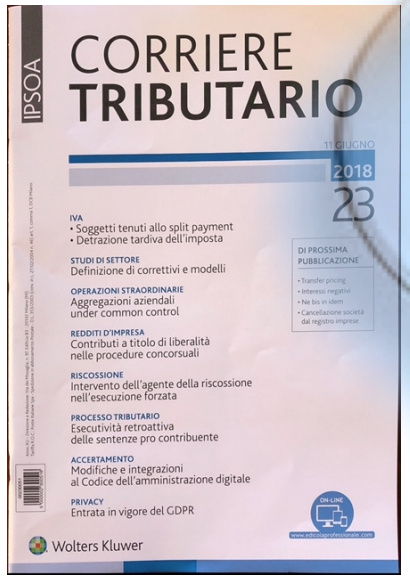
PRIVACY: LA RIVOLUZIONE GDPR

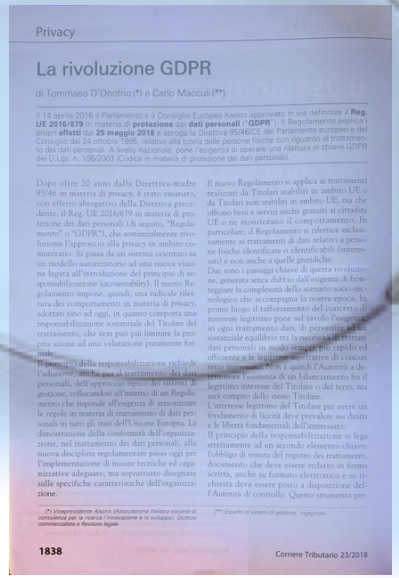
TOMMASO D'ONOFRIO

Parma 3 ottobre 2018

Due parole di presentazione…

Tommaso D'Onofrio: Laureato in Economia. Masterclass in Private Equity alla London Business School. Dottore commercialista e revisore legale; membro italiano, presso la Commissione Europea, nell'European Crowdfunding Stakeholder Forum (ECSF). E' stato, per un quadriennio, presidente di AISCRIS e Consigliere nazionale delegato (Formazione e Intellectual Property) di Confindustria Servizi Innovativi e Tecnologici della quale è attualmente membro della Giunta nazionale. Partecipa ai lavori del GDL legalità e 231/01 di Confindustria. Opera come consulente e formatore in materia di privacy e nell'elaborazione dei modelli di organizzazione e controllo ex d.lgs 231/01 in numerose organizzazioni ed imprese.





Di cosa parliamo…

- Contesto di riferimento
- Una nuova visione di responsabilizzazione (accountability)
- Revisione dei documenti attualmente adottati
- Nuovi adempimenti
- Nascita di una nuova figura professionale (DPO)
- La tenuta del registro
- Q&A

CONTESTO DI RIFERIMENTO

1

Quadro normativo di riferimento

Il 14 aprile 2016 il Parlamento e il Consiglio Europeo hanno approvato in via definitiva il Regolamento (UE) 2016/679 in materia di protezione dei dati personali (di seguito, «**Regolamento**» o «**GDPR**»). ***Il Regolamento esplica i propri effetti dal 25 maggio 2018,*** decorso un periodo di transizione di *due anni* dalla entrata in vigore.

Il Regolamento abroga la ***Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995*** «*relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali*». A livello nazionale, recentemente, è stato approvato il D.lgs n. 101 del 10 agosto 2018, recante le disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679. L'articolo 1 co.1 del predetto decreto recita: " Il trattamento dei dati personali avviene secondo le norme del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, di seguito «Regolamento»….

- Dal 25 maggio 2018 , il Regolamento UE è efficace indipendentemente dall'entrata in vigore del decreto nazionale
- E' dunque fondamentale comprendere sin da subito il livello di allineamento ai nuovi requisiti per definire un adeguato piano delle azioni di adeguamento.

La tempestiva implementazione del Regolamento consente alle organizzazioni da un lato di ottenere dei benefici, dall'altro di evitare di incorrere in costi, permettendo di:

- evitare **onerose sanzioni**;
- evitare **ricadute organizzative** importanti in termini di responsabilità;
- beneficiare di ritorni **di tipo reputazionale nei confronti degli *stakeholder*;**
- essere in grado di rispondere prontamente **alle richieste informative** che possono pervenire da parte dell'Autorità e degli interessati.

