General **D**ata **P**rotection **R**egulation

Giancarlo Turati

Tignale 5 giugno 2018

IL REGOLAMENTO UE N. 679/2016 E LE NOVITÀ NEL TRATTAMENTO DEI DATI

Entrata in vigore: 24 maggio 2016

Applicabilità in tutti i paesi dell'UE: 25 maggio 2018

Il Regolamento sostituisce la Direttiva 95/46/CE su cui in Italia si fonda il Codice Privacy (D.Lgs. 196/03)

Punto di svolta: da una serie di **norme da rispettare** si passa ad una serie di **principi ispiratori**

Le differenze di fondamento legislativo

- Il **D.Lgs. 196/03** o **Codice Privacy**: è fondato su di una Direttiva. Essa fissa un risultato ed è uno strumento normativo che ai fini attuativi richiede l'adozione di nuove normative/l'abrogazione di normative pre-esistenti

- Il **Regolamento**: esso è per sua natura uno strumento normativo che deve essere rispettato nella sua interezza e vincola tutti gli Stati membri ad adeguare le proprie legislazioni

Obiettivi del Regolamento 679/2016

- Aggiornamento: gli impianti normativi europei, soprattutto quello italiano, non sono andati di pari passo con gli sviluppi tecnologici, in particolare informatici, dell'ultimo decennio lasciando così delle lacune in tema di protezione dei dati che il legislatore europeo ha sentito la necessità di colmare
- Armonizzazione: finora, ogni stato dell'Unione ha avuto un suo Codice Privacy fondato sulla Direttiva 95/46/CE. Con l'introduzione del Regolamento l'obiettivo è quello di creare un unico corpo normativo uniforme su tutto il territorio

La «nuova filosofia» del Regolamento

Si passa da un approccio c.d. **formalistico** ad un approccio di sostanziale responsabilizzazione ovvero la c.d. ***Accountability***

a) Non più specifici adempimenti elencati e descritti -> *Compliance* rimessa ai destinatari che si traduce in un rafforzamento degli obblighi

b) Il Regolamento si applica esclusivamente ai trattamenti dei dati personali di persone fisiche → Non disciplina il trattamento dei dati relativi a persone giuridiche, come le imprese dotate di personalità giuridica

Gli interrogativi più frequenti per le aziende

- Sarà solo il GDPR a disciplinare la materia? **NO**. Art. 9, c. 4: gli Stati possono mantenere od introdurre ulteriori condizioni
- Ci saranno deroghe e semplificazioni per le PMI? **SI**. Art. 30, c. 5: alcuni obblighi, come ad es. la tenuta di un Registro dei Trattamenti, non si applicano alle imprese od organizzazioni con meno di 250 dipendenti, a meno che non sussistano alcuni elementi
- Il Titolare del Trattamento deve ottenere nuovamente il consenso per tutti i trattamenti in essere? **NO**. Considerando n. 171: se il trattamento dei dati si basa sul consenso a norma della direttiva 95/46/CE, non occorre che l'interessato presti di nuovo il consenso, se espresso secondo modalità conformi al Regolamento

Nuovi concetti

- A) **Privacy by design**: tutte le attività, i prodotti ed i servizi che comportano il trattamento di dati personali devono essere sin dall'inizio progettati, impostati e sviluppati in modo da assicurare il rispetto dei principi e delle garanzie a tutela della Privacy. Questo concetto ha lo scopo di garantire la tutela dei dati personali in ogni fase del ciclo di gestione dell'informazione che va dalla raccolta alla cancellazione

Nuovi concetti

- B) **Privacy by default**: significa che il trattamento dei dati deve avere ad oggetto solo i dati necessari al perseguimento delle finalità prefissate ed alla base della loro raccolta

Da qui il principio di Necessità: quantità dei dati raccolti, portata del trattamento, periodo di conservazione ed accessibilità

