MARSH RISK CONSULTING
RISK. DISPUTES. STRATEGY.

FNOVI
FEDERAZIONE NAZIONALE
ORDINI VETERINARI ITALIANI

Federazione Nazionale Ordini Veterinari Italiani

IL REGOLAMENTO EUROPEO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI - GDPR

Sessione Formativa

Roma, 19 Dicembre 2018

MARSH

Programma del corso

- **Introduzione**
- Principali Definizioni
- Principali impatti
- Contesto normativo
- Documentazione per l’adeguamento GDPR

Introduzione (1/2)

Che cosa è il GDPR?	Il GENERAL DATA PROTECTION REGULATION (GDPR) rappresenta il Regolamento Europeo in materia di protezione dei dati personali.
Qual è l'obiettivo?	Armonizzare le attività di trattamento dei dati, in maniera più omogenea e trasparente, così da assicurare la libera circolazione dei dati personali, ma soprattutto proteggere i diritti e le libertà fondamentali delle persone fisiche.
A chi si applica?	Il GDPR si applica a tutti gli Stati membri e si rivolge ad organizzazioni, associazioni, enti pubblici, liberi professionisti, aziende coinvolte nel Trattamento dei Dati Personali.
Quali sono le principali implicazioni?	Il GDPR sostituisce la precedente direttiva 95/46/CE, recepita nel Codice Privacy (D.lgs. 196/2003) come modificato dal D.Lgs. 101/2018 ed introduce nuove indicazioni sulla protezione dei dati personali, rafforzando il principio di responsabilizzazione dei Titolari e Responsabili del Trattamento.
Dove si applica?	Il GDPR si applica al trattamento dei dati personali, effettuato o meno all'interno dell'UE, da un Titolare o Responsabile del trattamento nell'UE / non nell'UE, che offre beni o servizi, anche gratuitamente, ad Interessati nell'UE o svolge monitoraggio del comportamento svolto da interessati nell'UE.

Introduzione (2/2)

Direttiva 1995/46/CE

Direttiva 2009/136/CE

Regolamento 2016/679/EU

- Carattere di obbligatorietà
- Direttamente applicabile nei Paesi EU

24 maggio 2016:
Entrata in vigore in EU

25 maggio 2018:
Applicazione disposizioni GDPR

D.Lgs. 196/2003:
- Codice in materia di protezione dei Dati Personali
- Provvedimenti del Garante

D.Lgs. 69/2012:
- Codice in materia di protezione dei Dati Personali e tutela della vita privata nel settore delle comunicazioni elettroniche

Atto di Governo n. 22 «Schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679»:
- **10 maggio 2018:** Atto di Governo sottoposto a parere parlamentare
- **22 maggio 2018:** Atto di Governo sottoposto a parere del Garante

D.Lgs. 101/2018:
- Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)

Programma del corso

- Introduzione
- **Principali Definizioni**
- Principali impatti
- Contesto normativo
- Documentazione per l’adeguamento GDPR

Principali Definizioni
Art. 4 GDPR (1/3)

- **Dato personale ex art. 4 GDPR:**

Con l'espressione *dato personale* si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento **a un identificativo** come il nome, **un numero di identificazione**, **dati relativi all'ubicazione**, **un identificativo online** o a uno o più elementi caratteristici della **sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale**

Categorie particolari di dati ex art. 9 GDPR:
Si tratta dei dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona

Dati personali relativi a condanne penali e reati ex art. 10 GDPR:
Si tratta di dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza

Principali Definizioni
Art. 4 GDPR (2/3)

➢ **Interessato**	Persona fisica a cui si riferiscono i dati personali oggetto del trattamento/dei trattamenti, ovvero il proprietario dei suoi dati.
➢ **Trattamento**	Qualsiasi operazione applicata a dati personali, come raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, limitazione, cancellazione o distruzione.
➢ **Titolare del trattamento**	Persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.
➢ **Responsabile del trattamento**	Persona fisica o giuridica, autorità pubblica, servizio od organismo che tratta dati personali per conto del Titolare del trattamento.
➢ **Responsabile della Protezione dei Dati (RPD)**	Responsabile della Protezione dei dati (RPD) designato al monitoraggio del corretto adempimento dei requisiti normativi in tema di Data Protection, coinvolto ogniqualvolta sia necessario effettuare valutazioni in merito ai processi di trattamento dei dati personali.

