GDPR UE 2016/679
IL REGOLAMENTO EUROPEO SULLA PROTEZIONE DEI DATI PERSONALI

30 MARZO 2022

UNI
UN MONDO FATTO BENE

Con il patrocinio di
ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO

UNITRAIN
Conoscere e applicare gli standard

PRESENTAZIONE

A seguito dell'adozione del Regolamento europeo sulla protezione dei dati personali (GDPR 679/2016), armonizzato dal Decreto legislativo 101/2018 con il vigente Codice della Privacy (Decreto legislativo 196/2003), le aziende, gli enti, i professionisti e le pubbliche amministrazioni sono tenuti ad adeguarsi alla nuova normativa europea e ad aggiornare tutte le procedure in materia (principio dell'accountability).
La materia è in continua evoluzione e sono molti i provvedimenti del Garante sui diversi e importanti aspetti oggetto della normativa: è quindi sempre il momento giusto per formarsi.

OBIETTIVI

Far acquisire al partecipante, attraverso l'analisi di casi ed esempi concreti, i nuovi concetti e gli strumenti che gli consentiranno di attuare un "sistema di gestione privacy" adeguato alla propria organizzazione e conforme ai nuovi dettami europei.

DESTINATARI

Titolari e responsabili trattamento dati, responsabili amministrativi (di PMI o di associazioni di categoria delle piccole e medie imprese), amministratori di sistema e informatici aziendali, professionisti e addetti agli adeguamenti normativi aziendali (legale e funzione compliance), consulenti aziendali, auditor.

DOCENTE

FRANCESCA MARCHINI - Legale Formatore qualificato e consulente esperto per la privacy. Ispettore ACCREDIA

GDPR e MODELLI DI ADEGUAMENTO

GDPR: obiettivi, disciplina e modelli di adeguamento aziendali

Fonti normative disciplina Privacy GDPR e normativa italiana di riferimento: interazioni

