GDPR – General Data Protection Regulation

PRIVACYLAB

LA PRIVACY IN UN CLICK

www.privacylab.it

«GDPR- COSA»

1. La Storia
2. Glossario
3. Chi
4. Privacy by Design
5. Informative e gestione del consenso
6. Registri dei trattamenti
7. Data Privacy Impact Assessment
8. Analisi dei rischi
9. Nomina di tutti gli addetti (incaricati, responsabili)
10. Adottare le misure di sicurezza al fine di evitare rischi che incombono sui dati
11. Verifica dei trattamenti esterni
12. Nomina del DPO/RPD – Data Protection officer, Responsabile Protezione Dati
13. Data Breach
14. Gestione dei diritti degli interessati
15. Conclusione

PRIVACYLAB
LA PRIVACY IN UN CLICK

«GDPR- La storia»

Legislazione Precedente
1995 – Direttiva 95/46/EC sulla protezione dei dati personali

Proposta di Riforma
2012 – Proposta iniziale di riforma del quadro legislativo per la protezione dei dati personali in UE

Approvazione e Adozione
2015 – 15 Gennaio - Il Parlamento e il Concilio hanno raggiunto un accordo sul testo finale del GDPR

2016 – 8 Aprile – Adozione da parte del Consiglio dell'Unione Europea
16 Aprile – Adozione da parte del Parlamento Europeo
4 Maggio – Il regolamento è stato pubblicato in Gazzetta Ufficiale
24 Maggio – Il regolamento è entrato in vigore

Applicabilità

2018 – 25 Maggio – Il GPDR entrerà in vigore in tutta l'UE

PRIVACYLAB
LA PRIVACY IN UN CLICK

«GDPR- COSA»

1. La Storia
2. Glossario
3. Chi
4. Privacy by Design
5. Informative e gestione del consenso
6. Registri dei trattamenti
7. Data Privacy Impact Assessment
8. Analisi dei rischi
9. Nomina di tutti gli addetti (incaricati, responsabili)
10. Adottare le misure di sicurezza al fine di evitare rischi che incombono sui dati
11. Verifica dei trattamenti esterni
12. Nomina del DPO/RPD – Data Protection officer, Responsabile Protezione Dati
13. Data Breach
14. Gestione dei diritti degli interessati
15. Conclusione

PRIVACYLAB
LA PRIVACY IN UN CLICK

«GDPR- GLOSSARIO»

GDPR:	General Data Protection Regulation (regolamento generale protezione dei dati)
DPO:	Data Protection Officer (RPD – Responsabile della protezione dei dati)
DPIA:	Data Privacy Impact Assessment Piano impatto sulla sicurezza
DATA BREACH:	Azione da svolgere entro 72 ore per informare il garante ed gli interessati

«GDPR- COSA»

1. La Storia
2. Glossario
3. Chi
4. Privacy by Design
5. Informative e gestione del consenso
6. Registri dei trattamenti
7. Data Privacy Impact Assessment
8. Analisi dei rischi
9. Nomina di tutti gli addetti (incaricati, responsabili)
10. Adottare le misure di sicurezza al fine di evitare rischi che incombono sui dati
11. Verifica dei trattamenti esterni
12. Nomina del DPO/RPD – Data Protection officer, Responsabile Protezione Dati
13. Data Breach
14. Gestione dei diritti degli interessati
15. Conclusione

PRIVACYLAB
LA PRIVACY IN UN CLICK

«GDPR- CHI»

Titolare o Responsabile (intra UE)

Il GDPR si applica al trattamento effettuato da un titolare o responsabile nell'ambito delle attività di uno stabilimento nell'Unione *indipendentemente* che sia effettuato o meno nell'Unione.