I soggetti della Privacy secondo il GDPR

CODICE PRIVACY ex D.Lgs. 196/03	GDPR
TITOLARE DEL TRATTAMENTO (e co-titolare)	TITOLARE DEL TRATTAMENTO **DATA CONTROLLER**
RESPONSABILE DEL TRATTAMENTO (e sub-responsabile)	RESPONSABILE DEL TRATTAMENTO **DATA PROCESSOR**
INCARICATO DEL TRATTAMENTO	**NON ESPRESSAMENTE PREVISTO** È chiunque agisca sotto l'autorità del Titolare o del Responsabile

L’interessato

L’**interessato al trattamento** dei dati è la persona fisica, identificata od identificabile, alla quale si riferiscono i dati

Il Titolare del Trattamento

E’ il soggetto che determina le finalità ed i mezzi del trattamento dei dati raccolti

Il Responsabile del Trattamento

- È il soggetto che tratta i dati **per conto** del Titolare
- Deve presentare **garanzie sufficienti** per attuare misure tecniche ed organizzative **adeguate**
- La sua è una nomina **obbligatoria** e documentata con un contratto od altro atto giuridico

Attenzione: nel GDPR questa figura ha obblighi più stringenti rispetto a quello che prevedeva l'art. 29 del D.Lgs. 196/03

L’incaricato del Trattamento

- Non viene espressamente disciplinato dal GDPR
- Sono tutti quei soggetti che agiscono sotto l’autorità del Titolare o del Responsabile e che trattano dati personali
- Per questa figura vigono obblighi di istruzione e formazione (anche se quest’ultima deve ancora essere espressamente dettagliata dal Garante nelle modalità e nelle tempistiche)

ATTENZIONE: **anche se non prevista dal Regolamento questa resta una figura con un ruolo assolutamente centrale e fondamentale nell’impianto applicativo della normativa**

Il Responsabile della Protezione dei Dati (DPO)

- È il soggetto che assiste il Titolare in merito al rispetto degli obblighi Privacy ed all'implementazione delle Policy interne alle aziende
- Deve essere obbligatoriamente nominato (dal Titolare oppure dal Responsabile del trattamento):

a) Nelle P.A.

b) Se le attività principali del Titolare consistono in «trattamenti su larga scala di dati particolari (ex sensibili)» o che «richiedono il monitoraggio regolare e sistematico degli interessati su larga scala» intendendosi l'uso di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale incidendo su di un elevato numero di interessati

La documentazione alla base dell'impianto Privacy del GDPR

Riportiamo di seguito quei documenti che accomunano in generale la base per ogni impianto Privacy all'interno di un'azienda:

- Informativa
- Consenso
- Incarichi
- Le policy aziendali

L’informativa ed i suoi requisiti

- Concisa, trasparente, intellegibile, facilmente accessibile, semplice e chiara;
- fornita per iscritto o con altri mezzi, anche elettronici;
- può essere fornita in combinazione con icone standardizzate.

L’informativa ed il suo contenuto

- estremi del Titolare, del Responsabile e del DPO;
- finalità e base giuridica del trattamento;
- destinatari o categorie di destinatari;
- specificazione degli interessi legittimi perseguiti dal Titolare o da terzi;
- eventuale trasferimento verso Paesi extra UE;
- periodo di conservazione dei dati o comunque criteri per determinarlo;
- diritti dell’interessato;
- natura del conferimento e conseguenze in caso di rifiuto;
- esistenza di un eventuale processo decisionale automatizzato (ad es. *profiling*), logica applicata e conseguenze del trattamento.

Il consenso: caratteristiche generali

- È svincolato dall'informativa e consiste nella manifestazione libera, specifica, informata ed inequivocabile dell'interessato;
- deve essere documentato;
- può consistere in un'azione positiva inequivocabile, quindi non più sempre espresso;
- è revocabile, senza che questo pregiudichi la liceità dei precedenti trattamenti.

Il consenso: quando deve essere esplicito

È prevista l'esplicita prestazione del consenso per:

- il trattamento di categorie particolari di dati personali;
- la profilazione – altrimenti vietata – dell'interessato;
- non è più richiesta l'autorizzazione del Garante.

