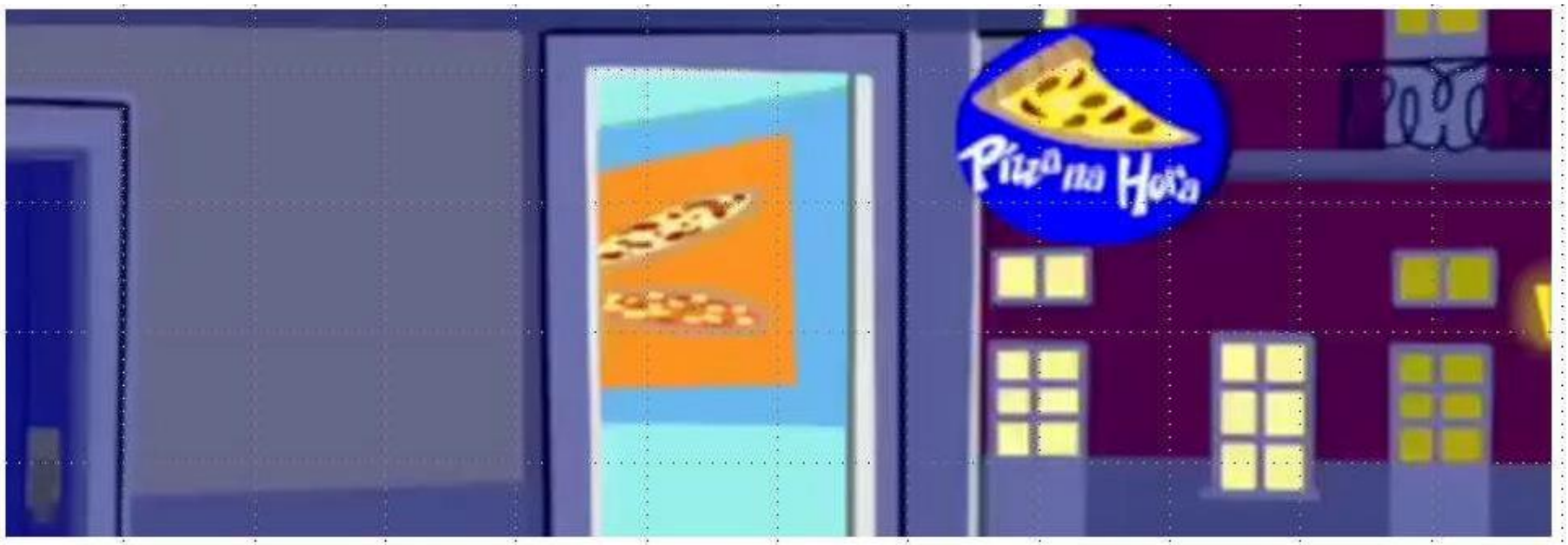
Dicembre 2018

Privacy digitale, protezione dei dati personali e sicurezza informatica

Giambattista Rosato
Esperto giuridico

… prima di tutto … una bella pizza



https://youtu.be/84Cy5fTMofY

Dateci una guardata …non è tutto vero ma manca poco!

Concetti che svilupperemo

- Regolamento Europeo 2016/679
- I nuovi ambiti di attenzione
- Titolare, Responsabile, … DPO
- To do list (cose da fare)
- Avviso ai naviganti

