Luca Di Leo

Consulenza e formazione in materia di protezione dei dati personali dal 2005

Studio Paci &C srl
(cda)

Associazione Protezione diritti e libertà privacy
(Vice presidente)

Contatti:
info@lucadileo.com
Cell. 3931019939

Linkedin: #luca di leo

Responsabile della Protezione dei Dati (DPO per aziende private, pubbliche, sanità)
certificazione UNI 11697:2017 (Registro Accredia)

Valutatore Privacy
certificazione UNI 11697:2017 (in aggiornamento)

Privacy Officer
Certificazione TUV Italia 2013 – certificazione competenze Federprivacy – Legge n.4/2013

Auditor GDPR
secondo lo schema di certificazione per il GDPR: ISDP@10003 (in aggiornamento)

Consulente per l'implementazione dello schema di certificazione ISDP@10003

Lead Auditor ISO 27001 , aggiornamento ISO 27701

Docente per il master in Cybersecurity Università delle Marche

Direttiva (UE) 2019/1937

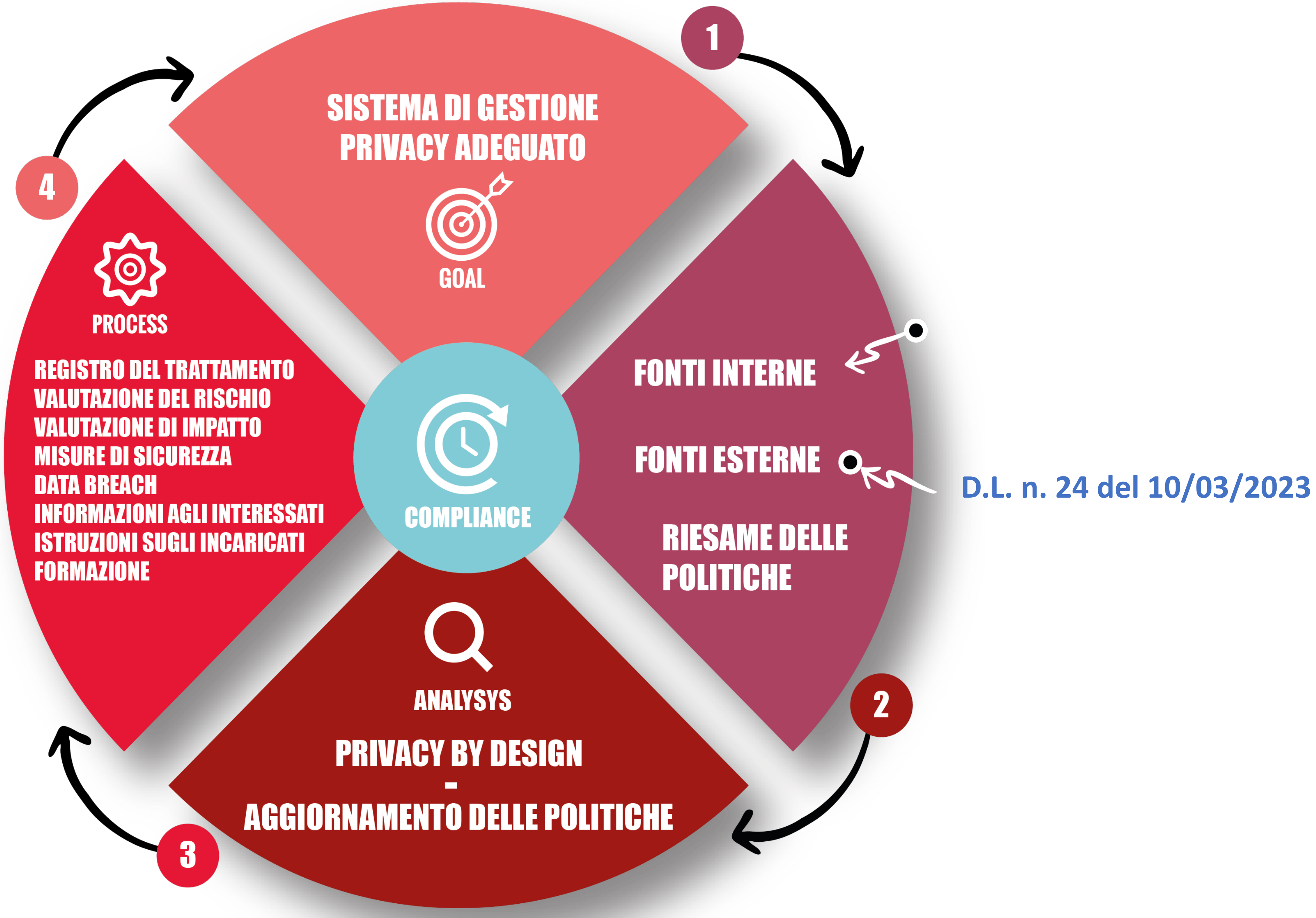
D.Lgs. n. 24 del 10 marzo 2023

"Whistleblowing"
a norma privacy

relatore: Luca Di Leo
consulente e DPO Studio Paci

vice presidente Associazione Protezione Diritti e libertà privacy, consulente e DPO


KEEP
CALM
AND
CALL YOUR
DPO


SISTEMA DI GESTIONE PRIVACY ADEGUATO
GOAL
1
FONTI INTERNE
FONTI ESTERNE
D.L. n. 24 del 10/03/2023
RIESAME DELLE POLITICHE
2
ANALYSYS
PRIVACY BY DESIGN
-
AGGIORNAMENTO DELLE POLITICHE
3
PROCESS
REGISTRO DEL TRATTAMENTO
VALUTAZIONE DEL RISCHIO
VALUTAZIONE DI IMPATTO
MISURE DI SICUREZZA
DATA BREACH
INFORMAZIONI AGLI INTERESSATI
ISTRUZIONI SUGLI INCARICATI
FORMAZIONE
4
COMPLIANCE