Principali Definizioni
Art. 4 GDPR (3/3)

➢ **Profilazione**	Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi ad una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.
➢ **Consenso**	Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.
➢ **Violazione dei dati personali (Data Breach)**	La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati trasmessi, conservati o comunque trattati.

Programma del corso

- Introduzione
- Principali Definizioni
- **Principali impatti**
- Contesto normativo
- Documentazione per l’adeguamento GDPR

Principali impatti

Le nuove disposizioni introducono una serie di **impatti** in termini **organizzativi, operativi e tecnologici**, oltre che un approccio alla **Data Privacy**, fondato sul principio del *Rischio associato alla valutazione delle misure applicate ai dati trattati*.

Ambito	Esempi di Impatti	Aree di Intervento
Misure Tecnologiche	• Adozione di misure tecnologiche in ambito Data Protection (adozione di pseudonimia, cifratura dati, etc.) • Abilitazione misure di monitoraggio per rilevazione di Data Breach • Adeguamento misure protezione di accesso ai Dati Sensibili (presenza di Dati Biometrici, etc.)	• Data Governance (Mappatura Dati, Owner e tipologie di accessi) • Cyber Threat Intelligence (monitoraggio attacchi Cyber) • Implementazioni Tecnologiche
Modello Operativo	• Recepimento delle disposizioni relative ai diritti degli Interessati (Richiesta di Modifica, Diritto all'Oblio, etc.) all'interno dell'attuale modello di Privacy • Adozione principio di Privacy by Default e Privacy by Design all'interno del processo di IT Change Management	• Gestione della Raccolta, Modifica e Cancellazione dei dati trattati (Clienti, Dipendenti, Terze Parti) • Adozione dei principi privacy all'interno del Processo di sviluppo di prodotti/servizi
Organizzazione / Risk Management	• Revisione Ruoli e Responsabilità per Titolare e Responsabili del trattamento, Verifica nomina del RPD (Responsabile della protezione dei dati) • Valutazione delle misure dei trattamenti sulla base dei Rischi associati ai Dati trattati (esecuzione di un DPIA – Data Protection Impact Assessment) • Valutazione esposizione rischi relativi a Terze Parti o dipendenti; • Revisione dell'attuale impianto delle Policy e Procedure di Sicurezza e Privacy	• Modello Organizzativo (introduzione RPD) e Modello di gestione Compliance • Predisposizione DPIA • Verifiche termini contrattuali verso Clienti, Dipendenti e Terze Parti

Programma del corso

- Introduzione
- Principali Definizioni
- Principali impatti
- **Contesto normativo**
- Documentazione per l’adeguamento GDPR

Contesto normativo
Panoramica – principali cambiamenti

1. Perimetro

La riforma coinvolge tutti gli Stati UE e chiunque tratti dati di cittadini europei.

2. Responsabilità

Viene disciplinato in modo più dettagliato il ruolo di responsabile del Trattamento.

3. Informazioni chiare

Viene rafforzato l'obbligo di fornire informative semplici e chiare al fine di rafforzare il controllo degli interessati.

4. Diritto all'oblio

Diritto dell'interessato di ottenere dal titolare del trattamento la cancellazione dei dati personali al ricorrere di determinate specifiche ipotesi.

5. Portabilità dei dati

Diritto alla portabilità del dato che permette all'interessato di ricevere i propri dati su un formato strutturato e leggibile e/o di farli trasmettere da un titolare all'altro.

6. Privacy by design & by default

Il titolare deve implementare misure idonee a proteggere i dati sin dal momento di determinazione dei mezzi di trattamento e garantire solo il trattamento dei dati necessari al perseguimento di specifiche finalità per cui sono raccolti.

7. 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 dalla violazione.

8. Data Protection Impact Assessment

Obbligo per ciascun titolare di svolgere, e documentare, una autovalutazione del rischio derivante dai trattamenti effettuati e, sulla base degli esiti delle analisi, di effettuare una consultazione preventiva con l'Autorità garante.

9. Responsabile della Protezione dei dati (RPD)

Responsabile della Protezione dei dati (RPD) addetto a: sorvegliare l'osservanza delle disposizioni privacy, fornire consulenza e pareri, fungere da contatto con il Garante o gli interessati.

