GDPR Compliance Program - Pilot Project Italy Overview

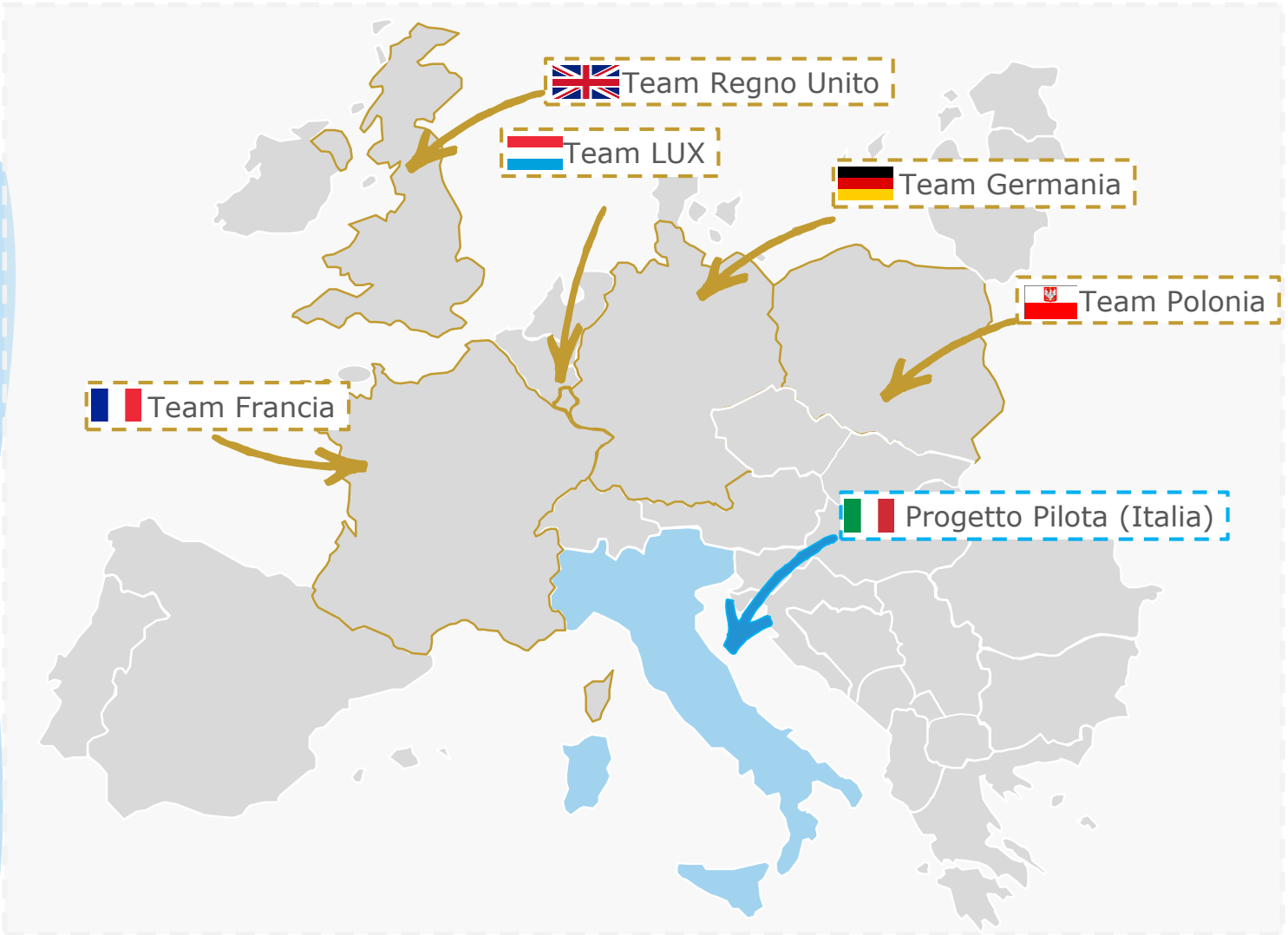
Agenda

Overview del Progetto di Gruppo

L'avviamento del Progetto di Gruppo…

Nell'ottobre 2017, Ferrero ha avviato un ampio Progetto di Gruppo finalizzato alla valutazione del livello di adeguatezza del sistema di gestione dei dati adottato rispetto al con il Regolamento 2016/679 ("GDPR"), alla definizione del Registro dei trattamenti, di una Gap Analysis e del Piano di Conformità.