Obiettivi, Logiche e Principi del GDPR

«Codice Privacy e GDPR»: principali elementi a confronto

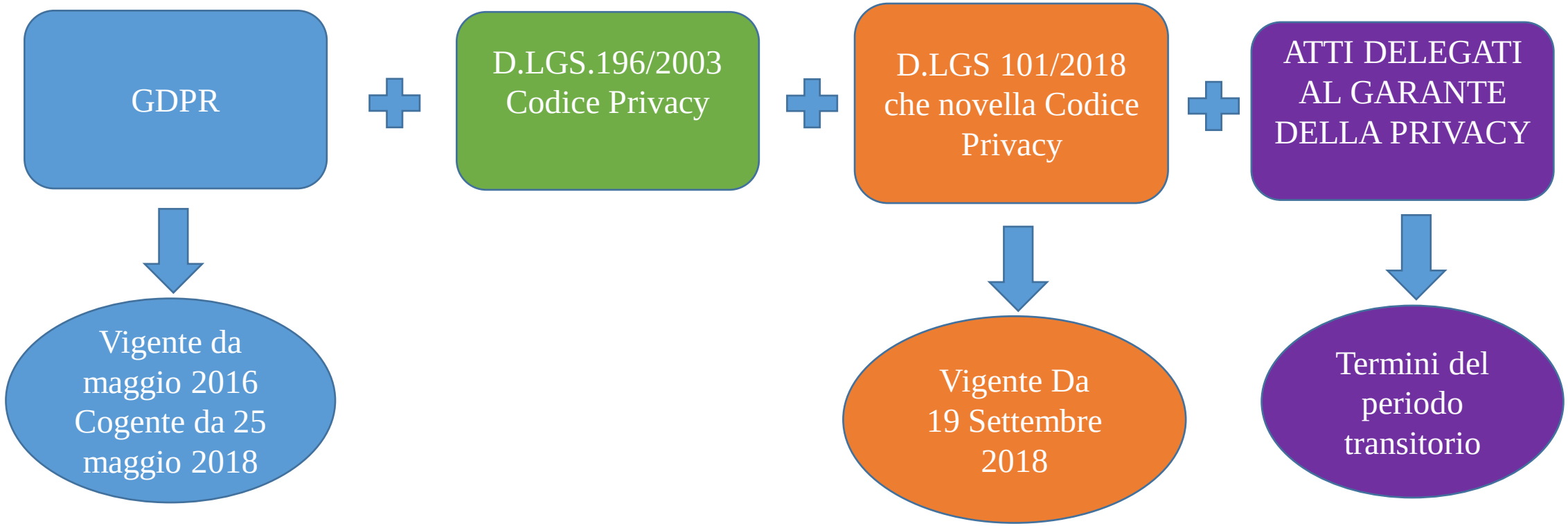
Sintesi novità del GDPR

Modello di adeguamento aziendale: elementi portanti

Zoom su elementi portanti spesso critici nelle organizzazioni

Conclusioni

Fonti normative disciplina Privacy GDPR e normativa italiana di riferimento: interazioni



Obiettivi, Logiche e Principi del GDPR

«Codice Privacy e GDPR»: principali elementi a confronto

DEFINIZIONI

Le principali definizioni delle due normative sono:

- **TRATTAMENTO DI DATI PERSONALI**
- **CLASSIFICAZIONE DI DATI PERSONALI**
- **SOGGETTI E RUOLI**

«Codice Privacy e GDPR»: principali elementi a confronto

TRATTAMENTO

Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, processi automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la strutturazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la limitazione, la cancellazione e la distruzione dei dati, anche se non registrati in una banca dati.

«Codice Privacy e GDPR»: principali elementi a confronto

CLASSIFICAZIONE DEI DATI

Personali: qualunque informazione relativa alla persona fisica, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale

Comuni: tutti i dati che non sono Sensibili o Giudiziali: nome, indirizzo, numero di identificazione, identificativo online..

«Sensibili»: Categorie particolari di dati personali: i dati personali idonei a rilevare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita e orientamento sessuale, dati biometrici e genetici (Art.9 del GDPR)

Giudiziali: I dati personali idonei a rivelare provvedimenti in materia di casellario giudiziario, di anagrafe delle sanzioni amministrative dipendenti da reato e relativi carichi pendenti: «*relativi alle condanne penali e ai reati o a connesse misure di sicurezza*..» (Art.10 del GDPR)

«Codice Privacy e GDPR»: principali elementi a confronto

SOGGETTI E RUOLI

Il Titolare

E' l'entità cui competono le decisioni in ordine alla finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza e la capacità di dimostrarne la conformità al Regolamento.

Il Contitolare: due titolari con competenze ripartire regolate da un accordo di contitolarità.

Il Responsabile

E' l'entità preposta dal titolare al trattamento di dati personali.

- Nomina facoltativa
- Possono essere designati più soggetti
- I compiti sono specificati per iscritto dal titolare.

Il Sub responsabile: il Soggetto delegato dal responsabile al trattamento dei dati personali.

SINTESI NOVITA' DEL GDPR

- La previsione delle figure dei «**joint controllers**» **(titolari congiunti),** che potranno «spartirsi» le responsabilità privacy in un apposito contratto, di cui si dovrà tenere conto in caso di controlli o contenziosi: questa novità sarà d'aiuto, in particolare, nel settore del cloud computing providing (fino ad oggi difficilmente inquadrabile nei vecchi schemi titolare/ responsabile)
- La previsione del concetto di «**stabilimento principale**» del titolare, per evitare che un'impresa attiva in più Stati EU debba fronteggiare gli adempimenti nazionali di ogni singolo Stato
- La previsione del ruolo di «**lead authority**», in modo tale che vi sia un solo Garante di volta in volta responsabile dei procedimenti multi – Stato

NEW

SINTESI NOVITA' DEL GDPR

- L'introduzione del principio della cosiddetta «**accountability**», per il quale ogni titolare, in caso di problemi o controlli, dovrà dimostrare nei fatti, al di là dei formalismi, di avere adottato i modelli organizzativi e le misure logiche, fisiche, elettroniche di sicurezza per proteggere i dati (onere della prova) – questo porterà a dover **creare un sistema documentale di gestione della privacy.**

LA VERA RIVOLUZIONE

NEW

SINTESI NOVITA' DEL GDPR

- L'obbligo di attenersi, nell'ideazione di nuovi prodotti o servizi, ai principi della «**data protection by design**» e della «**data protection by default**»
- La creazione **di codici di condotta nazionali** da definire come **schemi di certificazione** e sottoposti a verifiche da parte di Enti di Certificazione Accreditati
- **Sanzioni:** massimali di sanzioni decuplicati.