Regolamento Europeo 2016/679

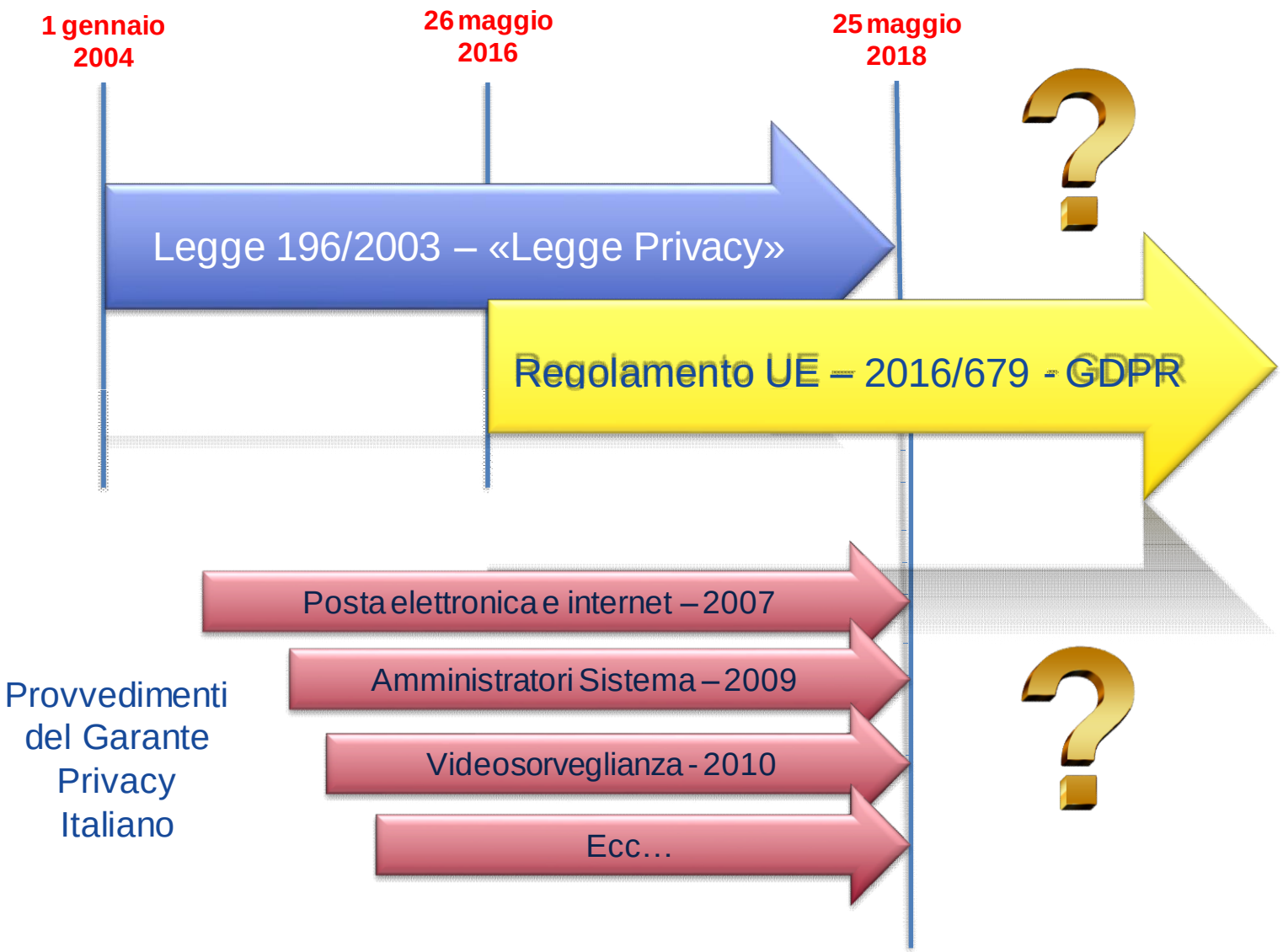
Il **4 maggio 2016**, sono stati pubblicati sulla Gazzetta Ufficiale dell'Unione Europea (GUUE) i testi del **Regolamento europeo in materia di protezione dei dati personali** (GDPR - General Data Protection Regulation) e della Direttiva che regola i trattamenti di dati personali nei settori di prevenzione, contrasto e repressione dei crimini.

Il **5 maggio 2016** è entrata ufficialmente **in vigore la Direttiva**, recepita dagli Stati membri entro 2 anni.

Il **24 maggio 2016** è entrato ufficialmente in vigore il Regolamento, che è **definitivamente applicabile in via diretta** in tutti i Paesi UE a partire dal **25 maggio 2018**.