FONTI ESTERNE:

AGGIORNAMENTO NORMATIVO
LINEE GUIDA EDPB E GARANTE PRIVACY
PROVVEDIMENTI SANZIONATORI

FONTI INTERNE:

NUOVI TRATTAMENTI DATI:
INSERIMENTO NUOVI STRUMENTI, SOFTWARE, WEB, APP
INCIDENTI - DATABREACH

RIESAME DELLE POLITICHE (ART. 5 E 24 GDPR)
PRIVACY BY DESIGN (ART. 25 GDPR)

VALUTAZIONE DEL RISCHIO
EVENTUALE VALUTAZIONE DI IMPATTO
INTERGAZIONE ED AGGIORNAMENTO MISURE DI SICUREZZA
INFORMAZIONI AI SOGGETTI INTERESSATI SUI TRATTAMENTI DATI NUOVI O INTEGRATI
AGGIORNAMENTO DEL REGISTRO DEL TRATTAMENTO
AGGIORNAMENTO DELLE ISTRUZIONI DEGLI INCARICATI
FORMAZIONE

SISTEMA DI GESTIONE PRIVACY ADEGUATO

Whistleblowing e GDPR

Con il termine whistleblowing s'intende:

la rivelazione spontanea da parte di un individuo, detto "segnalante" (in inglese "whistleblower") di un illecito o di un'irregolarità commessa all'interno dell'organizzazione, del quale lo stesso sia stato testimone nell'esercizio delle proprie funzioni.
Il segnalante spesso <u>è un dipendente</u> ma può anche essere <u>una terza parte, per esempio un fornitore o un cliente.</u>

Si parla di whistleblowing "interno" quando la <u>segnalazione</u> viene fatta da un dipendente dell'azienda per il tramite di <u>canali di segnalazione</u> interni all'azienda.

Questi strumenti hanno allo scopo di garantire una canale di comunicazione a tutti coloro che sono a conoscenza di illeciti o atti non etici avvenuti all'interno dell'organizzazione.

Ed è proprio qui che la disciplina sulla protezione dei dati personali trova applicazione!