Titolare o Responsabile (extra UE)

Il GDPR si applica al trattamento dei dati di interessati che si trovano nell'Unione quando:

- Offerta di beni o servizi, anche gratuiti (*search engine clause*);
- Monitoraggio comportamento in Europa

PRIVACYLAB
LA PRIVACY IN UN CLICK

«GDPR- COSA»

1. La Storia
2. Glossario
3. Chi
4. Privacy by Design
5. Informative e gestione del consenso
6. Registri dei trattamenti
7. Data Privacy Impact Assessment
8. Analisi dei rischi
9. Nomina di tutti gli addetti (incaricati, responsabili)
10. Adottare le misure di sicurezza al fine di evitare rischi che incombono sui dati
11. Verifica dei trattamenti esterni
12. Nomina del DPO/RPD – Data Protection officer, Responsabile Protezione Dati
13. Data Breach
14. Gestione dei diritti degli interessati
15. Conclusione

PRIVACYLAB
LA PRIVACY IN UN CLICK

«GDPR- COME – PRIVACY BY DESIGN»

ART. 25 Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

a) il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, volte ad attuare in modo efficace i principi di protezione dei dati

b) 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.

c) Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti

«GDPR- COSA»

1. La Storia
2. Glossario
3. Chi
4. Privacy by Design
5. Informative e gestione del consenso
6. Registri dei trattamenti
7. Data Privacy Impact Assessment
8. Analisi dei rischi
9. Nomina di tutti gli addetti (incaricati, responsabili)
10. Adottare le misure di sicurezza al fine di evitare rischi che incombono sui dati
11. Verifica dei trattamenti esterni
12. Nomina del DPO/RPD – Data Protection officer, Responsabile Protezione Dati
13. Data Breach
14. Gestione dei diritti degli interessati
15. Conclusione

PRIVACYLAB
LA PRIVACY IN UN CLICK

«GDPR- COME - informative»

Codice Privacy

Art. 13

Documento **rivolto all'interessato** volto a fargli comprendere quale sarà l'utilizzo dei dati personali. Deve specificare :

(i)finalità del trattamento;

(ii)modalità di effettuazione;

(iii)natura obbligatoria o facoltativa del trattamento;

(iv)conseguenze del rifiuto a fornire dati;

(v)limiti alla comunicazione e diffusione dati;

(vi)modalità di esercizio dei diritti individuali;

(vii)identificazione precisa di titolare e responsabile.

NB: in caso di **trattamento di dati sensibili**, l'informativa è necessariamente **scritta**, così **come il relativo consenso**.

Regolamento Europeo

Art. 13

La definizione base non cambia, diventano tuttavia necessari elementi diversi e più dettagliati:

(i)identificazione precisa del titolare e del suo rappresentante (titolare extra-UE);

(ii)eventuali contatti DPO;

(iii)finalità trattamento e base giuridica;

(iv)eventuali legittimi interessi del titolare;

(v)destinatari o categorie di destinatari;

(vi)trasferimenti dati e garanzie di tutela.

NB: viene inoltre richiesta anche una serie di **ulteriori specifiche** a **garanzia di correttezza e trasparenza del trattamento** (art. 13, comma 2).

«GDPR- COME - consenso»

Codice Privacy

Art. 23

Elemento **scriminante** tra **utilizzo lecito** e **illecito** dei dati personali da parte di un titolare di trattamento. Il **consenso è validamente e prestato quando è:**

(i)libera e specifica espressione di volontà;

(ii)riferito a un trattamento individuato in maniera chiara;

(iii) documentato per iscritto (*ad probationem*);

(iv) manifestato per iscritto in caso di trattamento di dati sensibili (*ad substantiam*);

(v)fornita informativa *ex* art. 13 del Codice Privacy;

NB: art. 24 disciplina i casi di **esonero dal consenso**

Regolamento Europeo

Art. 7

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

1. **Titolare in gradi di dimostrare il consenso**
2. **Richiesta chiara, comprensibile**
3. **Revoca in qualsiasi momento**
4. **Valutazione consenso presupposto ad esecuzione di contratti**

5. **Art. 8: prevede norme stringenti per il consenso prestato dai minori**

PRIVACYLAB
LA PRIVACY IN UN CLICK

«GDPR- COSA»

1. La Storia
2. Glossario
3. Chi
4. Privacy by Design
5. Informative e gestione del consenso
6. Registri dei trattamenti
7. Data Privacy Impact Assessment
8. Analisi dei rischi
9. Nomina di tutti gli addetti (incaricati, responsabili)
10. Adottare le misure di sicurezza al fine di evitare rischi che incombono sui dati
11. Verifica dei trattamenti esterni
12. Nomina del DPO/RPD – Data Protection officer, Responsabile Protezione Dati
13. Data Breach
14. Gestione dei diritti degli interessati
15. Conclusione