Regolamento Europeo 2016/679 - GDPR

La fasi



Regolamento Europeo 2016/679 - GDPR

Articolo 1: Oggetto e finalità

1. *Il presente regolamento stabilisce norme relative alla* ***protezione delle persone fisiche con riguardo al trattamento dei dati personali****, nonché norme relative alla* ***libera circolazione di tali dati****.*

2. *Il presente regolamento* ***protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.***

3. ***La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata*** *per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.*

Di cosa parliamo (artt.4, 9 e 10 GDPR)

1) **« dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»);** 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; (C26, C27, C30)

2) « **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;

Di cosa parliamo: modalità di trattamento (d.lgs. 196/2003)

Il trattamento deve avvenire riducendo al minimo l'utilizzo di dati personali *(principio di necessità - articolo 3 del Codice)*, oltre che nel rispetto dei seguenti principi *(articolo 11 del Codice)*:

a. liceità e correttezza del trattamento;
b. finalità del trattamento;
c. esattezza e aggiornamento dei dati;
d. pertinenza, completezza e non eccedenza dei dati raccolti rispetto alle finalità del trattamento;
e. conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento.

Aspetti di novità – maggiore importanza

Novità

- Accountability del titolare (art. 5)
- Approccio by design & by default (art. 25)
- Obbligo di informativa e consenso (art. 13-15, art. 7-11)
- Data Retention (art. 13 comma 2.a)
- Diritto di opposizione (art. 21)
- Diritto all'oblio (art. 17)
- Portabilità dei dati (art. 20)
- Data Breach (art. 33-34)
- Registro dei trattamenti (art. 30)
- Responsabilità solidale di Titolare e Responsabile (art. 24-29)
- Sicurezza del trattamento (art. 32)
- Valutazione d'impatto sulla protezione dei dati (art. 35)
- DPO – Data Protection Officer (art. 37-39)
- Codici di condotta e certificazione (art. 40-43)
- Entità delle sanzioni (art. 83-84)

Accountability (art. 5 GDPR)

Il **principio della accountability** consiste nel dimostrare l'avvenuta adozione, in maniera chiara e non interpretabile, di tutte le misure privacy necessarie per ottemperare al rispetto del Regolamento Europeo.

To Do List

1. Censimento interno e redazione del **registro dei trattamenti**;
2. rivedere tutta **la modulistica** (es. informativa, incarichi, etc);
3. riesaminare l'impianto **ruoli privacy interni ed esterni;**
4. articolare le procedure tecniche ed organizzative per consentire **l'esercizio nei "nuovi diritti"**;
5. prevedere procedure tecniche ed organizzative per gestire un eventuale ***data breach;***
6. valutare il **trasferimento dei dati fuori dall'Unione.**

To Do List 1
Censimento interno e registro trattamenti (art. 30)

1. **Censimento interno:** partire dall'elenco dei trattamenti, che indichi le categorie dei dati trattati, chi li tratta e dove vengono trattati. In altre parole è la redazione del **registro dei trattamenti** (art. 30), che tanto ricorda il **DPS**, d'obbligo per le scuole. Così si possono definire le **attività tecniche necessarie all'adeguamento** dei sistemi e delle procedure:
   a)le misure di sicurezza adottate/da adottare, ormai svincolate da prescrizioni specifiche (le cosiddette "misure minime" previste dal Codice e dall'ALL.B, che concettualmente non esistono più) ed affidate a valutazioni di "adeguatezza ed efficacia" da parte del titolare;
   b)alla necessità o meno di dare seguito alla **valutazione d'impatto** (DPIA - art. 35 e, se del caso, *prior consultation* art. 36): con un quadro completo dei trattamenti si potrà essere in grado di verificare se sussistano o meno i presupposti per dare seguito alla valutazione d'impatto fissati. L'esclusione delle aziende sotto i 250 dipendenti dall'obbligo del registro dei trattamenti (art. 30 comma 5) sembra piuttosto virtuale: è certamente consigliabile per tutti partire comunque dal registro dei trattamenti, anche come primissimo strumento per "dimostrare" l'adempimento degli obblighi previsti dal GDPR ;

2. Il GDPR è un'opportunità per gli enti/aziende per rivedere le politiche in tema di gestione dei dati in generale, compresi quelli personali. Un'occasione per fare un controllo e mettere in ordine le cose. In molti casi è possibile che ci siano stati negli anni dei cambiamenti che sono sfuggiti al controllo, soprattutto della "privacy", che **nell'ottica del vecchio "Codice" è vista da molti solo come un obbligo burocratico.**

Registro Trattamenti (art. 30 GDPR)

È un registro, anche elettronico, all'interno del quale **il Titolare** registra i trattamenti su dati personali effettuati.
Contiene tutte le seguenti informazioni:

a) nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

Registro Trattamenti (art. 30 GDPR)

È un registro, anche elettronico, in alternativo all'interno del quale **il Responsabile** registra i trattamenti su dati personali effettuati.
Contiene tutte le seguenti informazioni:

a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

Registro/i Trattamenti (art. 30 GDPR)

Quanto importante è la corretta compilazione delle informazioni?