SINTESI NOVITA' DEL GDPR

Articolo 6 Liceità del trattamento

1.Il trattamento dei dati personali **è lecito solo se e nella misura in** cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

b) il trattamento **è necessario all'esecuzione di un contratto** di cui l'interessato è parte o all'esecuzione di misure precontrattuali prese su richiesta dello stesso;

c) il trattamento **è necessario per adempiere un obbligo legale** al quale è soggetto il titolare del trattamento;

d) il trattamento **è necessario per la salvaguardia degli interessi vitali** dell'interessato o di un'altra persona fisica;

e) il trattamento **è necessario per l'esecuzione di un compito di interesse pubblico** o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento **è necessario per il perseguimento del legittimo interesse del titolare** del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

SINTESI NOVITA' DEL GDPR

Articolo 7 Condizioni per il consenso

1. Qualora il trattamento sia basato sul consenso, **il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali**.

2. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso **è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.** Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.

3**. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento**. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.

4. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

SINTESI NOVITA' DEL GDPR

Articolo 8 Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione

1. Qualora si applichi l'articolo 6, paragrafo 1, lettera a), per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni**. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale. Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni.**

2. Il titolare del trattamento si adopera in ogni modo ragionevole per verificare in tali casi che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili.

3. Il paragrafo 1 non pregiudica le disposizioni generali del diritto dei contratti degli Stati membri, quali le norme sulla validità, la formazione o l'efficacia di un contratto rispetto a un minore.

SINTESI NOVITA' DEL GDPR

Articolo 9 Trattamento di categorie particolari di dati personali

1. È vietato trattare 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.

2. Il paragrafo 1 **non si applica se si verifica** uno dei seguenti casi:

a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1;

b) il **trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale** e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;

c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

SINTESI NOVITA' DEL GDPR

d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;

e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;

f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;

g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;

h) il 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 sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3;

COSA CAMBIA?
Estensione dei dati particolari e definizioni sui dati genetici e biometrici

Articolo 9 Trattamento di categorie particolari di dati personali

1. È vietato trattare 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.

SINTESI NOVITA' DEL GDPR

Articolo 10 Trattamento dei dati personali relativi a condanne penali e reati

Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.

SINTESI NOVITA' DEL GDPR

Articolo 11 Trattamento che non richiede l'identificazione

1. Se le finalità per cui un titolare **del trattamento tratta i dati personali non richiedono o non richiedono più l'identificazione dell'interessato, il titolare del trattamento non è obbligato a conservare, acquisire o trattare ulteriori informazioni per identificare l'interessato al solo fine di rispettare il presente regolamento.**

2. Qualora, nei casi di cui al paragrafo 1 del presente articolo, il titolare del trattamento possa dimostrare di non essere in grado di identificare l'interessato, ne informa l'interessato, se possibile. In tali casi, gli articoli da 15 a 20 non si applicano tranne quando l'interessato, al fine di esercitare i diritti di cui ai suddetti articoli, fornisce ulteriori informazioni che ne consentano l'identificazione.

SINTESI NOVITA' DEL GDPR

CAPO III DIRITTI DELL'INTERESSATO SEZIONE 1 TRASPARENZA E MODALITÀ

Articolo 12 Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato

1. Il titolare del trattamento adotta misure appropriate **per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.** Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

2. **Il titolare del trattamento agevola l'esercizio** dei diritti dell'interessato ai sensi degli articoli da 15 a 22. Nei casi di cui all'articolo 11, paragrafo 2, il titolare del trattamento non può rifiutare di soddisfare la richiesta dell'interessato al fine di esercitare i suoi diritti ai sensi degli articoli da 15 a 22, salvo che il titolare del trattamento dimostri che non è in grado di identificare l'interessato.

SINTESI NOVITA' DEL GDPR

3. **Il titolare del trattamento fornisce all'interessato le informazioni** relative all'azione intrapresa riguardo a una richiesta ai sensi degli articoli da 15 a 22 senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Il titolare del trattamento informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta. Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato.