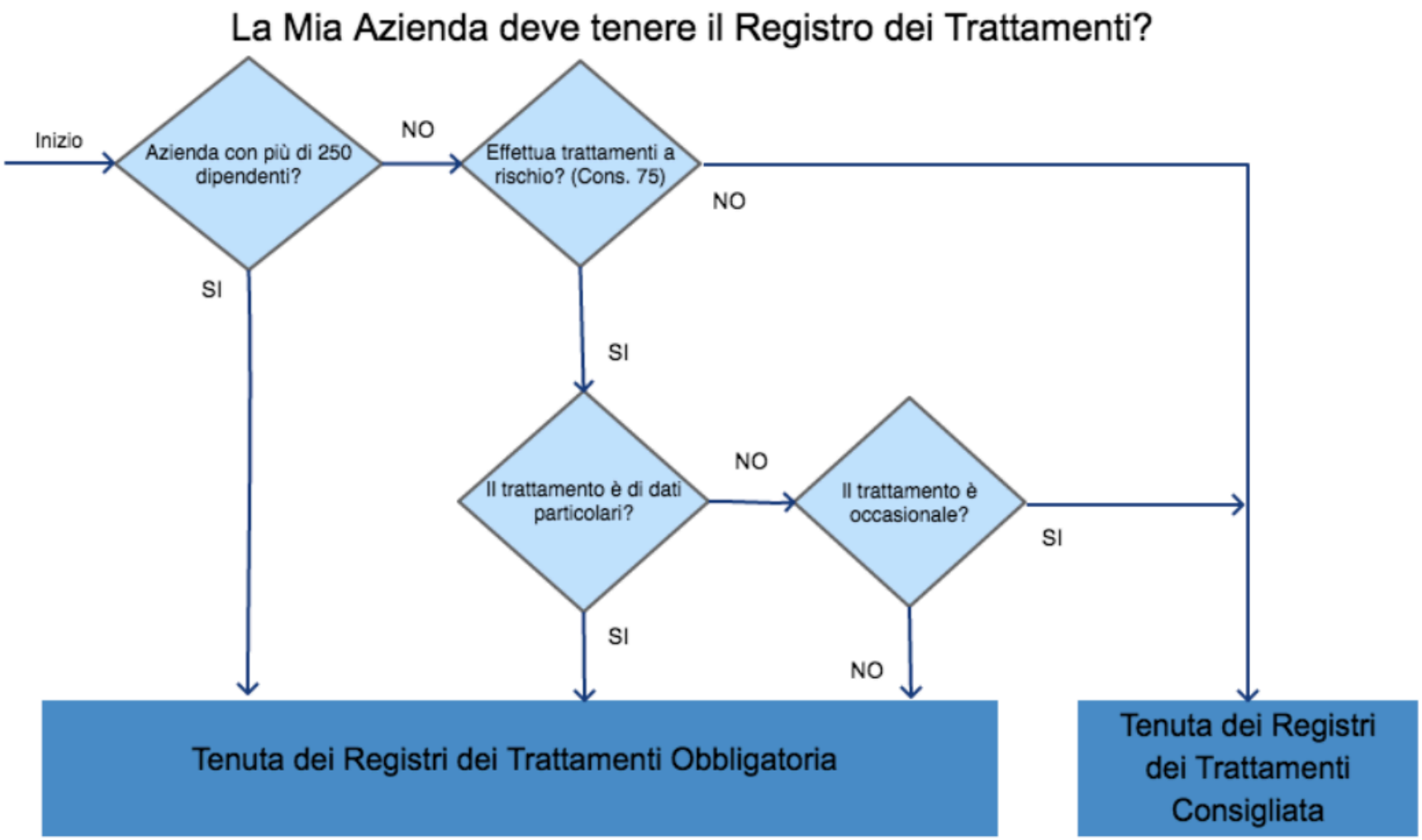
PRIVACYLAB
LA PRIVACY IN UN CLICK

«GDPR- COME –REGISTRI»

- **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
   b) le finalità del trattamento;
   c) una descrizione delle categorie di interessati e delle categorie di dati personali per comunicazione e o diffusione
   d) ove applicabile, i trasferimenti di dati personali verso un paese terzo
   e) ove possibile, i termini ultimi previsti per la cancellazione
   f) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32

«GDPR- COME -registro»



PRIVACYLAB
LA PRIVACY IN UN CLICK

«GDPR- COSA»