Queste informazioni daranno la fotografia dei trattamenti dei dati personali effettuati a soggetti interni/esterni.

•Se i dati non sono congruenti al comportamento danno origine a confusione e possibili sanzioni

•Se i dati non sono corretti il Titolare non ha la sensazione vera dei livelli di rischio e potrebbe comportarsi in maniera non coerente rispetto al rischio

To Do List 2
Rivedere la modulistica (es. informativa, incarichi,etc)

A)Informativa ai dipendenti, agli alunni, ai fornitori, agli esperti esterni, etc, visto che gli artt. 13 e 14 GDPR introducono degli elementi nuovi (per es. base giuridica del trattamento; tempi di conservazione etc.), che nessuno fino a oggi poteva aver considerato;

B)Nomina di Responsabile del trattamento, Incaricato del trattamento, Amministratore con le allegate "istruzioni";

C)Consenso, <u>che la scuola non deve chiedere mai</u> , solo in caso che il trattamento non sia previsto dalla legge (es. elenchi alunni diplomati inviati a imprese per collocamento diplomati) sempre formale/per iscritto, nonostante il nuovo concetto di "*azione positiva inequivocabile*" per gli uni e di consenso "*esplicito*" per gli altri.

To Do List 3
Riesaminare l'impianto dei ruoli privacy interni ed esterni

Tenere conto:
a)del superamento del concetto di "*designazione*" del **responsabile del trattamento**, lo sostituisce con quello di **"contratto o altro atto giuridico"**, e soprattutto consente ad un responsabile di "ricorrere" ad un sub-responsabile (art. 28 GDPR);
b)del superamento del concetto di "*designazione*" degli **incaricati**, essendo onere del titolare (e del responsabile) esclusivamente quello di **"istruire"** coloro che operano sotto la loro autorità (art. 29 GDPR);
c)della necessità o meno di designare un Data Protection Officer (DPO o in italiano RPD), figura obbligatoria solo per le P.A. (art. 37 GDPR) ... ma per la scuola, ad oggi, non obbligatoria;
d)il titolare deve adottare "misure adeguate" e dovrà dimostrare quali misure ha adottato e perché: non è quindi una mera indicazione burocratica, occorre documentare tutto. Dovrà pertanto progettare – e dimostrare - misure di sicurezza adeguate al rischio, sulla base della "valutazione dell'impatto"...

Data Protection Officer (art. 37-39 GDPR)

Chi è:

Il Data Protection Officer è una figura storicamente già presente in alcune legislazioni europee ed è un professionista che deve avere un ruolo (sia esso soggetto interno o esterno) con competenze giuridiche, informatiche, di risk management e di analisi dei processi.

Cosa fa:

La sua responsabilità principale è quella di: osservare, valutare, indicare, formare e organizzare la gestione del trattamento di dati personali (e dunque la loro protezione) all'interno di un ente pubblico, affinché questi siano trattati nel rispetto delle normative privacy europee e nazionali

Che ruolo attivo ha:

Ha il ruolo di assistenza e consiglio rispetto all'applicazione delle normative sul trattamento dei dati personali da parte dell'organizzazione; verifica il rispetto delle regole evidenziando eventuali situazioni di non conformità (audit); si fa parte diligente rispetto all'organizzazione nel divulgare le norme al fine di rendere responsabile l'organizzazione rispetto all'attuazione

Posizione organizzativa:

Risponde ai vertici dell'organizzazione con un alto grado di autonomia e il più possibile libero da vincoli che possano condizionare le sue indicazioni sulla tematica

Data Protection Officer (art. 37-39 GDPR)

E':

•Il riferimento del Titolare per le indicazioni sul tema;
•Il riferimento degli Interessati che vogliano conoscere il trattamento sui loro dati o abbiano riserve sull'argomento;
•Il riferimento per l'Autorità di Controllo a fronte di necessità;
•Il supporto attivo dell'Organizzazione in fase di progettazione di nuovi sistemi o l'avvio di nuovi trattamenti.