4. **Se non ottempera alla richiesta dell'interessato, il titolare del trattamento informa l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale.**

5. Le informazioni fornite ai sensi degli articoli 13 e 14 ed eventuali comunicazioni e azioni intraprese ai sensi degli articoli da 15 a 22 e dell'articolo 34 sono gratuite. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento può:
a) **addebitare un contributo spese ragionevole** tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; oppure
b) **rifiutare di soddisfare la richiesta**.

Incombe al titolare del trattamento l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

SINTESI NOVITA' DEL GDPR

6. Fatto salvo l'articolo 11, qualora il titolare del trattamento nutra ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta di cui agli articoli da 15 a 21, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato.

7. **Le informazioni da fornire agli interessati a norma degli articoli 13 e 14 possono essere fornite in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone sono leggibili da dispositivo automatico.**

8. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 92 al fine di stabilire le informazioni da presentare sotto forma di icona e le procedure per fornire icone standardizzate.

SEZIONE 2 **INFORMAZIONE E ACCESSO AI DATI**

Articolo 13 Informazioni da fornire qualora i dati siano raccolti presso l'interessato

1. In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:

a) **l'identità e i dati di contatto del titolare del trattamento** e, ove applicabile, del suo rappresentante;

b) i dati di contatto del **responsabile della protezione dei dati**, ove applicabile;

c) **le finalità del trattamento** cui sono destinati i dati personali nonché la **base giuridica** del trattamento;

d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), **i legittimi interessi** perseguiti dal titolare del trattamento o da terzi;

e) gli **eventuali destinatari o le eventuali categorie di destinatari** dei dati personali;

f) ove applicabile, l'intenzione del titolare del trattamento di **trasferire dati personali a un paese terzo** o a **un'organizzazione internazionale** e **l'esistenza o l'assenza di una decisione di adeguatezza della Commissione** o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, **il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili**.

SINTESI NOVITA' DEL GDPR

SEZIONE 2 **INFORMAZIONE E ACCESSO AI DATI**

2. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie **per garantire un trattamento corretto e trasparente:**

a) il **periodo di conservazione dei dati personali** oppure, se non è possibile, **i criteri utilizzati per determinare tale periodo;**
b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento **l'accesso ai dati** personali e **la rettifica** o **la cancellazione degli stessi** o **la limitazione del trattamento** che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), **l'esistenza del diritto di revocare il consenso in qualsiasi momento** senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
d) il **diritto di proporre reclamo** a un'autorità di controllo;
e) se **la comunicazione di dati personali è un obbligo legale o contrattuale** oppure un **requisito necessario per la conclusione di un contratto**, e **se l'interessato ha l'obbligo di fornire i dati personali** nonché **le possibili conseguenze della mancata comunicazione di tali dati;**

SINTESI NOVITA' DEL GDPR

SEZIONE 2 **INFORMAZIONE E ACCESSO AI DATI**

f) **l'esistenza di un processo decisionale automatizzato**, compresa **la profilazione** di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi**, informazioni significative sulla logica utilizzata**, **nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato**.

3. Qualora il titolare del trattamento intenda trattare ulteriormente **i dati personali per una finalità diversa** da quella per cui essi sono stati raccolti, **prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2.**

4. […]

Informative

Un concetto fondamentale ed importante della normativa è: se tratto i dati di un soggetto devo informarlo di cosa ne faccio....

- Identificazione dei soggetti esterni
  - Clienti
  - Fornitori
  - Dipendenti
- Identificazione degli ambiti
  - Contatti commerciali per clienti e fornitori
  - Nuovi sistemi di contatto: siti internet, mailing, web marketing
  - Procedure di assunzione per i dipendenti

Consenso

Qualsiasi manifestazione di volontà **libera, specifica, informata e inequivocabile** dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento

Deve seguire sempre l'informativa e prima del trattamento

Titolare deve **dimostrare** di aver acquisito il consenso

Il consenso può essere revocato in qualsiasi momento, prima di esprimere il proprio consenso l'interessato è informato di questo diritto.