1. La Storia
2. Glossario
3. Chi
4. Privacy by Design
5. Informative e gestione del consenso
6. Registri dei trattamenti
7. Data Privacy Impact Assessment
8. Analisi dei rischi
9. Nomina di tutti gli addetti (incaricati, responsabili)
10. Adottare le misure di sicurezza al fine di evitare rischi che incombono sui dati
11. Verifica dei trattamenti esterni
12. Nomina del DPO/RPD – Data Protection officer, Responsabile Protezione Dati
13. Data Breach
14. Gestione dei diritti degli interessati
15. Conclusione

PRIVACYLAB
LA PRIVACY IN UN CLICK

«GDPR- COME - pia»

IL PRIVACY IMPACT ASSESSMENT (PIA) È L'ANALISI DEI RISCHI SUI DATI TRATTATI PER I TRATTAMENTI

- occorre verificare di quali dati parliamo e della loro natura,
- occorre verificarne le finalità al trattamento e le modalità,
- chi sono le figure che internamente possono trattare queste informazioni e con quali autorizzazioni,
- se i dati vengono comunicati a terzi oppure vengono diffusi.
- Inoltre occorre verificare la reale ubicazione dei dati: se sono fuori dalla Comunità Europea si deve verificare che lo Stato ospitante abbia le carte in regola con la normativa Europea.
- Una volta verificati i dispositivi ospitanti il titolare al trattamento deve verificarne la messa in sicurezza, andando in modo puntuale a verificarne gli aspetti tecnici ed organizzativi.

DOPO l'analisi dei rischi che possono incombere su questi dati e solo a questo punto potrà arrivare alla **corretta decisione** "del se e del come" trattare i dati.

«GDPR- COME- esempi»

Esempi di lavorazione	Possibili criteri	DPIA richiesta?
Il trattamento dei dati genetici e di salute dei pazienti in un ospedale (sistema informativo dell'ospedale).	I dati sensibili Dati relativi interessati vulnerabili	Si
L'uso di un sistema di telecamere per monitorare il comportamento di guida in autostrada. Il titolare prevede di utilizzare un sistema di analisi video intelligente per individuare autoveicoli e riconoscere automaticamente le targhe.	Il monitoraggio sistematico L'uso innovativo o l'applicazione di soluzioni tecnologiche o organizzative	
Una società che monitora le attività dei suoi dipendenti inclusa la loro postazione di lavoro, attività internet, ecc	Il monitoraggio sistematico I dati relativi interessati vulnerabili	
La raccolta di dati dai profili social usate da compagnie private per generare profili per database di contatti	Valutazione o assegnazione di un punteggio I dati trattati su larga scala	
Una rivista online utilizza una mailing list per inviare un sommario giornaliero generico ai suoi abbonati.	Nessuno	Non necessariamente
Un sito di e-commerce visualizza annunci pubblicitari di auto d'epoca includendo una limitata profilazione ispirata al passato comportamento d'acquisto su alcune parti del proprio sito Web.	Valutazione o assegnazione di un punteggio, ma non sistematica o estesa	

PRIVACYLAB
LA PRIVACY IN UN CLICK

«GDPR- COSA»

1. La Storia
2. Glossario
3. Chi
4. Privacy by Design
5. Informative e gestione del consenso
6. Registri dei trattamenti
7. Data Privacy Impact Assessment
8. Analisi dei rischi
9. Nomina di tutti gli addetti (incaricati, responsabili)
10. Adottare le misure di sicurezza al fine di evitare rischi che incombono sui dati
11. Verifica dei trattamenti esterni
12. Nomina del DPO/RPD – Data Protection officer, Responsabile Protezione Dati
13. Data Breach
14. Gestione dei diritti degli interessati
15. Conclusione