Di fatto il Reg. UE 2016/679 «GDPR» si applica <u>a tutti i trattamenti dati dell'organizzazione</u>, ed in particolare in questo contesto occorre <u>disciplinare i canali di comunicazione</u> in termini di sicurezza, e…

TRATTAMENTO DATI:
GESIONE DELLE SEGNALAZIONI WHISTELBLOWING

CARTA DEI DIRITTI FONDAMENTALI DELL'UNIONE EUROPEA

SOGGETTI INTERESSATI: SEGNALANTE, SEGNALAZIONI, SOGGETTI COINVOLTI

Efficacia delle Segnalazioni

DPIA

Considerando 4 del Reg. UE 2016/679

Rispetto della dignità della persona
Non discriminazione,
Rispetto della vita privata e familiare,
del domicilio e delle comunicazioni,
La protezione dei dati personali, la libertà di pensiero,
di coscienza e di religione, nonché la
diversità culturale, religiosa e linguistica.

IL BILANCIAMENTO DEI DIRITTI DEVE AVVENIRE ATTRAVERSO LE MODALITA' ORGANIZZATIVE E LE RELATIVE MISURE DI SICUREZZA.

IL SOGGETTO RESPONSABILE E' IL TITOLARE DEL TRATTAMENTO!!!
Art. 5 e 24 Reg. UE 2016/679
CONSAPEVOLEZZA E PRINCIPIO DI RESPONSABILIZZAZIONE

Associazione
Protezione Diritti e Libertà
Privacy

Quando un trattamento dati è legittimo?

Deve rispettare i principi di responsabilizzazione c.d. ‘accountability’ di cui all’art. 5 del Reg. UE 2016/679

Di chi è la responsabilità di dimostrare che il trattamento dati è legittimo?

IL TITOLARE DEL TRATTAMENTO

è competente per il rispetto dei principi di accountability ed <u>è in grado di comprovarlo</u>
(art. 5 par. 2 del Reg. UE 2016/679)

Cosa deve fare il titolare del trattamento?

1) *Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, <u>ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento.</u>*
<u>Dette misure sono riesaminate e aggiornate qualora necessario</u>

2) *Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono <u>l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.</u>*

…Omissis…

(Art. 24 Reg. UE 2016/679)

Whistleblowing e GDPR

Da fare:

1) Coinvolgere il Responsabile sulla Protezione dei dati personali – RPD – DPO anche in merito ai requisiti della piattaforma – art. 37-38-39 GDPR

2) Individuare i ruoli e determinare le politiche per il trattamento («atto organizzativo», «MOG 231/2001») e la sicurezza dei dati relativi al WB – art. e 24 GDPR
(titolare, co-titolare, responsabile del trattamento, «incaricati» – soggetti designati sotto l'autorità del titolare)

3) Accordi di co-titolarità – art. 26 GDPR

4) Registro del trattamento – art. 30 GDPR

5) Privacy by design by default e la valutazione dei rischi – art. 25 GDPR

6) Valutazione di impatto – DPIA – art. 35 GDPR e D.Lgs. 24/2023 (obbligatoria)

7) Implementazione di misure di sicurezza tecniche ed organizzative specifiche sia dell'organizzazione del titolare, che applicate al canale di comunicazione ed al trattamento stesso (richieste al gestore della piattaforma in qualità di responsabile del trattamento dei dati) sulla base dell'esito della DPIA. Parere del DPO sulla DPIA. Pubblicazione parti essenziali della DPIA (esito sul sito) – *linee guida WP 248 rev.1 sempre attuali.* – art. 32 GDPR e misure speciali cogenti D.Lgs. 24/2023 (pseudoanonimizzaione, cifratura sia del canale di trasmissione, dei contenuti/conservazione dei dati anagrafici del segnalante, nel backup, no accesso agli ADS, pseudoanonimizzaione, autenticazione a doppio fattore, conservazione separata delle identità dei segnalanti dalla segnalazione. Comunicazione ad altri soggetti solo su consenso dell'interessato)