Il progetto è stato avviato allo scopo di identificare le azioni di rimedio necessarie al fine di raggiungere la conformità con il GDPR. ***Il progetto è guidato dal Lussemburgo e coinvolge i Paesi europei. L'Italia è stata scelta come Progetto Pilota.***



Stato di Avanzamento

Nell'ambito del Progetto di Gruppo, il team italiano ha concluso le attività e ha condiviso con Ferrero Italia i risultati finali ed i deliverable di progetto

Timeline Progetto di Gruppo

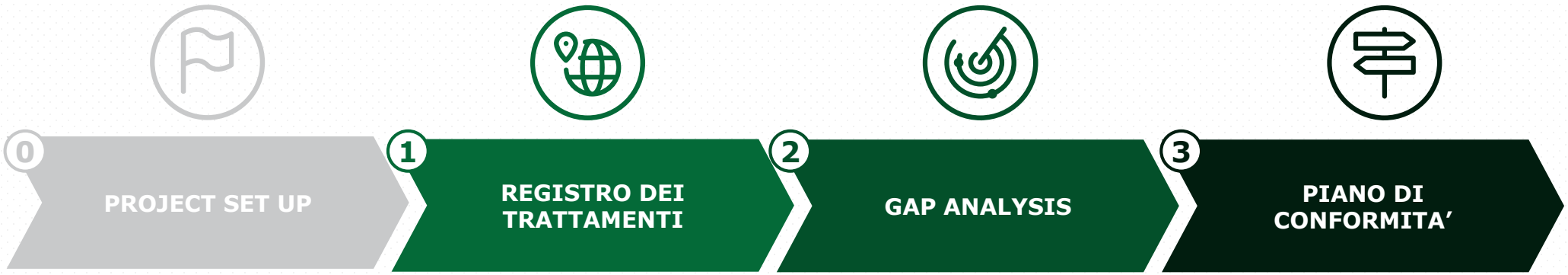
Overview del Progetto Pilota (Italia)

Deloitte GDPR Pilot Project: Attività e deliverable

FASI PROGETTUALI

L'esecuzione del Progetto Pilota (Italia) ha visto il coinvolgimento di Deloitte Italia. Il Progetto Pilota ha comportato lo svolgimento delle seguenti attività:

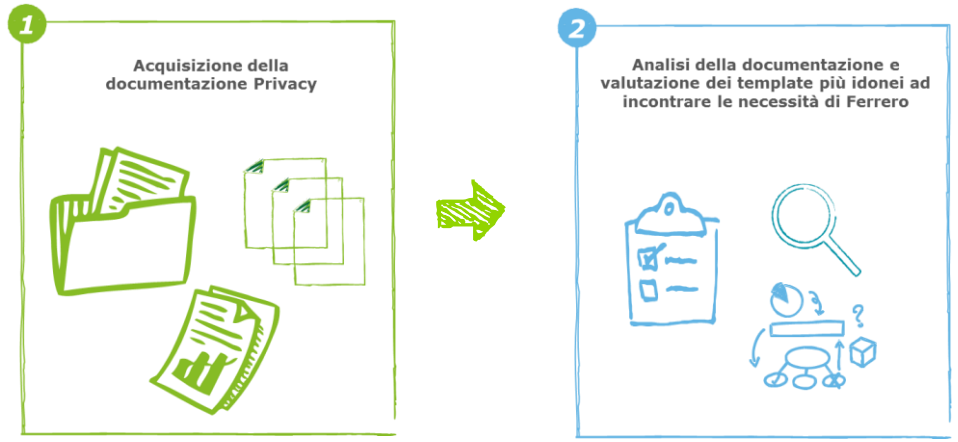
- **Project Set Up:** Il Progetto Pilota (Italia) si è innestato sulle attività già avviate da Ferrero nei mesi precedenti ai fini del raggiungimento della compliance con il GDPR.
- **Registro dei trattamenti: consolidamento e finalizzazione dei Registri di Ferrero**
- **Gap Analysis**: assessment con riferimento al *framework* normativo delineato dal GDPR
- **Piano di Conformità**: identificazione delle macro aree di intervento e delle azioni di rimedio, classificazione delle stesse in base al loro livello di priorità (alta, media, bassa)