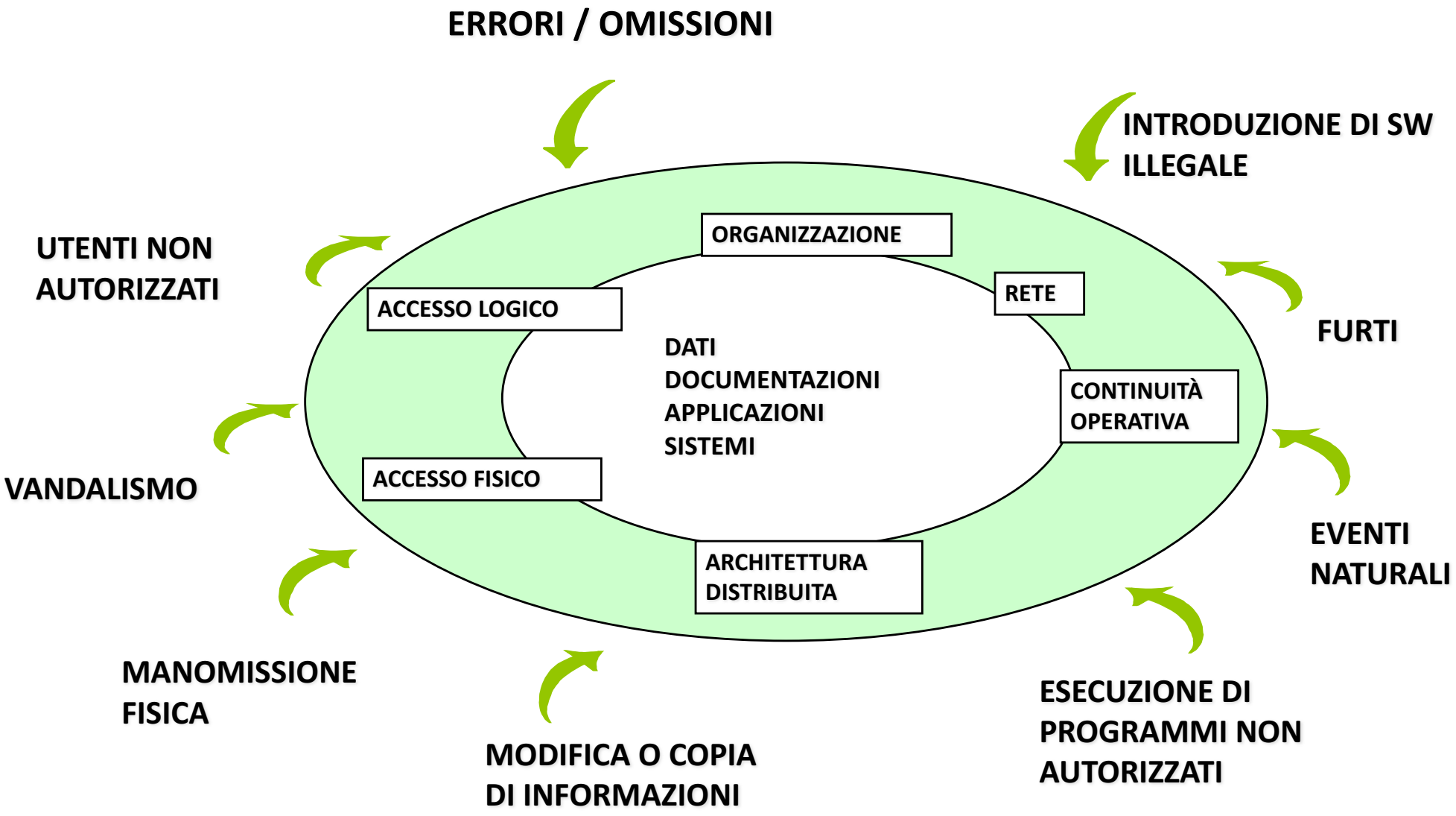
PRIVACYLAB
LA PRIVACY IN UN CLICK

«GDPR- COME – i rischi»

I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare:

se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; **se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza**;
in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione 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, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

«GDPR- COME – minacce»



PRIVACYLAB
LA PRIVACY IN UN CLICK

«GDPR- COSA»

1. La Storia
2. Glossario
3. Chi
4. Privacy by Design
5. Informative e gestione del consenso
6. Registri dei trattamenti
7. Data Privacy Impact Assessment
8. Analisi dei rischi
9. Nomina di tutti gli addetti (incaricati, responsabili)
10. Adottare le misure di sicurezza al fine di evitare rischi che incombono sui dati
11. Verifica dei trattamenti esterni
12. Nomina del DPO/RPD – Data Protection officer, Responsabile Protezione Dati
13. Data Breach
14. Gestione dei diritti degli interessati
15. Conclusione

PRIVACYLAB
LA PRIVACY IN UN CLICK

«GDPR- Addetti»

Articolo 28
Definizioni Art 4

PRIVACYLAB
LA PRIVACY IN UN CLICK

«GDPR- Addetti»