ATTENZIONE: ogni stato può mantenere od introdurre ulteriori condizioni per il trattamento di dati genetici, biometrici o dati relativi alla salute

Ipotesi di liceità del trattamento

- Trattamento necessario all'esecuzione di un contratto di cui l'interessato è parte o di misure precontrattuali adottate su richiesta dello stesso;
- trattamento necessario per adempiere un obbligo legale al quale è soggetto il Titolare;
- trattamento necessario per il perseguimento del legittimo interesse del Titolare o di terzi a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato.

Gli incarichi interni in azienda

Il recente Regolamento non prevede espressamente la figura dell'incaricato come era prevista nel Codice Privacy ossia chiunque in un contesto aziendale o altro ente trattasse un dato. L'incaricato era solitamente istruito con regole e istruzioni precise, spesso per iscritto. Nel regolamento si indica espressamente l'obbligo per il titolare di "istruire" chiunque tratti dati all'interno della realtà produttiva

Gli incarichi interni in azienda

Il quarto Paragrafo dell'Articolo 32 sulle misure di sicurezza stabilisce che "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".

Per essi è quindi opportuno redigere delle lettere di incarico con le quali vengano specificati i compiti, le tipologie di dati trattati e le relative modalità dalla raccolta alla conservazione, nonché renderli edotti attraverso le c.d. policy aziendali

Le policy aziendali

Esse sono documenti contenenti istruzioni, regole o indicazioni di comportamento che possano orientare le attività di chi si trova quotidianamente a trattare dati.

La presenza, nella realtà produttiva, di soggetti che trattano i dati che siano istruiti dal titolare o dal responsabile comporta, di default, un innalzamento della sicurezza complessiva dell'ambiente, soprattutto se le regole sono presentate come stringenti e uniformi.

Nell'ottica del GDPR e delle sue misure di sicurezza, importante sarebbe, innanzitutto, far comprendere il "peso" del dato, ossia evidenziare come non tutti i dati siano uguali e, quindi, non tutti debbano essere protetti allo stesso modo

I nuovi obblighi del GDPR rispetto al Codice Privacy

- Obblighi generali
- Obblighi di sicurezza

Obblighi generali

Il Titolare deve:

mappare i rischi e implementare (attraverso il riesame e l'aggiornamento) un sistema con **adeguate misure tecniche/organizzative** idonee a garantire e dimostrare che il trattamento è conforme al Regolamento

-> Responsabilizzazione

Obblighi di sicurezza

Integrità e riservatezza -> principi fondamentali

I dati personali devono essere trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante **misure tecniche ed organizzative adeguate**, da trattamenti non autorizzati od illeciti e dalla perdita, dalla distruzione o dal danno accidentali

Il **GDPR** deve rappresentare **un'opportunità** da cogliere al volo….

Il nuovo sistema privacy deve comportare all'interno di ogni organizzazione un **rafforzamento** e non uno stravolgimento dei presidi esistenti posti a tutela dei dati personali

Considerarlo in una prospettiva di **opportunità** e **scelta strategica** per l'organizzazione è la **soluzione giusta** per aumentare le potenzialità di business, anziché rappresentare un adempimento / costo fine a sé stesso

Le organizzazioni **«GDPR ready»** offrono maggiori garanzie di affidabilità nella gestione dei dati, aumentando il proprio livello reputazionale e di immagine

Dal 25 maggio 2018

cambia la prospettiva sul trattamento dei dati

Il **Codice della Privacy** (approccio formale)

Il **GDPR** (approccio sostanziale)

I principi di “privacy by design” e “privacy by default” impongono a chi gestisce i dati una mappatura dei rischi dei processi privacy al fine di verificare l’adeguatezza delle **misure tecniche** ed **organizzative** adottate

I principi fondamentali introdotti dal GDPR

Il principio di **accountability** impone di considerare:

1. la natura del dato;
2. il contesto in cui opera il titolare / responsabile;
3. la finalità del trattamento;
4. i rischi per i diritti e le libertà dell'interessato

In vista del 25 maggio, dobbiamo chiederci:

- nei rapporti commerciali con i clienti acquisiti / potenziali siamo in grado di garantire di trattare i dati in conformità al GDPR?
- cosa potrebbe accadere se un cliente nazionale / internazionale richiedesse la conformità al GDPR come requisito indispensabile per continuare / instaurare un rapporto commerciale?
- abbiamo valutato con attenzione (in termini economici, d'immagine e reputazionali) le conseguenze per la nostra organizzazione in caso di sospensione / cessazione di un rapporto commerciale rilevante?