Fase 0: Project Set Up

Attività svolte

- **Coordinamento con i Team Lussemburghesi**, con particolare riferimento a:
  a. Definizione dei *template* di progetto (i.e. Registro dei Trattamenti, Gap Analysis, Piano di Conformità)
  b. Allineamento periodico con i Team di lavoro Deloitte Lux/Ferrero Lux (es. conference call settimanali, etc.)
- **Acquisizione della documentazione** (oltre 400 documenti, es std contratti, informative..) definita da Ferrero Italia a seguito della pubblicazione del GDPR ai fini della compliance con il nuovo *framework* normativo



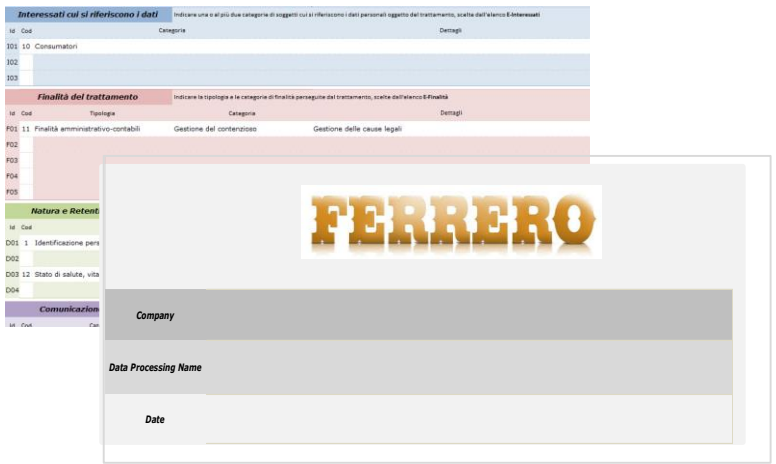
Deliverable

- **Template** del Registro dei trattamenti
- **Template** della Gap Analysis
- **Template** del Piano di Conformità

Fase 1: Registro dei trattamenti

Attività svolte

- Analisi del livello di conformità di Ferrero Italia, attraverso **analisi documentale e interviste** con le figure chiave dell'organizzazione
- **Identificazione e analisi dei principali processi** aziendali che comportano il trattamento di dati personali
- Analisi dei Registri dei Trattamenti forniti da Ferrero Italia. **Consolidamento e formalizzazione** del *deliverable*

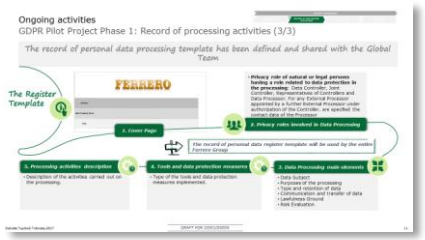


Template Registro dei Trattamenti

Deliverable

- **Consolidamento** dei Registri dei trattamenti

Il Registro, definito alla luce dei requisiti previsti all'art. 30 GDPR, contiene una descrizione dei principali elementi del trattamento di dati svolti dalle società del Gruppo Ferrero Italia



Il Registro dei Trattamenti verrà messo a disposizione degli Amministratori Delegati e Referenti Privacy delle società appartenenti al Gruppo Ferrero Italia per condivisione e validazione

In caso di ispezioni, il Registro dei Trattamenti dovrà essere messo a disposizione dell'Autorità Garante per la Protezione dei Dati Personali

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Fase 2: Gap Analysis

Attività svolte

- **Analisi** dell'attuale livello di compliance di Ferrero Italia ai principali requisiti del GDPR - attraverso attività di **analisi documentale e interviste** privacy