Panoramica sul nuovo *General Data Protection Regulation* (GDPR)

- *Informazioni da fornire all'interessato / 2*

I soggetti che trattano i dati ed i loro compiti principali

Codice Privacy *Artt. 28, 29 e 30*	Regolamento Europeo *Artt. 24, 26, 27, 28 e 29*
• **Titolare:** *persona/e giuridica pubblica o privata che decide in merito alle modalità di trattamento dati personali in piena autonomia.* • **Responsabile:** *persona/e fisica o giuridica che viene designata dal titolare facoltativamente per il compimento di attività di trattamento specifico.* • **Incaricato:** *persona/e fisiche incaricate di porre in essere le operazioni tecniche di trattamento per il titolare o il responsabile.*	• **Titolare:** • **Responsabile** Definizione **formale** non cambia rispetto al Codice Privacy, tuttavia vengono introdotte regole e principi volti a **rafforzare l'autonomia negoziale delle parti nell'esatta allocazione delle responsabilità di ogni soggetto privacy.** • **Incaricato:** Pur non prevedendo espressamente la **figura dell' "incaricato" del trattamento** (ex art. 30 Codice), il regolamento **non ne esclude** la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile" *(si veda, in particolare, art. 4, n. 10, del regolamento)*.

PRIVACYLAB
LA PRIVACY IN UN CLICK

«GDPR- COSA»

1. La Storia
2. Glossario
3. Chi
4. Privacy by Design
5. Informative e gestione del consenso
6. Registri dei trattamenti
7. Data Privacy Impact Assessment
8. Analisi dei rischi
9. Nomina di tutti gli addetti (incaricati, responsabili)
10. Adottare le misure di sicurezza al fine di evitare rischi che incombono sui dati
11. Verifica dei trattamenti esterni
12. Nomina del DPO/RPD – Data Protection officer, Responsabile Protezione Dati
13. Data Breach
14. Gestione dei diritti degli interessati
15. Conclusione

PRIVACYLAB
LA PRIVACY IN UN CLICK

«GDPR- COME – le contromisure»

Il grado di sicurezza si valuta attraverso le **contromisure** che si sono applicate per proteggere i dati personali dalle minacce individuate

PRIVACYLAB
LA PRIVACY IN UN CLICK

«GDPR- COME – le contromisure»

- Le misure di sicurezza da implementare devono essere dimensionate in funzione delle minacce.
- L'organizzazione determina le proprie misure di sicurezza in relazione al fattore di rischio residuo che intende sostenere.
- I criteri adottati possono essere:
  - Bilanciare il costo di sicurezza contro il valore dei beni da proteggere e gli obblighi di legge
  - Bilanciare i bisogni di sicurezza contro i bisogni del business
  - Bilanciare probabilità contro possibilità

«GDPR- COSA»

1. La Storia
2. Glossario
3. Chi
4. Privacy by Design
5. Informative e gestione del consenso
6. Registri dei trattamenti
7. Data Privacy Impact Assessment
8. Analisi dei rischi
9. Nomina di tutti gli addetti (incaricati, responsabili)
10. Adottare le misure di sicurezza al fine di evitare rischi che incombono sui dati
11. Verifica dei trattamenti esterni
12. Nomina del DPO/RPD – Data Protection officer, Responsabile Protezione Dati
13. Data Breach
14. Gestione dei diritti degli interessati
15. Conclusione

PRIVACYLAB
LA PRIVACY IN UN CLICK

«GDPR- COME – Responsabili»

Quando prendiamo un dato personale e lo comunichiamo a qualcun altro stiamo facendo un trattamento

Se facciamo un trattamento dobbiamo applicare tutte le misure fisiche ed organizzative per far si che al dato non succeda nulla di male

La scelta dell'intermediario a cui comunichiamo fa parte di questo processo ed è sotto la responsabilità del Titolare

«GDPR- COME – Responsabili»

Art 28

Deve operare con Contrattualizzazione

Responsabile deve garantire misure tecniche

Istruzioni documentate

Garanzia sugli addetti/incaricati alla riservatezza

Adotti misure di sicurezza (Art. 32)

PRIVACYLAB
LA PRIVACY IN UN CLICK

«GDPR- COSA»

