, lett. f), 25 e 32 – sanzione 30.000
  - Mancata adozione di misure adeguate a rilevare tempestivamente la violazione dei dati personali
  - Mancata adozione di misure adeguate a garantire la sicurezza delle reti
  - protezione dei dati fin dalla progettazione

Qualche provvedimento

Provincia, responsabile e sub responsabile – FSE accesso non autorizzato ai documenti sanitari di alcuni assistiti determinato dalla vulnerabilità del servizio relativo al Fascicolo sanitario elettronico

- Titolare – misure (autorizzazione accesso ai servizi offerti dal portale) - violazione artt. 5, par. 1, lett. f), 25, 32 e 33 – sanzione 30.000
- Responsabile - violazione artt. 5, par.1, lett. f), e 32 – sanzione 10.00
- Sub – responsabile - 15.000

Ente pubblico - attacco SQLj

- Sanzione 6.000
- conservazione delle password degli utenti senza l'utilizzo di tecniche crittografiche allo stato dell'arte
- obsolescenza del software applicativo dei portali
- mancata adozione di misure di sicurezza applicativa dei portali

Grazie per l’attenzione