> 400 DOCUMENTI ACQUISITI

...LIANCE
...Supporting documentation

1. Premesse Generali
2. Story Board
3. DPS e Misure Sicurezza Tecnico Organizzative
4. Valutazioni di Impatto sulla protezione trattamento dati
5. Registro Trattamento dati
6. Azioni remediation
7. Policies
8. Tavolo Privacy
9. Norme e Procedure ambito IT
10. Privacy Std
11. Privacy Awareness
12. Nomine

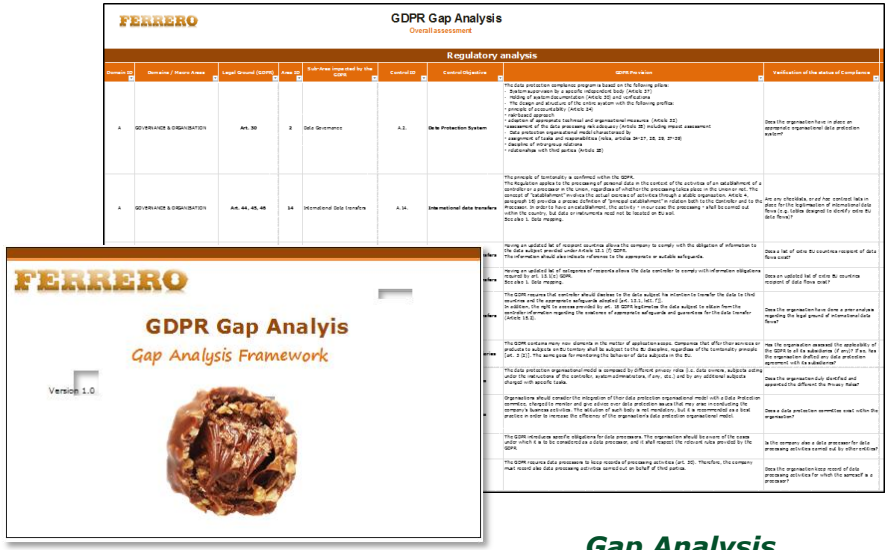
GDPR COMPLIANCE
IT Supporting documentation

A. Amministratori di Sistema
B. Elenco Applicativi & DB_Privacy Relevant
C. Encryption_Elenco Applicativi & DB
D. Security Baseline Measures
E. Security Baseline_Cloud Computing
F. Analisi dei Rischi Data Protection
G. Piano di Sicurezza IT
H. Assessment IT
I. Verifiche Ambito 231 & Rischi Informatici
L. Sistemi in DR & BCRS
M. Ultimo VA-PT
N. Videosorveglianza
Document Retention Schedule.txt
ITOO-PL016 Gestione dei Log.txt
ITOO-PL021 Esecuzione degli audit sull'utilizzo della strumentazione informatica.txt
Norme.zip
Policy per la classificazione e gestione dei documenti_Secret Unit.txt
Procedure.zip

Documentazione prodotta da Ferrero Italia

Deliverable

- **Gap Analysis Report**: il documento è volto ad analizzare e descrivere la situazione esistente (As-Is) e ad individuare i disallineamenti rispetto al GDPR
- L'analisi ha riguardato le attività svolte nonché la documentazione definita da Ferrero nell'ambito del programma di compliance al GDPR
- **Dall'analisi svolta è stata riscontrata maturità nel Modello Organizzativo Privacy delineato da Ferrero Italia**