Cosa cambia

2

Accountability

Il concetto di *accountability* comporta una responsabilizzazione sostanziale dell'impresa, spostando l'attenzione da un precedente approccio puramente formale. Il sistema privacy viene visto come un sistema di gestione. Come anticipato, l'*accountability* comporta, quindi, l'adozione di misure tecniche ed organizzative «adeguate» a dimostrare la *compliance* con il Regolamento del trattamento dei dati. Uno dei passaggi chiave del principio la ritroviamo nella tenuta del registro che mira a dimostrare la capacità del titolare o del responsabile di conformarsi al GDPR e di conservare in maniera ordinata, **ricostruibile ex post** e verificabile da terzi le considerazioni svolte in merito all'adozione di misure adeguate ed efficaci volte ad attuare il principio di responsabilizzazione.

Art. 32 GDPR vs Allegato b - D.lgs 196/03 (abrogato da D. lgs 101/2018)

Art. 32 GDPR 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 adeguate 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.

MISURE ALLEGATO B: password, firewall, antivirus, screen saver attivo, backup….

Nella Guida al Regolamento in materia di protezione dei dati personali, il Garante specifica che: “ facendo anche riferimento alle prescrizioni contenute, in particolare, nell’allegato B al Codice l’Autorità potrà valutare la definizione di linee guida…”

Oggi non esistono misure obbligatorie o definitive, ma le abrogate misure minime di sicurezza possono rappresentare, soprattutto per le organizzazioni di piccole dimensioni un punto di riferimento formativo efficace.

Ambito di applicazione (artt. 1,2,3)

- Si applica solo ai trattamenti relativi a persone fisiche, (interessati: persona fisica identificata o identificabile alla quale si riferiscono i dati) non anche a quelle giuridiche; In via generale, la profilazione è vietata. Viene ammessa però in circostanze specifiche e, in particolare, previo consenso esplicito dell'interessato;

- Si applica ai trattamenti realizzati da titolari stabiliti in ambito UE

- Si applica ai trattamenti realizzati da titolari non stabiliti in ambito UE, ma che:
  - offrono beni e servizi anche gratuiti ai cittadini UE;
  - monitorano il comportamento dei cittadini UE;

Le nuove definizioni

Dai dati sensibili della 196/03 si passa a particolari categorie di dati personali (art. 9) che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, i dati biometrici (che ne consentono o ne confermano l'identificazione univoca), i dati relativi alla salute (compresa la prestazione di servizi di assistenza sanitaria) o alla vita sessuale o all'orientamento sessuale della persona;

Viene introdotto il concetto di **pseudonimizzazione**: il trattamento volto a nascondere l'identità dell'interessato e a impedirne l'identificazione senza l'utilizzo di informazioni aggiuntive.

Liceità del trattamento (art.6)

Il trattamento è lecito solo se ricorrono alternativamente o cumulativamente una serie di condizioni:

a) Presenza di un consenso per una o più finalità;

b) Il trattamento avviene in esecuzione di un contratto o di misure precontrattuali;

c) Il trattamento è legato ad un obbligo legale al quale è soggetto il titolare del trattamento;

d) Il trattamento è legato alla salvaguardia di interessi vitali;

e) Il trattamento è necessario in quanto correlato ad interesse pubblico o all'esercizio di pubblici poteri

f) Il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi

Legittimo interesse

Il bilanciamento fra legittimo interesse del titolare o del terzo e diritti e libertà dell'interessato non spetta all'Autorità ma è compito dello stesso titolare; si tratta di una delle principali espressioni del principio di "responsabilizzazione" introdotto dal nuovo pacchetto protezione dati.

L'interesse legittimo del titolare o del terzo deve prevalere sui diritti e le libertà fondamentali dell'interessato per costituire un valido fondamento di liceità.

Informative (art. 13 e 14)

Forma: concisa, trasparente, intellegibile, facilmente accessibile, semplice e chiara.

Conferimento: per iscritto o con mezzi elettronici. Può essere orale solo se richiesto dall'interessato e purché sia comprovata con altri mezzi l'identità. Può essere anche fornita con icone standardizzate.