SINTESI NOVITA' DEL GDPR

Contenuto minimo contratto tra Titolare e Responsabile: art. 28

Adempimenti base del Responsabile del trattamento

- Trattare i dati secondo le istruzioni scritte del Titolare
- Garantire che le persone autorizzate al trattamento siano tenute all'obbligo di riservatezza
- Adottare le misure di sicurezza del trattamento
- Acquisire autorizzazione scritta del Titolare per nominare dei sub-responsabili
- Definire nel contratto con sub-responsabile stessi obblighi esistenti nel contratto con il Titolare
- Assistere il Titolare con misure tecniche e organizzative adeguate, ove possibile, per garantire l'esercizio dei diritti interessato da parte del Titolare e nella sicurezza del trattamento e nella consultazione preventiva
- Terminata la prestazione, secondo richiesta del Titolare :cancellare o restituire i dati, cancellare le copie, sempre nel rispetto degli obblighi di legge
- Mettere a disposizione del Titolare tutte le evidenze necessarie a dimostrare la conformità al contratto
- Consentire e contribuire alle ispezione del Titolare e di soggetto da questo incaricato.

Articolo 29 Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento

Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Articolo 30 Registri delle attività di trattamento

1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

a) il 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;

SINTESI NOVITA' DEL GDPR

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**.**

2. **Ogni responsabile del trattamento** e, ove applicabile, il suo rappresentante tengono un **registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente**:

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;

SINTESI NOVITA' DEL GDPR

d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

3 I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico..

4. **Su richiesta**, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento **mettono il registro a disposizione dell'autorità di controllo**.

5. Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni **con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato**, **il trattamento non sia occasionale** o **includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.**

COSA CAMBIA?

I registri dei trattamenti

Base della valutazione dei rischi

Il Responsabile deve avere un registro per il trattamento dei dati per conto di ogni Titolare

SEZIONE 2 SICUREZZA DEI DATI PERSONALI

Articolo 32 Sicurezza del trattamento

1 Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del **rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative a**deguate per garantire un **livello di sicurezza adeguato al rischio**, che comprendono, tra le altre, se del caso:

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.

SINTESI NOVITA' DEL GDPR

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special **modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.**

3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.

4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

ZOOM DISCIPLINA DEL DPO: Artt. 37, 38 e 39

Articolo 37: DESIGNAZIONE DEL DPO

Responsabile della protezione dei dati

Articolo 37

Designazione del responsabile della protezione dei dati

1. Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:

a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure

c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

Articolo 37 (continua)

Articolo 37: DESIGNAZIONE DEL DPO

2. Un gruppo imprenditoriale può nominare un unico responsabile della protezione dei dati, a condizione che un responsabile della protezione dei dati sia facilmente raggiungibile da ciascuno stabilimento.

3. Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.

4. Nei casi diversi da quelli di cui al paragrafo 1, il titolare e del trattamento, il responsabile del trattamento o le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento possono o, se previsto dal diritto dell'Unione o degli Stati membri, devono designare un responsabile della protezione dei dati. Il responsabile della protezione dei dati può agire per dette associazioni e altri organismi rappresentanti i titolari del trattamento o i responsabili del trattamento.

5. Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39.

6. Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.

7. Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo.

Articolo 38: POSIZIONE DEL DPO

Articolo 38

Posizione del responsabile della protezione dei dati

1. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

2. Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.

3. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.

4 Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.

5. Il responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri.

6. Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi.

Articolo 39: COMPITI DEL DPO

Articolo 39

Compiti del responsabile della protezione dei dati

1. Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;

d) cooperare con l'autorità di controllo; e

e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

2. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Le sanzioni: art. 83

PRINCIPIO:

Le sanzioni irrogate devono essere: **effettive, proporzionate e dissuasive**

Criteri di irrogazione. Alcuni criteri:

- la **natura, la gravità e la durata della violazione**
- **carattere doloso o colposo**
- **misure adottate dal titolare del trattamento o dal responsabile** del trattamento per attenuare il danno subito dagli interessati
- **misure tecniche e organizzative da essi messe in atto**
- **precedenti violazioni pertinenti**
- **grado di cooperazione con l'autorità di controllo** per porre rimedio/ attenuare effetti negativi
- **categorie di dati personali** interessate dalla violazione..