- conosciamo davvero il valore dei dati / informazioni che trattiamo?
- siamo certi che i dati in nostro possesso e/o in possesso di terzi siano adeguatamente protetti?
- ci serviamo di terze parti per il trattamento dei dati?
- abbiamo verificato se con i nostri clienti / fornitori abbiamo sottoscritto adeguati contratti per la gestione dei dati (Data Management Agreement) che tutelino la nostra organizzazione in caso di illiceità dei trattamenti?

- utilizziamo in azienda tecnologie biometriche, di videosorveglianza o di localizzazione fisica?
- eseguiamo attività di profilazione della nostra clientela e per quali finalità?
- i nostri clienti possono acquistare i prodotti sul web con l'ausilio di smartphone e/o tablet?
- È necessaria / opportuna la nomina del DPO?

Per rispondere esaurientemente a queste domande è necessaria una **mappatura dei rischi dei processi privacy** dell'organizzazione

Assessment & Gap analysis

Action Plan

1. Adeguare o introdurre misure organizzative;
2. analizzare i processi, formalizzare policy, procedure, lettere di incarico, contratti con responsabili, formazione del personale, etc.;
3. introdurre misure tecniche adeguate (sicurezza adeguata al rischio);
4. analisi preventiva della struttura / garanzie minime da raggiungere:

- pseudonimizzazione
- cifratura dei dati personali o utilizzazione codici identificativi
- integrità
- disponibilità
- resilienza dei sistemi
- ripristino accesso dei dati
- test di valutazione / funzionamento sistemi

Alcune definizioni con cui familiarizzare….

Anonimizzazione (non identificabilità)

Pseudonimizzazione (crittografia)

Esattezza del dato

Portabilità del dato

Data breach (violazione dei dati)

Periodo di conservazione

Il Sistema Privacy si costruisce mediante le seguenti attività

1. Identificare il contesto aziendale

- individuare la tipologia di dati trattati e la finalità del trattamento;
- verificare necessità di eseguire la DPIA ed eventuale Consultazione preventiva

2. adeguare / predisporre la "documentazione privacy"

- predisporre informative al consenso, avvisi, disclaimer, cookies e privacy policy, implementare / adeguare procedure aziendali;
- redazione / revisione doc. contrattuale (dipendenti, clienti, fornitori, professionisti, agenti, procacciatori, etc.);
- valutare l'opportunità / necessità di adottare il "Registro dei trattamenti"