Gap Analysis

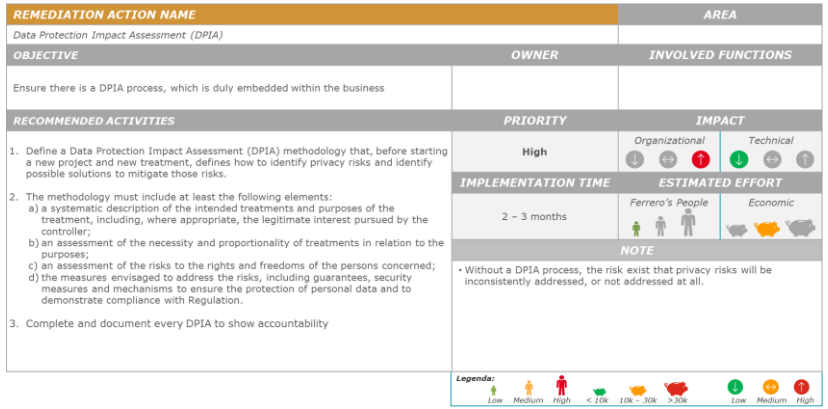
Fase 3: Piano di Conformità

Attività svolte

- Identificazione delle **aree di intervento** per Ferrero Italia, sulla base di un'analisi comparata tra la situazione As-Is ed i requisiti target definiti dal GDPR

Deliverable

- **Piano di Conformità**: il documento mira ad identificare le **Aree di Intervento**, evidenziate e raggruppate per priorità (Alta, Media, Bassa) da implementare – anche in coordinamento con il Gruppo – nei prossimi mesi (entro il 25 Maggio 2018) al fine di ulteriormente rafforzare il livello di maturità del Modello Organizzativo privacy di Ferrero e definire un sistema di gestione dei dati conforme al GDPR



REMEDIATION ACTION NAME		AREA
Data Protection Impact Assessment (DPIA)		
OBJECTIVE	OWNER	INVOLVED FUNCTIONS
Ensure there is a DPIA process, which is duly embedded within the business		
RECOMMENDED ACTIVITIES	PRIORITY	IMPACT
1. Define a Data Protection Impact Assessment (DPIA) methodology that, before starting a new project and new treatment, defines how to identify privacy risks and identify possible solutions to mitigate those risks. 2. The methodology must include at least the following elements: a) a systematic description of the intended treatments and purposes of the treatment, including, where appropriate, the legitimate interest pursued by the controller; b) an assessment of the necessity and proportionality of treatments in relation to the purposes; c) an assessment of the risks to the rights and freedoms of the persons concerned; d) the measures envisaged to address the risks, including guarantees, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with Regulation. 3. Complete and document every DPIA to show accountability	High	Organizational / Technical
IMPLEMENTATION TIME		ESTIMATED EFFORT
2 – 3 months		Ferrero's People / Economic
NOTE		
• Without a DPIA process, the risk exist that privacy risks will be inconsistently addressed, or not addressed at all.		

Legenda: Low Medium High < 10k 10k – 30k >30k Low Medium High

Piano di Conformità

Le principali Aree di Intervento per Ferrero nel suo percorso per la compliance al GDPR (1/2)

AREE DI INTERVENTO

Area di Intervento	Descrizione dell'Area di Intervento
1. DATA PROTECTION IMPACT ASSESSMENT (solo per trattamenti a rischio elevato)	• **Soltanto alcuni dei trattamenti identificati dovranno essere soggetti a DPIA:** secondo l'art. 35 GDPR, la valutazione d'impatto sulla protezione dei dati è necessaria solo per i trattamenti a **rischio elevato** • La metodologia DPIA dovrà essere definita in coerenza con le **Linee Guida di Gruppo,** in corso di definizione
2. POLICY DATA RETENTION (definizione/implementazione)	• Il titolare deve **definire il periodo di conservazione** dei dati trattati. Il GDPR richiede che i dati personali siano conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (art. 5 GDPR) • Dovrà essere definita, **in conformità alla Linee Guida del Gruppo,** una policy in materia di **data retention.** I principi di data retention dovranno essere implementati attraverso l'adozione di **misure tecniche**
3. DIRITTI DEGLI INTERESSATI (definizione/implementazione)	• Il GDPR attribuisce agli **interessati** i **diritti** di seguito elencati: diritto di accesso, diritto di rettifica, diritto alla cancellazione, diritto di limitazione, diritto alla portabilità dei dati, diritto di opposizione (artt. 15-22 GDPR) • Ferrero Italia dovrà definire una procedura e adottare misure tecniche e organizzative appropriate al fini di facilitare l'esercizio dei diritti da parte degli interessati
4. DATA BREACH MANAGEMENT (definizione/implementazione)	• Il GDPR richiede al titolare di essere in grado di reagire prontamente in caso di data breach • Ferrero Italia dovrà definire e implementare **un sistema di gestione dei data breach** coerente con **le Linee Guida di Gruppo**, in corso di definizione, e attuare adeguate misure tecniche e organizzative per garantire una pronta reazione