Contenuto: Estremi responsabile e DPO; finalità e base giuridica del trattamento; specificazione degli interessi legittimi (se presenti) del titolare; destinatari o categorie di destinatari; eventuale trasferimento dati extra Ue con strumento di liceità; periodo di conservazione o criteri di determinazione; diritti dell'interessato; natura del conferimento e conseguenze in caso di rifiuto a conferirli; eventuale esistenza di un processo decisionale automatizzato (logica applicata e conseguenze del trattamento);

Consensi

Forma: manifestazione di volontà libera, informata e inequivocabile dell'interessato. Può consistere in una dichiarazione o in un'azione positiva inequivocabile; documentato e distinto e revocabile senza pregiudicare la liceità dei precedenti trattamenti;

Obbligo forma esplicita: riguarda il trattamento di particolari categorie di dati personali e per la profilazione;

Gli Stati membri possono mantenere o introdurre ulteriori condizioni per il trattamento di dati genetici, dati biometrici o dati relativi alla salute

Responsabilità

TITOLARE: È il soggetto che determina le finalità e i mezzi del trattamento;

CONTITOLARI: Ulteriori soggetti che determinano congiuntamente le finalità e i mezzi del trattamento (necessario accordo interno su ruoli e responsabilità;

RESPONSABILE DEL TRATTAMENTO: È il soggetto che tratta i dati per conto del Titolare. Deve presentare garanzie professionali sufficienti per attuare misure tecniche e organizzative adeguate. La sua nomina è obbligatoria ed è documentata con un contratto o altro atto giuridico (art. 28);

L'INCARICATO AL TRATTAMENTO: Agisce sotto l'autorità del Titolare e del responsabile, ma non è espressamente disciplinato (neppure escluso) dal regolamento.

NB: I Titolari, ovvero il Titolare e il Responsabile, ovvero i Responsabili coinvolti nel medesimo trattamento, rispondono in solido per l'intero ammontare del danno cagionato dalla violazione del Regolamento

Diritto all'oblio (art. 17)

L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;

c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;

d) i dati personali sono stati trattati illecitamente; e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;

e) f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione (minori) di cui all'articolo 8, paragrafo 1.

Diritto all'oblio

Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione **adotta le misure ragionevoli**, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali. *Il diritto alla deindicizzazione sussiste anche rispetto a notizie soltanto inesatte* (Trib. Milano sent. N. 7846 del 5 settembre 2018)

Diritto alla portabilità (art.20)

L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora il trattamento si basi sul consenso precedentemente rilasciato o si basa su un contratto o su trattative precontrattuali in corso.

Nell'esercitare i propri diritti relativamente alla portabilità dei dati **l'interessato ha il diritto** di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.

Tale diritto sussiste solo se i dati sono trattati con il consenso dell'interessato (art. 6.1 lett.a) o sulla base di un contratto (art. 6.1. lett. B), mentre non sussiste nei casi si basi sull'esercizio di pubblici poteri

Privacy by design e by default (art. 25)

La privacy by design comporta che le attività, i prodotti e i servizi che comportano il trattamento di dati personali devono essere progettati, impostati e sviluppati in modo da assicurare il rispetto dei principi e delle garanzie a tutela della privacy. Nella progettazione bisogna adottare misure per minimizzare l'utilizzo di dati personali, consentire all'interessato il controllo dei propri dati, garantire trasparenza e sicurezza.

La privacy by default comporta che il trattamento, per impostazione predefinita, debba avere ad oggetto solo i dati necessari al perseguimento della specifica finalità prefissata in termini di quantità, di portata del trattamento, di periodo di conservazione e di accessibilità;

Data breach notification (art.33 – 34)

Obbligo previsto: In caso di violazione dei dati personali, il Titolare effettua una notifica all'Autorità di controllo senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà degli interessati. La comunicazione deve contenere la natura della violazione, la descrizione delle possibili conseguenze e delle misure adottate per rimediare e ridurre gli effetti negativi. Vige altresì un obbligo di implementazione e conservazione di documentazione di qualsiasi violazione dei dati personali (circostanze, conseguenze e azioni poste in essere per porvi rimedio) per permettere all'Autorità di controllo il rispetto delle prescrizioni in tema di data breach;

Data Protection Impact Assessment (DPIA) (art. 35)

Quando un tipo di trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche il titolare effettua una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.