Le sanzioni: art. 83

4. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 10 000 000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

a) gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8 (consenso dei minori), 11 (trattamento che non richiede l'identificazione), da 25 a 39 (titolare, responsabile, registri delle attività, sicurezza del trattamento, data breach, comunicazioni all'interessato, DPO), 42 e 43;

b) gli obblighi dell'organismo di certificazione a norma degli articoli 42 e 43;

c) gli obblighi dell'organismo di controllo a norma dell'articolo 41, paragrafo 4;

5. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

a) i principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5 («liceità, correttezza e trasparenza», limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza, responsaabilizzazione) 6 (liceità del trattamento), 7 (condizioni consenso: dimostrabilità, chiarezza, inequivocabilità, revocabilità) e 9 (trattamento di categorie particolari di dati);

b) i diritti degli interessati a norma degli articoli da 12 a 22;

c) i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49;

Le sanzioni: art. 83

d) qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX;

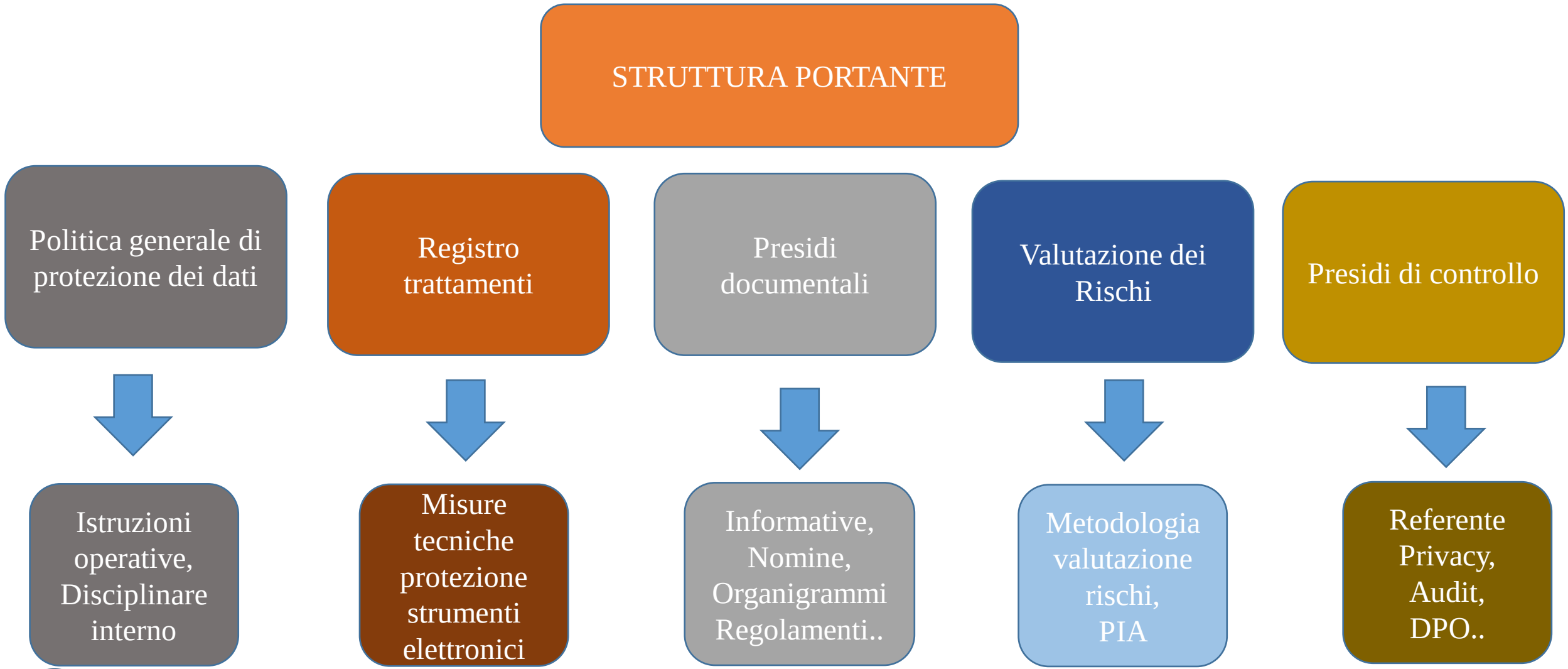
e) l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1.