8) Formazione su due livelli:
 8.1) ai referenti che a qualsiasi titolo dovranno gestire, custodire l'identità, etc. le segnalazioni
 8.2) tutti i dipendenti

Whistleblowing e GDPR

9) Redigere una informativa ai sensi dell'art. 13 e 14 specifica per tutti i soggetti interessati al trattamento dati del WB (segnalanti, etc.) – integrare le informative esistenti di: candidati, dipendenti, fornitori e clienti (per quest'ultimi solo nella circostanza in cui abbiano rapporti con l'organizzazione del titolare del trattamento)

10) Istruzioni, compiti e funzioni, accordo di riservatezza per il trattamento ai soggetti reputati a ricevere e/o gestire tali segnalazioni art. 29 GDPR e art. 2 quaterdecies D.Lgs. 196/2003

11) Se ci si avvale di servizi esterni per l'utilizzo dei canali di segnalazione interni occorre anche valutare preliminarmente in termini di garanzie di applicazione al GDPR e al D.Lgs. 24/2023 del soggetto ed <u>individuarlo quale responsabile del trattamento, e quindi occorrerà la formulazione di una **nomina a responsabile da fare sottoscrivere a tale soggetto – art. 28 GDPR -** incluse le misure di sicurezza tecnche ed organizzative nonché misure speciali in virtù del D.Lgs. 24/2023.</u>

12) Le organizzazioni (PA e soggetti privati) <u>**non si possono avvalere della posta elettronica quale canale di comunicazione**</u> *(Parte prima – I canali e le modalità di presentazione delle segnalazioni / Istituzione dei canali di segnalazione – linee guida ANAC 12 luglio 2023)*. Si possono invece avvalere di piattaforme, e altri canali tradizionali (telefono, presenza) con determinate modalità.

13) Log degli accessi del personale che gestisce le segnalazioni

14) Divieto di tracciamento delle attività del segnalante *(tracciamento log segnalante eventualmente IP su firewall rete interna – anche se solo visibile all'ADS – provv. sanzionatorio – Azienda Ospedaliera di Perugia)*

15) Procedura per l'esercizio dei diritti degli interessati

Alcune sanzioni a soggetti pubblici, privati e gestori di piattaforme per le segnalazioni

Ordinanza ingiunzione nei confronti di Aeroporto Guglielmo Marconi di Bologna S.p.a. - 10 giugno 2021
Registro dei provvedimenti n. 235 del 10 giugno 2021 (40.000 euro)

Ordinanza ingiunzione nei confronti di XXXXXXX (società fornitore della piattaforma) - 10 giugno 2021
Registro dei provvedimenti n. 236 del 10 giugno 2021 (20.000 euro)

Ordinanza ingiunzione nei confronti di Azienda ospedaliera di Perugia - 7 aprile 2022
Registro dei provvedimenti n. 134 del 7 aprile 2022 (40.000 euro)

Ordinanza ingiunzione nei confronti di YYYYYYYY - 7 aprile 2022
Registro dei provvedimenti n. 135 del 7 aprile 2022 (40.000 euro)

Un esempio di applicazione del principio di Accountability

PRIVACY BY DESIGN ART. 25 GDPR

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.
3. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo.

Articolo 5 Reg. UE 2016/679

Principi applicabili al trattamento di dati personali

1. I dati personali sono: (C39)

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»). (C74)

1) lo “stato dell’arte”

inteso come obbligo, per i Titolari, di determinare le misure tecniche e organizzative appropriate, **tenendo conto degli attuali progressi tecnologici disponibili sul mercato**.

Questo implica che i Titolari siano costantemente aggiornati sui progressi tecnologici.

NECESSITA’ DI INDIVIDUARE CANALI DI INFORMAZIONE

Se ne deduce che lo “stato dell'arte” è un concetto dinamico che non può essere definito staticamente in un unico momento temporale, ma dovrebbe essere valutato continuamente nel contesto del progresso tecnologico.