La valutazione d'impatto sulla protezione dei dati è richiesta in particolare nei casi seguenti:

- ✓ a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- ✓ b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;
- ✓ c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Ruolo dell'autorità garante: L'Autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti alla valutazione d'impatto. L'Autorità di controllo può altresì redigere e rendere pubblico un elenco delle tipologie di trattamenti non soggetti a valutazione d'impatto.

Contenuto: Il PIA contiene la descrizione sistematica dei trattamenti e delle finalità, la valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; la valutazione dei rischi e misure previste per affrontarli

Data Protection Impact Assessment (DPIA) (art. 35)

Le autorità di controllo (art. 29) nella linea guida WP 248 hanno definito i seguenti 9 criteri a cui il titolare può fare riferimento:

1. **Valutazione o assegnazione di un punteggio**, inclusiva di profilazione e previsione, in particolare in considerazione di *"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"* (considerando 71 e 91).
2. **processo decisionale automatizzato** che ha effetto giuridico o incide in modo analogo significativamente: trattamento che mira a consentire l'adozione di decisioni in merito agli interessati che *"hanno effetti giuridici*" o che "*incidono in modo analogo significativamente su dette persone fisiche*" (articolo 35, paragrafo 3, lettera a)).
3. **monitoraggio sistematico:** trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o *"la sorveglianza sistematica su larga scala di una zona accessibile al pubblico*" (articolo 35, paragrafo 3, lettera c)).
4. **dati sensibili o dati aventi carattere altamente personale**: questo criterio include categorie particolari di dati personali così come definite all'articolo 9 (ad esempio informazioni sulle opinioni politiche delle persone), nonché dati personali relativi a condanne penali o reati di cui all'articolo 10.
5. **trattamento di dati su larga scala**: il regolamento generale sulla protezione dei dati non definisce la nozione di "su larga scala", tuttavia fornisce un orientamento in merito al considerando 91.
6. **creazione di corrispondenze o combinazione di insiemi di dati,** ad esempio a partire da dati derivanti da due o più operazioni di trattamento svolte per finalità diverse e/o da titolari del trattamento diversi secondo una modalità che va oltre le ragionevoli aspettative dell'interessato;
7. **dati relativi a interessati vulnerabili (es: minori)** (considerando 75): il trattamento di questo tipo di dati è un criterio a motivo dell'aumento dello squilibrio di potere tra gli interessati e il titolare del trattamento, aspetto questo che fa sì che le persone possono non essere in grado di acconsentire od opporsi al trattamento dei loro dati o di esercitare i propri diritti.
8. **uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative**, quali la combinazione dell'uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici, ecc.
9. **quando il trattamento in sé *"impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto"*** (articolo 22 e considerando 91). (trattamento automatizzato atto a produrre effetti giuridici)

IL DPO (DATA PROTECTION OFFICER)

3

Data Protection Officer DPO

Di chi si tratta: È il soggetto che assiste il Titolare in merito al rispetto degli obblighi privacy e all'implementazione delle policies cooperando con l'Autorità di controllo e funge da punto di contatto per questioni connesse al trattamento;

La designazione è obbligatoria per: la PA, nei casi nei quali le attività principali del Titolare consistono in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala (comportano l'utilizzo di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e incidono su un elevato numero di interessati) o se le attività principali del Titolare consistono in trattamenti su larga scala di dati "sensibili".

Requisiti: Può essere un soggetto interno o esterno all'organizzazione che deve poter disporre di risorse (personale, locali, attrezzature, ecc.) necessarie per l'espletamento dei propri compiti.
Viene designato in funzione delle sue qualità professionali (non sono richieste specifiche attestazioni), in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i propri compiti. Riferisce direttamente al Titolare e i suoi dati sono comunicati direttamente all'Autorità Garante. **Deve inoltre agire in piena indipendenza** (considerando 97 del Regolamento UE 2016/679) **e autonomia**, senza ricevere istruzioni

DPO: per chi non è obbligatoria la nomina

Nei casi diversi da quelli previsti dall'art. 37, par. 1, lett. b) e c), del Regolamento (UE) 2016/679, la designazione del responsabile del trattamento non è obbligatoria (ad esempio, in relazione a trattamenti effettuati **da liberi professionisti operanti in forma individuale**; agenti, rappresentanti e mediatori operanti non su larga scala; **imprese individuali** o familiari; piccole e medie imprese, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti: v. anche considerando 97 del Regolamento, in relazione alla definizione di attività "accessoria").