10. Registri del trattamento

Obbligo di conservare, anche in formato elettronico, un registro dei trattamenti effettuati, contenente alcuni specifici dettagli.

11. Sanzioni

Sino ad un massimo di € 20.000.000 o al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Contesto normativo
Punti Chiave del Regolamento UE (1/4)

	Elementi chiave	*Obblighi*
Principi e Disposizioni Generali **(Art. 5, 6, 7, 8, 9)**	Principi applicabili al trattamento di dati: • Liceità, correttezza e trasparenza • Limitazione della finalità • Minimizzazione dei dati • Esattezza • Limitazione della conservazione • Integrità e riservatezza • Responsabilizzazione del Titolare del Trattamento **Principio di Liceità del Trattamento e definizione delle condizioni di validità del Consenso.** Divieto di trattamento dei «dati sensibili» se non a determinate condizioni.	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, ed essere in grado di dimostrare, che **il trattamento è effettuato conformemente al Regolamento.**
Diritti degli Interessati **(Art.15, 16, 17, 18, 20, 21, 22)**	Tipologia di diritto: • Diritto di accesso • Diritto di rettifica • Diritto alla cancellazione («diritto all'oblio») • Diritto di limitazione di trattamento • Diritto alla portabilità dei dati • Diritto di opposizione • Diritto di revoca del consenso • Diritto di proporre un reclamo all'Autorità di Controllo Definizione di norme relative alla Profilazione e Marketing Diretto sui dati personali trattati.	Il Titolare del Trattamento adotta misure appropriate per fornire all'Interessato tutte le **informazioni** relative al trattamento e in forma **concisa, trasparente, intellegibile e facilmente accessibile**, **con linguaggio semplice e chiaro**, nonché attua misure tecniche ed organizzative per favorire e garantire l'esercizio dei diritti ed il riscontro alle richieste presentate dagli Interessati.

Contesto normativo
Punti Chiave del Regolamento UE (2/4)

	Elementi chiave	*Obblighi*
Privacy by Design & Privacy by Default **(Art. 25)**	*Privacy by Design* – Protezione dei dati dalla progettazione *Privacy by Default* – Protezione dei dati per impostazione predefinita Introduzione del tema della «Minimizzazione» dei dati raccolti. Adozione di Misure Tecniche e Organizzative che garantiscano la protezione dei dati trattati.	Tenendo conto dello stato dell'arte, dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi per i diritti e le libertà dell'Interessato, il Titolare del Trattamento adotta un **sistema di protezione dei dati personali fin dalla progettazione e misure tecniche a protezione di tali dati, per impostazione predefinita,** al fine di trattare solo i dati personali necessari per ogni specifica finalità del trattamento.
Registro dei Trattamenti **(Art. 30)**	Ogni Titolare e Responsabile del Trattamento tiene un registro delle attività di trattamento contenente: • nome e dati di contatto di Titolare del trattamento, del rappresentante del Titolare e del RPD • finalità del trattamento • descrizione delle categorie di interessati e delle categorie di dati • destinatari a cui i dati sono stati o saranno comunicati; • trasferimenti di dati verso un paese terzo o un'organizzazione internazionale • data retention • misure di sicurezza tecniche e organizzative adottate.	Strumento fondamentale, sia in formato cartaceo che in formato elettronico, per l'eventuale supervisione da parte dell'Autorità di Controllo nonchè per la predisposizione di un quadro aggiornato dei trattamenti posti in essere dal Titolare del Trattamento o dal Responsabile del Trattamento, come anche per la valutazione ed analisi del rischio. **Il Registro è un adempimento obbligatorio per le imprese o organizzazioni con più di 250 dipendenti.**

Contesto normativo
Principio di liceità

Secondo l'art. 6 GDPR, il trattamento è lecito solo se e nella misura in cui ricorre almeno una di queste condizioni:

- Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso
- Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento
- Il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica
- Il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento
- Il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è minore

Contesto normativo
Informativa & Consenso

Le informazioni contenute nell'informativa devono essere precise ed esposte con un linguaggio chiaro.
L'informativa deve contenere le seguenti informazioni:

- identità e dati di contatto del Titolare del trattamento
- dati di contatto del RPD/Privacy Focal Point/Ufficio Privacy
- finalità del trattamento e base giuridica del trattamento
- eventuali destinatari/categorie di destinatari dei dati personali
- possibilità di trasferimento dei dati a terzi
- periodo di conservazione dei dati trattati
- diritti dell'interessato
- possibilità di revocare il consenso
- diritto di proporre un reclamo all'autorità di controllo
- conseguenze della mancata comunicazione del dato.