6. In conformità del paragrafo 2 del presente articolo, l'inosservanza di un ordine da parte dell'autorità di controllo di cui all'articolo 58, paragrafo 2, è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

7. Fatti salvi i poteri correttivi delle autorità di controllo a norma dell'articolo 58, paragrafo 2, ogni Stato membro può prevedere norme che dispongano se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti in tale Stato membro.

8-9 …

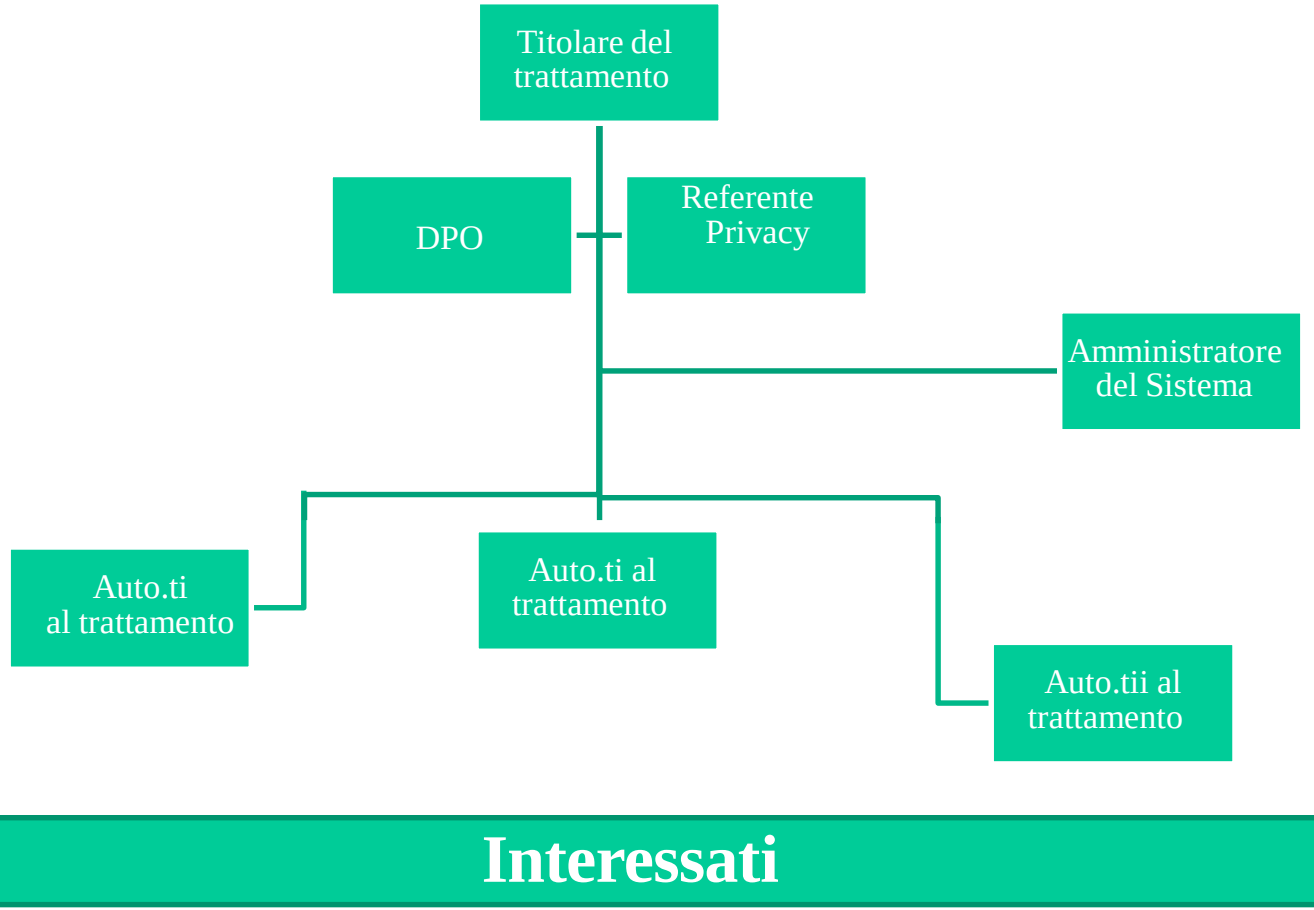
GDPR e Modello di adeguamento aziendale



Gestire il sistema privacy in 15 punti

- Analisi del Sistema e contestualizzazione nel «business» dell'organizzazione
- Analisi dei rischi
- Analisi della sicurezza
- Analisi dei flussi e del tipo dei dati
- Gestione documentale
- Controllo documentale
- Controllo ed aggiornamento normativo /legislativo
- Controllo «informatico» : log, web, cookies…
- Effettuare Audit
- Interfacciarsi con tutti i livelli organizzativi e offrire loro supporto
- Relazionarsi con le istituzioni
- Formare il personale
- Redigere il rapporto Privacy
- Informare il Titolare e i Responsabili
- Diffondere la cultura «Privacy»

Organigramma privacy - posizionamento DPO



GDPR e Modello di adeguamento aziendale

ZOOM STRUTTURA PORTANTE

Registro trattamenti e procedura di gestione

Politica generale di protezione dei dati- disciplinare interno

NB: chiare regole scritte interne: chi fa cosa, come e perché

Presidi organizzativi: flussi titolare, designati, autorizzati interni ed esterni, responsabili ex art.28, contitolari (se), subresponsabili (se) Organigrammi Privacy

Presidi di controllo: I livello (IT), II Livello (Referente Privacy e Compliance), III Livello Audit, DPO

Informative, Nomine, Regolamenti interni (regolamento informatico, sistema sanzionatorio…)

Valutazione dei Rischi: Analisi rischi- azioni di mitigazione-monitoraggio documentato, PIA

Zoom su elementi portanti spesso critici nelle organizzazioni

Acquisizione dati clienti – nomina DPO – PIA

Acquisizione dati clienti per creare portafogli clienti

Principi di necessità e minimizzazione:

- l'azienda è autorizzata a raccogliere solo i dati necessari per lo scopo connesso alla propria attività: non tutto ciò che si può acquisire

- L'elaborazione deve essere proporzionale e con il volume di dati strettamente necessari

Nomina DPO: Ruolo rafforzato del presidio di controllo compliance =>nomina obbligatoria per le organizzazioni con trattamenti ex art. 37 dl GDPR: fondamentale la competenza dei DPO interni