NON è:

•Il referente del Titolare rispetto al trattamento dei dati personali;
•Il responsabile/custode del Registro dei trattamenti;
•Colui che ricopre un ruolo operativo per calare sull'organizzazione le indicazioni del DPO.

Può essere:

•Dipendente dell'Ente ma anche un incaricato esterno (con PRO e CONTRO), soggetto fisico o soggetto giuridico.

Sicurezza per i trattamenti con strumenti elettronici (ALL. B Codice Privacy 196/2003)

Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto, le seguenti misure minime:

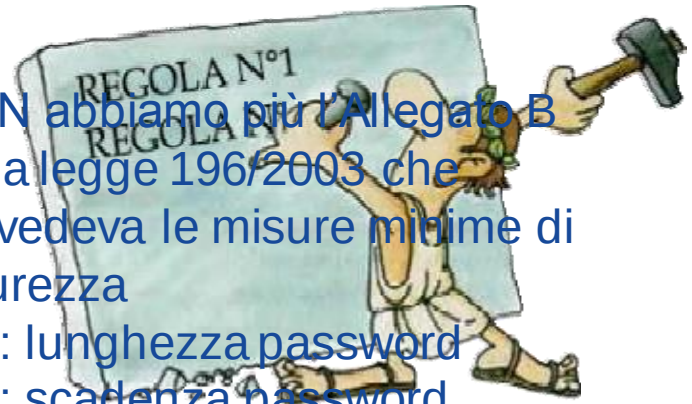
a) autenticazione informatica;
b) adozione di procedure di gestione delle credenziali di autenticazione;
c) utilizzazione di un sistema di autorizzazione;
d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
g) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Sicurezza del trattamento (art. 32 GDPR)

NON abbiamo più l'Allegato B della legge 196/2003 che prevedeva le misure minime di sicurezza

- Es: lunghezza password
- Es: scadenza password

Sulla base delle nuove regole normative dobbiamo analizzare i rischi definendo le regole adatte alla loro eliminazione o contenimento



NON abbiamo più l'Allegato B della legge 196/2003 che prevedeva le misure minime di sicurezza

- Es: lunghezza password
- Es: scadenza password

Sicurezza del trattamento (art. 32 GDPR)

Sulla base delle nuove regole normative dobbiamo analizzare i rischi definendo le regole adatte alla loro eliminazione o contenimento

NON abbiamo più l'Allegato B della legge 196/2003 che prevedeva le misure minime di sicurezza

- Es: lunghezza password
- Es: scadenza password

Adozione di misure tecniche e organizzative adeguate ... regolamento del MIUR, come in passato??

Sicurezza del trattamento (art. 32 GDPR)

*… che comprende, **tra le altre**, se del caso:*

- Cifratura (art. 34 – considerando 83)
- Anonimizzazione (considerando 26 – parere 5/2014)
- Capacità di
  1. assicurare la continua **riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi** che trattano i dati personali;
  2. **ripristinare tempestivamente** la disponibilità e l'accesso dei dati in caso di incidente fisco o tecnico;
- Procedura per **provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative** al fine di garantire la sicurezza del trattamento

To Do List 4

Articolare le procedure tecniche ed organizzative per consentire l'esercizio nei "nuovi diritti"

In attesa delle regole italiano, bisogna tenere conto del necessario **esercizio nei "nuovi diritti"** previsti dal GDPR in capo all'interessato, con specifico riferimento alla:

- cancellazione/oblio, da estendere *urbi et orbi* (art. 17 comma 2 GDPR);
- limitazione del trattamento, cioè un contrassegno che identifichi i dati a trattamento limitato (art. 18 GDPR);
- portabilità dei dati (formato interoperabile di uso comune – art. 20 GDPR);
- opposizione alla profilazione ed ai trattamenti automatizzati.

To Do List 5

Prevedere procedure tecniche ed organizzative per gestire un eventuale *data breach*

Tre passi:

1. verificare la rispondenza alle misure della Circ. AgID 18.04.2017, n. 2 "*Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)*".

2.la valutazione delle vulnerabilità (*vulnerability assessment*) è necessaria sui sistemi in generale e sui singoli sottosistemi.

3.tutti gli aspetti tecnici vanno ricontrollati e su ciascuno di essi va fatta un'analisi dei rischi.