Le principali Aree di Intervento per Ferrero nel suo percorso per la compliance al GDPR (2/2)

AREE DI INTERVENTO

Area di Intervento	Descrizione dell'Area di Intervento
5. ANALISI DEL RISCHIO	• L'art. 32 richiede al titolare del trattamento di adottare misure di sicurezza adeguate ai rischi presentati dal trattamento • Ferrero dovrà definire e adottare una **metodologia di analisi del rischio**, coerente con le linee guida definite a livelli di Gruppo, **al fine di valutare e affrontare i rischi** e attuare adeguate misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio.
6. GESTIONE DELLE TERZE PARTI	• Ferrero dovrà rafforzare i presidi sulla filiera dei fornitori mediante: i) **mappatura di tutte le terze parti** coinvolte nel trattamento; ii) **revisione e integrazione dei relativi contratti** alla luce dei requisiti di cui all'art. 28 GDPR, prevedendo clausole volte ad assicurare che i responsabili/sub-responsabili rispettino le previsioni del GDPR e contestualmente si impegnino ad assicurare lo stesso livello di protezione dei dati applicato da Ferrero; iii) attività di **monitoraggio** (ad es. anche attraverso ispezioni periodiche).
7. FORMALIZZAZIONE DEL MODELLO PRIVACY e della NOMINA del DPO	• Ferrero potrà valutare la possibilità di formalizzare l'adozione del Modello Organizzativo Privacy e la nomina del DPO tramite una delibera del Consiglio di Amministrazione. Tale opzione, in linea con la best practice, rappresenta un elemento chiave per il titolare del trattamento al fine di dimostrare la propria *accountability*

Consapevolezza e sinergie rappresentano elementi chiave …

… per il raggiungimento degli obiettivi entro il 25 maggio 2018

Principali Impatti del GDPR – Cosa cambia

Registro del trattamento ✓
Il regolamento introduce l'obbligo di istituire, anche in formato elettronico, e mantenere aggiornato un registro dei trattamenti effettuati

Informative
Viene rafforzato l'obbligo di fornire informative semplici e chiare al fine di consolidare il controllo degli interessati rispetto al trattamento dei propri dati personali

Diritti degli interessati
Il titolare deve facilitare l'esercizio diritti (accesso, cancellazione, portabilità, limitazione, opposizione) da parte degli interessati.

Misure tecniche e organizzative
Il titolare deve adottare misure tecniche ed organizzative comparando rischi individuati e misure di contrasto per minimizzarli

Sanzioni
La riforma ha incrementato in modo significativo le sanzioni derivanti dall'inosservanza delle disposizioni del GDPR, sino ad un massimo di 20M o al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore

Gestione delle terze parti
Il GDPR chiede una selezione accorta delle terze parti e il loro assoggettamento a clausole di responsabilità

Data Protection Officer ✓
Viene introdotta la figura del DPO, avente il compito di sorvegliare l'osservanza del Regolamento, fornire consulenza al titolare nonché fungere da contatto con il Garante o gli interessati

Privacy Impact Assessment
Viene introdotto l'obbligo per ciascun titolare di svolgere e di documentare, un' autovalutazione del rischio derivante dai trattamenti effettuati e, sulla base degli esiti di tale analisi, di effettuare una eventuale consultazione preventiva con l'Autorità garante

Data breach notification
Determinate violazioni di dati devono essere segnalate sia al Garante che agli interessati senza ritardo e in alcuni casi entro 72 ore dal momento in cui ne si viene a conoscenza

Privacy by design and by default
Il titolare deve implementare misure tecniche e organizzative adeguate al fine di proteggere i dati sin dalla progettazione, e garantire che siano trattati solo i dati personali necessari per ogni specifica finalità del trattamento