In ogni caso, resta comunque raccomandata, anche alla luce del principio di "accountability" che permea il Regolamento, la designazione di tale figura (v., in proposito, le menzionate linee guida), i cui criteri di nomina, in tale evenienza, rimangono gli stessi sopra indicati.

La tenuta del registro

4

Registro della attività di trattamento

Soggetti passivi: Il GDPR introduce l'obbligo in capo al titolare e al responsabile del trattamento di tenere registri delle attività di trattamento dei dati svolte (artt. 30.1, 30.2, GDPR). Destinatari di tale obbligo sono le imprese o organizzazioni con oltre 250 dipendenti, nonché quelle che effettuano trattamenti che possono presentare un rischio per i diritti e le libertà dell'interessato, o abbiano ad oggetto dati sensibili, biometrici, genetici, relativi alla salute o a reati e condanne penali (art. 30.5, GDPR).

Tenuta dei registri: I registi dei trattamenti di titolare e responsabile del trattamento devono essere tenuti in forma scritta, anche su formato elettronico (art. 30.3, GDPR).

Poteri del Garante: Su richiesta, titolare e responsabile del trattamento sono tenuti a mettere i registri a disposizione dell'autorità di controllo (art. 30.4, GDPR)

Contenuti del registro: Il GDPR (art. 30.1) elenca le informazioni che il titolare deve conservare nel registro:

- → Nome e contatti di Titolare, Contitolare, Rappresentante del titolare e DPO;
- → Finalità del trattamento;
- → Descrizione delle categorie di interessati e dei dati personali oggetto di trattamento;
- → Categorie di destinatari;
- → Eventuali trasferimenti di dati personali verso un paese terzo o organizzazione internazionale
- → Ove possibile, termini ultimi di cancellazione per categoria di dati;
- → Descrizione generale misure di sicurezza tecniche e organizzative (vd. art. 32, par. 1, GDPR).

Nonostante non vi sia identità testuale nel dettato del GDPR, analoga informativa deve essere contenuta nel registro dei trattamenti tenuto dal responsabile del trattamento (art. 30.2, GDPR).

COSA FARE ?

5

Sanzioni

Responsabilità civile: Chiunque subisca un danno materiale o immateriale causato da una violazione del Regolamento ha il diritto di ottenere il risarcimento del danno. Il Titolare o il Responsabile del trattamento è esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile

Responsabilità amministrativa: Le sanzioni amministrative pecuniarie possono arrivare fino a 20.000.000 euro o, per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore; Le sanzioni amministrative possono essere inflitte congiuntamente o in luogo di: avvertimenti, ammonimenti, ingiunzioni, limitazioni, divieti e sono dimensionate in funzione della natura, gravità, durata, carattere doloso o colposo della violazione, grado di responsabilità e comportamenti precedenti del titolare, adozione delle misure di prevenzione, grado di cooperazione con l'Autorità di controllo per rimediare alla violazione

Responsabilità penale: Gli Stati membri stabiliscono le norme relative alle altre sanzioni per le violazioni del Regolamento, in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie, e adottano tutti i provvedimenti necessari per assicurarne l'applicazione. Le sanzioni devono essere effettive, proporzionate e dissuasive

Cosa si dovrebbe fare ?

Audit iniziale: Il regolamento nella sua strutturazione propone un audit iniziale finalizzato a determinare l'impatto che le norme in oggetto possono avere sull'azienda di riferimento. I contenuti della relazione di audit potranno, all'occorrenza confluire nella valutazione di impatto privacy (DPIA), ove questa fosse ritenuta necessaria:

Attività: Il titolare del trattamento (studio di architettura) deve procedere:

a) nella valutazione di impatto privacy (se applicabile) contenente la descrizione delle misure previste per affrontare i rischi, comprese le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione
b) Nell'elaborazione delle informative e degli eventuali contratti con i responsabili del trattamento
c) nell'implementazione (riesame e aggiornamento) delle misure tecniche e organizzative idonee a garantire e dimostrare che il trattamento è conforme al Regolamento;
d) nell'implementazione e aggiornamento del registro dei trattamenti, se necessaria.

Attività successiva e figure professionali: Monitoraggio, gestione registro (se necessario) e attivazione nuove figure professionali in materia di privacy;

@TommasoDOnofrio

Grazie per l’attenzione

DISPONIBILE SU AMAZON