2) I costi di attuazione

Non è richiesto al Titolare di spendere una quantità sproporzionata di risorse quando esistono misure alternative, meno impegnative in termini di risorse, ma efficaci.

Il costo di attuazione è un fattore da considerare per implementare la protezione dei dati fin dalla progettazione.

Pertanto, le misure scelte devono assicurare che le attività di trattamento previste dal Titolare consentano di non trattare i dati personali in violazione dei principi, indipendentemente dal costo.

SAREBBE AUSPICABILE CHE SIA DATA EVIDENZA DI UNA VALUTAZIONE DEI COSTI E LA RELATIVA DECISIONE (ESEMPI)

3) La natura, l'ambito di applicazione, il contesto e le finalità del trattamento

I Titolari devono prendere in considerazione l'ambito di applicazione, il contesto e le finalità del trattamento quando determinano le misure necessarie da adottare.

Il concetto di natura può essere inteso come le caratteristiche intrinseche del trattamento (ad es. categorie particolari di dati personali, processi decisionali automatici, rapporti di potere distorti, trattamenti non previsti, difficoltà per l'interessato di esercitare i diritti, ecc).

L'ambito di applicazione si riferisce alla dimensione e al tipo di trattamento.
Il contesto si riferisce alle circostanze del trattamento, che può influenzare le aspettative dell'interessato, mentre lo scopo riguarda le finalità del trattamento.

4) I rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento

Il gdpr adotta un approccio coerente basato sul rischio in molte delle sue disposizioni, agli articoli 24, 25, 32 e 35, al fine di individuare misure tecniche e organizzative adeguate per tutelare gli individui, i loro dati personali in conformità ai requisiti del gdpr. Le risorse da proteggere sono sempre le stesse (le persone, tramite la tutela dei dati personali), a fronte degli stessi rischi (per i diritti degli individui), tenendo conto delle stesse condizioni (natura, ambito, contesto e finalità).

Quando esegue l'analisi dei rischi per la conformità con l'articolo 25, il Titolare deve identificare i rischi per i diritti degli interessati che una violazione dei principi potrebbe presentare e determinarne la probabilità e gravità al fine di attuare misure per mitigare efficacemente i rischi identificati. La valutazione sistematica e approfondita del trattamento è fondamentale quando si effettuano le valutazioni del rischio.

L'aspetto del tempo

La protezione dei dati fin dalla progettazione deve essere implementata “al momento di determinare i mezzi del trattamento", con ciò facendo espresso riferimento al periodo di tempo in cui il Titolare decide come sarà condotto il trattamento, il modo in cui il trattamento avverrà e quali meccanismi verranno utilizzati per condurre tale elaborazione. È nel prendere tali decisioni che il Titolare deve valutare le misure e le garanzie appropriate per attuare efficacemente i principi e i diritti degli interessati nel trattamento e tener conto di elementi quali lo stato dell'arte, i costi di implementazione, la natura, la portata, il contesto, lo scopo ed rischi. Ciò include il tempo necessario per procurarsi e implementare software di elaborazione dati, hardware e servizi.

Una volta avviato il trattamento, il Titolare ha l'obbligo di mantenere la continua ed efficace attuazione dei principi al fine di tutelare i diritti, rimanendo aggiornati sullo stato dell'arte, rivalutando il livello di rischio, ecc. La natura, la portata e il contesto delle operazioni di trattamento, così come il rischio può cambiare nel corso del trattamento, il che significa che il Titolare deve rivalutare le proprie operazioni di trattamento attraverso revisioni e valutazioni periodiche sull'efficacia delle misure e delle garanzie scelte.

L'obbligo di mantenere, rivedere e aggiornare, se necessario, l'operazione di trattamento si applica anche ai sistemi preesistenti. Ciò significa che i sistemi progettati prima dell'entrata in vigore del gdpr devono essere revisionati per garantire l'attuazione delle misure e delle garanzie che attuano i principi e i diritti degli interessati in modo efficace, come delineato dalle linee guida in commento.


KEEP
CALM
AND
CALL YOUR
DPO