... quindi si deve decidere se le misure già implementate siano da considerarsi adeguate o meno.

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI … e altre 12 pagine modello AgID

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

Data Breach (artt 33-34 GDPR)

incidente di sicurezza in cui **dati sensibili, protetti o riservati** vengono: **consultati, copiati, alterati, trasmessi, rubati o utilizzati da un soggetto non autorizzato**.

Il data breach si realizza con una divulgazione di dati riservati o confidenziali all'interno di un ambiente privo di misure di sicurezze (ad esempio sul web) in maniera involontaria o volontaria.

Tale divulgazione può avvenire in seguito a:

- **perdita accidentale:** ad esempio, data breach causato da smarrimento di una chiavetta USB contenente dati riservati
- **furto:** ad esempio, data breach causato da furto di un notebook contenente dati confidenziali
- **infedeltà aziendale:** ad esempio, data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico
- **accesso abusivo:** ad esempio, data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite (fonte Bit4Law)
- il garante ha annunciato che pubblicherà un modulo, per i fornitori di servizi di comunicazioni elettroniche che, unici nella attuale disciplina del Codice Privacy, sono tenuti ad oggi a notificare una violazione di dati.

To Do List 6
Valutare il trasferimento dei dati fuori dall'Unione

Valutare quali leve utilizzare tra quelle previste dal GDPR (valutazione di adeguatezza, *binding corporate rules* etc).
Ad oggi, il trasferimento di dati personali verso Paesi non appartenenti all'UE è possibile **quando**:
- ricorre una delle condizioni previste dall' *articolo 43* del Codice Privacy 196/2003 - oppure, è autorizzato dal Garante per la protezione dei dati personali sulla base di adeguate garanzie per i diritti dell'interessato *(articolo 44 del Codice* Privacy 196/2003*)*
Fuori da questi casi, il trasferimento è vietato quando l'ordinamento del Paese di destinazione o di transito dei dati personali non assicura un livello adeguato di tutela delle persone *(articolo 45 del Codice* Privacy 196/2003*)*.

Il trasferimento di dati personali effettuato in violazione dell'articolo 45 del Codice* Privacy 196/2003 *è punito con la sanzione amministrativa del pagamento di una somma da diecimila euro a centoventimila euro (articolo 162,comma 2 bis del Codice* Privacy 196/2003 *).

Sanzioni (art. 83-84 GDPR)

Violazione	Sanzione
Consenso dei minori (art. 8)	Fino a 10.000.000 Euro, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore
Trattamento che non richiede l'identificazione (art.11)	
Privacy by design/default (art.25)	
Contitolarità (art.26)	
Responsabile del trattamento (art.28)	
Soggetti che trattano dati (art. 29)	
Registro delle attività (art. 30)	
Cooperazione con Autorità (art. 31)	
Sicurezza (art. 32)	
Notifica di violazione (art. 33)	
Comunicazione di violazione (art. 34)	
Valutazione d'impatto (art. 35)	
Consultazione preventiva (art. 36)	
Designazione DPO (art. 37)	
Posizione DPO (art. 38)	
Compiti DPO (art. 39)	

Sanzioni (art. 83-84 GDPR)

Violazione	Sanzione
Principi applicabili al trattamento: correttezza, trasparenza, ecc (art. 5)	Fino a 20.000.000 Euro, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore
Liceità del trattamento: consenso, finalità, ecc (art. 6)	
Condizioni per il consenso (art. 7)	
Trattamento di categorie particolari di dati (art. 9)	
Informazioni trasparenti per l'esercizio dei diritti (art.12)	
Informazioni su dati non ottenuti presso interessato (art. 15)	
Diritto di accesso dell'interessato (art. 15)	
Diritto di rettifica (art. 16)	
Diritto di cancellazione «diritto all'oblio» (art. 17)	
Diritto di limitazione del trattamento (art. 18)	
Obbligo di notifica rettifica, cancellazione o limitazione (art. 19)	
Diritto alla portabilità dei dati (art. 20)	
Diritto di opposizione (art. 21)	
Processo decisionale automatizzato (art. 22)	
Trasferimento di dati paese terzo o org. Internazionale (art. 44-49)	

DOMANDE??????

Grazie dell’attenzione e buon divertimento