3. Adottare misure di sicurezza, anche organizzative

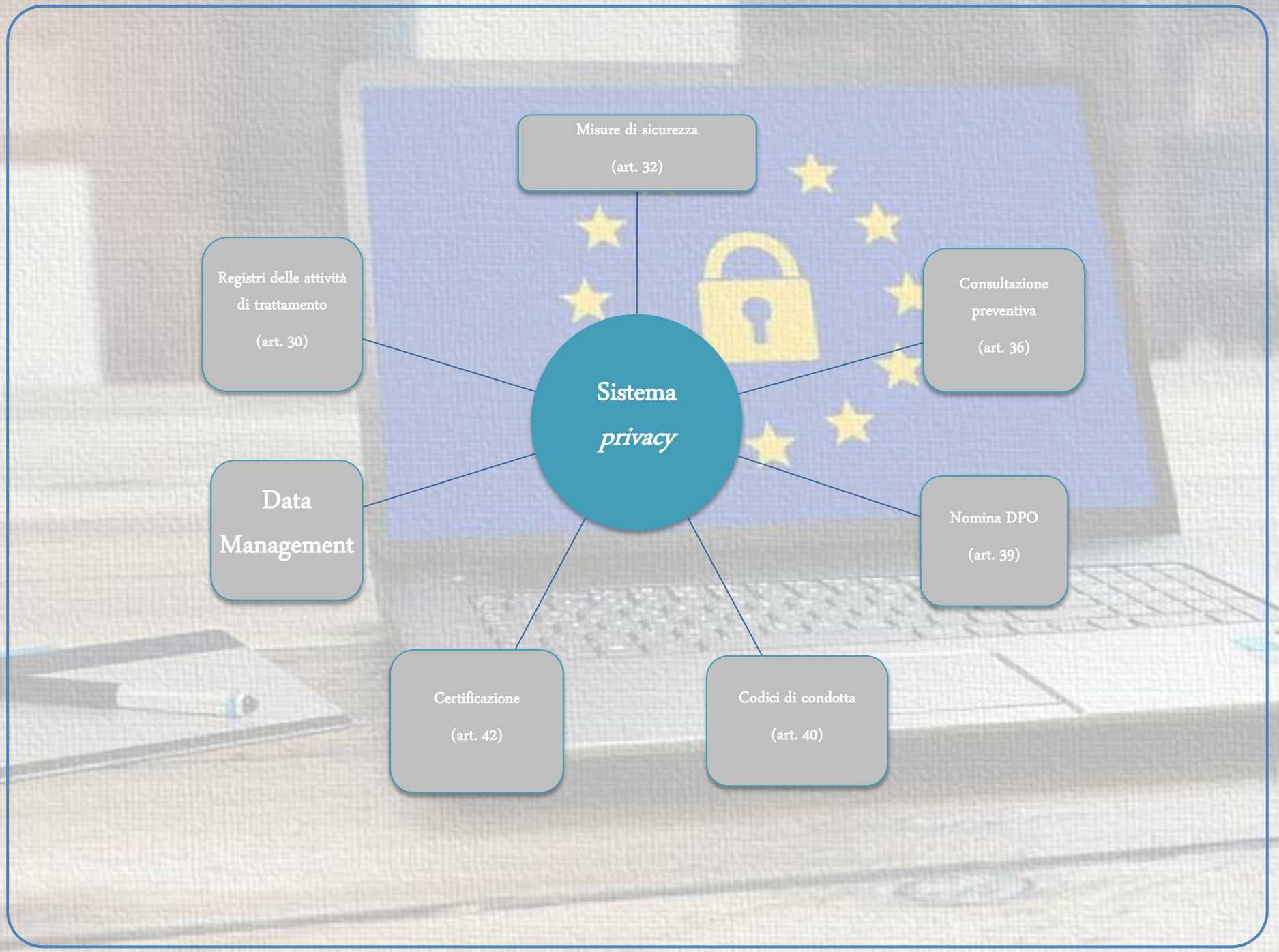
- introdurre dei presidi di controllo nei singoli dipartimenti aziendali;
- eventuale nomina DPO

4. Adottare un sistema di data management

- verificare con il responsabile IT (ove presente) e l'ADS l'adeguatezza dei sistemi informatici;
- gestione tecnica ed organizzativa per data breach, portabilità, conservazione e distruzione dei dati

5. Eseguire controlli sui rapporti interni ed esterni all'azienda

- verificare rapporti con fornitori, agenti, procacciatori, consulenti, professionisti, etc.;
- audit sulle attività illecite, anche potenziali;
- training con e-learning


Misure di sicurezza
(art. 32)
Registri delle attività di trattamento
(art. 30)
Consultazione preventiva
(art. 36)
Sistema
privacy
Data Management
Nomina DPO
(art. 39)
Certificazione
(art. 42)
Codici di condotta
(art. 40)

FASE 1. ASSESSMENT E GAP ANALYSIS

Obiettivi

- Individuare e analizzare i processi e le attività dell'organizzazione in cui sussiste un effettivo profilo di rischio rispetto alle questioni privacy;
- rilevare il relativo sistema di controllo, le eventuali aree di debolezza e le possibili azioni di mitigazione