1. La Storia
2. Glossario
3. Chi
4. Privacy by Design
5. Informative e gestione del consenso
6. Registri dei trattamenti
7. Data Privacy Impact Assessment
8. Analisi dei rischi
9. Nomina di tutti gli addetti (incaricati, responsabili)
10. Adottare le misure di sicurezza al fine di evitare rischi che incombono sui dati
11. Verifica dei trattamenti esterni
12. Nomina del DPO/RPD – Data Protection officer, Responsabile Protezione Dati
13. Data Breach
14. Gestione dei diritti degli interessati
15. Conclusione

PRIVACYLAB
LA PRIVACY IN UN CLICK

«GDPR- COME – DPO»

Sarà obbligatorio nella pubblica amministrazione e sarà fortemente consigliato nel privato.

Nel settore privato, tuttavia, sarà obbligatorio nominare un DPO qualora i trattamenti coinvolti saranno su larga scala e monitorati sistematicamente o nel caso di trattamenti effettuati su larga scala di dati sensibili. Accanto al concetto di larga scala occorre far riferimento al core business aziendale per determinarne l'obbligatorietà o meno:

le aziende ospedaliere,
le aziende che offrono servizi proprietari in cloud,
le aziende che offrono servizi di sorveglianza,

«GDPR- COME – DPO compiti»

- **informare e fornire consulenza al titolare del trattamento** o al responsabile del trattamento nonchè ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonchè da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- **sorvegliare l'osservanza del presente regolamento**, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonchè 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;
- **fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati** e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
- **cooperare con l'autorità di controllo;**
- **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.

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.

«GDPR- COME – DPO»

DPO

l DPO avrà quindi autonomia di spesa finalizzata al raggiungimento e mantenimento di standard idonei di conformità del proprio Modello Organizzativo Privacy e per la propria formazione continua, e sarà un soggetto indipendente all'interno della propria organizzazione, in quanto gli unici soggetti ai quali sarà tenuto a riportare, saranno solo coloro che rappresentano il "più alto livello di gestione".

Il DPO potrà essere sia un soggetto interno che un professionista esterno, purché in assenza di conflitto di interessi, non potrà essere rimosso o penalizzato nell'esercizio dei suoi compiti, e non si pone nessuna limitazione al suo mandato.

Una società con più filiali (un "gruppo di imprese") può designare un unico DPO a condizione che questo soggetto sia "facilmente accessibile da ogni stabilimento".

PRIVACYLAB
LA PRIVACY IN UN CLICK

«GDPR- COME – le contromisure»

DPO

l DPO è responsabile:

- della sensibilizzazione (informare e consigliare),
- del controllo
- della formazione
- del supporto strategico (contribuire a PIA e risk assessment)
- della rappresentanza (verso il Garante)

IL RUOLO NON SEMBRA ESSERE OPERATIVO

Quindi Chi fa le cose?????

PRIVACYLAB
LA PRIVACY IN UN CLICK

«GDPR- COME – DPO»

Posto che il DPO, deve essere designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati, e della capacità di adempiere ai compiti che gli sono assegnati.

- Le certificazioni ad oggi rilasciate da Enti qualificati relative alla figura professionale di Privacy Officer e Consulente della Privacy rappresentano un concreto strumento di misurazione delle competenze ma non equivalgono ad una vera e propria "abilitazione" allo svolgimento del ruolo previsto dalla nuova normativa comunitaria.

«GDPR- COME – DPO»

Il Data Protection Officer avrà competenze normative sul trattamento dei dati personali e competenze sui processi informatici, ma se nominato internamente all'organizzazione

NON potrà svolgere mansioni che possano andare in conflitto d'interesse come ad esempio la figura dell'IT Manager.

«GDPR- COSA»

1. La Storia
2. Glossario
3. Chi
4. Privacy by Design
5. Informative e gestione del consenso
6. Registri dei trattamenti
7. Data Privacy Impact Assessment
8. Analisi dei rischi
9. Nomina di tutti gli addetti (incaricati, responsabili)
10. Adottare le misure di sicurezza al fine di evitare rischi che incombono sui dati
11. Verifica dei trattamenti esterni
12. Nomina del DPO/RPD – Data Protection officer, Responsabile Protezione Dati
13. Data Breach
14. Gestione dei diritti degli interessati
15. Conclusione

PRIVACYLAB
LA PRIVACY IN UN CLICK

«GDPR- COME – Data Breach»

ART 33 e ART 34

PRIVACYLAB
LA PRIVACY IN UN CLICK

«GDPR- COME – Data Breach»

I dati personali conservati, trasmessi o trattati da aziende e pubbliche amministrazioni possono essere soggetti al rischio di perdita, distruzione o diffusione indebita,

ad esempio a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi, come incendi o altre calamità.