Zoom su elementi portanti spesso critici nelle organizzazioni

Acquisizione dati clienti – nomina DPO – PIA

PIA: **Principio di Accountability** (Elenco tipologie trattamenti da sottoporre a PIA, Garante Privacy Novembre 2017)

- Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad "**aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato".**
- **Trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato**, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi).

Fondamentale la verifica di privacy by design e by default circa necessità PIA

Zoom elementi portanti spesso critici nelle organizzazioni

Acquisizione dati clienti – nomina DPO – PIA

PIA: Principio di Accountability (Elenco tipologie trattamenti da sottoporre a PIA, Garante Privacy Novembre 2017)

- Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.
- Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).

Zoom elementi portanti spesso critici nelle organizzazioni

Acquisizione dati clienti – nomina DPO – PIA

PIA: Principio di Accountability (Elenco tipologie trattamenti da sottoporre a PIA, Garante Privacy Novembre 2017)

- Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).
- Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).
- Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01
- Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.
- Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment).

Zoom elementi portanti spesso critici nelle organizzazioni

Acquisizione dati clienti – nomina DPO – PIA

PIA: Principio di Accountability (Elenco tipologie trattamenti da sottoporre a PIA, Garante Privacy Novembre 2017)

- Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.
- Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

Per tutte le tipologie di trattamenti declinati

Fondamentale la verifica di privacy by design e by default circa necessità PIA

CONCLUSIONI

Il sistema di protezione dei dati personali **varia** in funzione del business dell'organizzazione

la costante

esistenza di strumenti regolamentari e operativi che siano in grado di DIMOSTRARE l'ADEGUATEZZA delle MISURE ORGANIZZATIVE – DOCUMENTALI – LOGISTICHE ED INFORMATICHE nel TEMPO a prevenire un rischio violazione dei dati personali e dei diritti fondamentali delle persone.


Grazie

UNITRAIN

Conoscere e applicare gli standard

– Via Sannio, 2 – 20137 Milano

02 70024379 - 228 formazione@uni.com www.uni.com