Attività

- analisi della documentazione normativa e organizzativa aziendale;
- individuazione delle aree a potenziale rischio e relativi referenti aziendali;
- esecuzione di interviste con i referenti identificati;
- formalizzazione del sistema di controllo interno posto in essere per fronteggiare il rischio e analisi dell'adeguatezza dei presidi di controllo;
- definizione delle azioni di rafforzamento / mitigazione dell'attuale sistema di controllo interno e condivisione delle stesse

Deliverable

- matrice di identificazione delle aree di rilevanza privacy;
- gap Analysis;
- action Plan

FASE 2. ADEGUAMENTO DEL SISTEMA

Obiettivi

Adeguamento / aggiornamento, sulla base delle best practice di settore e degli output dell'assessment – gap analysis della documentazione e adempimenti necessari

Attività

- descrizione sistematica dei trattamenti e loro finalità;
- valutazione dei rischi per i diritti e le libertà degli interessati con adozione delle misure tecniche di sicurezza dei dati;
- individuazione dei processi di emergenza e meccanismi per garantire la protezione dei dati;
- valutazione d'impatto Privacy (ove necessaria);
- consultazioni preventive al Garante (ove opportune / necessarie)

Deliverable

- predisposizione della documentazione (informative, nomine, contratti, clausole, cartellonistica, registro delle attività di trattamento, codici di condotta e processi di certificazione, linee guida, policy, etc.);
- nomine figure privacy (incaricati, responsabili, amministratori di sistema, etc.);
- redazione di data management agreement e clausole contrattuali

In base al diverso trattamento dei dati

il GDPR IMPONE o CONSIGLIA

di eseguire un **Data Protection Impact Assessment**

Data Protection Impact Assessment (DPIA)

La valutazione d'impatto sulla protezione dei dati può / deve essere utilizzata dal titolare quando un trattamento (che prevede l'uso di nuove tecnologie) può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, considerati la natura, l'oggetto, il contesto e le finalità del trattamento.

Il processo mira a: 1) individuare la presenza di potenziali rischi sulla sicurezza dei dati e libertà fondamentali, 2) valutare la criticità delle procedure e sistemi utilizzati, 3) prevenire e limitare le conseguenze negative degli eventi-rischio.

Il DPIA è **obbligatorio** nei seguenti casi (art. 35):

- il trattamento, su larga scala, di categorie particolari di dati (art. 9, par.1) che rivelano origine razziale, o etnica, opinioni politiche, religiose o filosofiche, dati genetici, biometrici, relativi alla salute o alla vita o orientamento sessuale della persona;
- la valutazione sistematica e globale di aspetti personali di persone fisiche basata su trattamenti automatizzati, compresa la profilazione;
- la sorveglianza sistematica di una zona accessibile al pubblico su larga scala

1° Fase: Diagnostica

Identificazione e comprensione del perimetro dei dati trattati → Analisi degli adempimenti legali e contrattuali ai fini privacy → Individuazione delle aree di miglioramento ("*Gap Analysis*")

2° Fase: Compliance

Adeguamento della documentazione e delle procedure aziendali → Adeguamento del sistema informatico → Verifica dell'adeguatezza e dell'efficacia operativa del sistema elaborato → Verificare nel tempo il mantenimento del sistema privacy

3° Fase: Formazione

Formazione del personale → Aggiornamento della formazione del personale

Apparato sanzionatorio

Esempi	Violazioni	Sanzioni
Trattamento di dati per tempo indeterminato	Violazione art. 25 GDPR	Sanzione fino a €10.000.000 o annuo di gruppo se superiore
Trattamento illecito di dati	Violazione art. 9 GDPPR	Sanzione fino a €20.000.000 o annuo di gruppo se superiore
Invio di newsletter o materiale senza consenso	Violazione art. 12 comma 1	Sanzione fino a €20.000.000 o annuo di gruppo se superiore
Trattamento dei dati attraverso responsabile in assenza delle GDPR (ad es. assenza	Violazione art. 28 comma 1	Sanzione fino a €10.000.000 o annuo di gruppo se superiore
Assenza di «firewall», tecniche idonee a tutelare la	Violazione art. 32 comma 1	Sanzione fino a €10.000.000 o annuo di gruppo se superiore