ESISTE obbligo di comunicare eventuali violazioni di dati personali(data breach) all'Autorità stessa e, in alcuni casi, anche ai soggetti interessati. Il mancato o ritardato adempimento della comunicazione espone alla possibilità di sanzioni amministrative.

«GDPR- COME – Data Breach»

In caso di violazione dei dati personali, il titolare o il responsabile del trattamento notifica la violazione all'autorità di controllo competente ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza

descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonchè le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

descrivere le probabili conseguenze della violazione dei dati personali;

descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

VA FATTO SEMPRE

PRIVACYLAB
LA PRIVACY IN UN CLICK

«GDPR- COSA»

1. La Storia
2. Glossario
3. Chi
4. Privacy by Design
5. Informative e gestione del consenso
6. Registri dei trattamenti
7. Data Privacy Impact Assessment
8. Analisi dei rischi
9. Nomina di tutti gli addetti (incaricati, responsabili)
10. Adottare le misure di sicurezza al fine di evitare rischi che incombono sui dati
11. Verifica dei trattamenti esterni
12. Nomina del DPO/RPD – Data Protection officer, Responsabile Protezione Dati
13. Data Breach
14. Gestione dei diritti degli interessati
15. Conclusione

PRIVACYLAB
LA PRIVACY IN UN CLICK

«GDPR- COME – Data Breach»

Comunicazione di una violazione dei dati personali all'interessato

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo

SI PUO' EVITARE SE :

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura

b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

«GDPR- COSA»

1. La Storia
2. Glossario
3. Chi
4. Privacy by Design
5. Informative e gestione del consenso
6. Registri dei trattamenti
7. Data Privacy Impact Assessment
8. Analisi dei rischi
9. Nomina di tutti gli addetti (incaricati, responsabili)
10. Adottare le misure di sicurezza al fine di evitare rischi che incombono sui dati
11. Verifica dei trattamenti esterni
12. Nomina del DPO/RPD – Data Protection officer, Responsabile Protezione Dati
13. Data Breach
14. Gestione dei diritti degli interessati
15. Conclusione

PRIVACYLAB
LA PRIVACY IN UN CLICK

«GDPR- GLOSSARIO»

GDPR:	General Data Protection Regulation (regolamento generale protezione dei dati)
DPO:	Data Protection Officer (RPD – Responsabile della protezione dei dati)
DPIA:	Data Privacy Impact Assessment Piano impatto sulla sicurezza
DATA BREACH:	Azione da svolgere entro 72 ore per informare il garante ed gli interessati

PRIVACYLAB
LA PRIVACY IN UN CLICK

«GDPR- MINESTRONE – riassunto»

Sanzioni severe:
multe fino a

4% del fatturato globale

€20 mln

tra le due la maggiore.

Il regolamento si applica anche alle **società non UE** che trattano dati di individui in UE

Il **trasferimento internazionale di dati** sarà regolato dalle norme del GDPR

Si amplia la categoria di **dati personali**

genetici

mentali

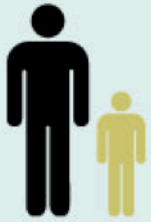
culturali

economici

di identità sociale

La richiesta di consenso per il trattamento dei dati personali deve essere chiara e ricevere risposta affermativa

SI'



Il consenso dei genitori è richiesto per il trattamento di **dati personali di minori** di 16 anni

I data subjects hanno **diritto all'oblio** e alla cancellazione dei record

Gli utenti possono richiedere copia dei **dati in un formato utilizzabile**

PRIVACYLAB
LA PRIVACY IN UN CLICK

«GDPR- COSA»

1. La Storia
2. Glossario
3. Chi
4. Privacy by Design
5. Informative e gestione del c
6. Registri dei trattamenti
7. Data Privacy Impact
8. Analisi dei rischi
9. Nomina di tu esponsabili)
10. Adottare ne di evitare rischi che incombono sui d
11. V erni
12. Data Protection officer, Responsabile
13. D
14. Ges i diritti degli interessati
15. Conc ione