La richiesta del consenso deve essere presentata in modo distinto da altre richieste, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro → l'interessato ha il diritto di revocare il consenso in qualsiasi momento.

Consenso ✓
- Barrare apposita casella
- Firma

N.B. la revoca del consenso non pregiudica la liceità del trattamento basato sul consenso prestato prima di tale revoca; il consenso è revocato con la stessa facilità con cui è accordato.

Contesto normativo
Punti Chiave del Regolamento UE (3/4)

	Elementi chiave	*Obblighi*
Misure di Sicurezza **(Art. 32)**	Adozione di Misure Tecniche e Organizzative: • pseudonimizzazione e cifratura dei dati personali • assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento • capacità di ripristinare la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico • procedura per testare, verificare e valutare l'efficacia delle misure tecniche e organizzative.	- Nomine degli Amministratori di Sistema - Esposizione della cartellonistica di informativa minima per dispositivi di videosorveglianza - Nomina del Responsabile per la Videosorveglianza - Adozione di specifiche procedure IT.
Notifica del data breach **(Art. 33, 34)**	• Introduzione della Responsabilità di Notifica verso l'Autorità di Controllo; • Comunicazione di una violazione dei dati personali all'interessato, qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica violata.	In caso di data breach, il Titolare del trattamento **notifica la violazione all'Autorità di Controllo competente** senza ingiustificato ritardo **entro 72 ore** dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà degli Interessati.
Valutazione d'impatto sulla protezione dei dati **(Art. 35)**	La valutazione dell'impatto sulla protezione dei dati (*Data Protection Impact Assessment)* è richiesta in caso di: • valutazione sistematica e globale di aspetti personali dell'Interessato basata su trattamento automatizzato e sulla quale si fondano decisioni aventi effetti giuridici od incidono significativamente • trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e a reati • sorveglianza sistematica di una zona accessibile al pubblico.	A seguito di Risk Assessment**, se il trattamento presenta un rischio elevato per i diritti e le libertà** degli Interessati, prima di procedere al trattamento, si esegue obbligatoriamente la **valutazione d'impatto sulla protezione dei dati.** Il Titolare del Trattamento, prima di procedere al trattamento, **consulta l'Autorità di Controllo** qualora la valutazioni indichi che il trattamento presenterebbe un rischio elevato in assenza di misure per attenuare il rischio.

Contesto normativo
Punti Chiave del Regolamento UE (4/4)

	Elementi chiave	*Obblighi*
Responsabile Protezione dei dati (RPD) (Art. 37-39)	Introduzione della figura Responsabile della Protezione dei dati (RPD) per supportare il Titolare e il Responsabile del Trattamento nonché vigilare sulla corretta adozione del GDPR e cooperare con le autorità di controllo.	Testo di nomina del RPD. Modello di comunicazione al Garante dei Dati del RPD
Codice di Condotta & Certificazioni (Art. 40 -43)	Introduzione dei requisiti di dettaglio su formalizzazione e contenuti dei Codici di Condotta e Monitoraggio degli aggiornamenti. Introduzione di norme per enti certificatori e modalità di certificazione.	Stati Membri, Autorità di controllo, Comitato e Commissione incoraggiano: - Associazioni/organismi rappresentanti di Titolari e Responsabili nell'elaborazione di codici di condotta per la corretta applicazione del GDPR - Istituzioni di meccanismi di certificazione della protezione dei dati per conformità al GDPR (volontaria e accessibile).
Trasferimento dati verso Paesi terzi o organizz. internaz. (Art. 44-50)	Principio generale per il trasferimento Trasferimento sulla base di una decisione di adeguatezza Introduzione delle Norme per il trasferimento dei Dati Personali (per esempio dovuti ad adozione di servizi in Cloud extra EU o utilizzo di servizi di Outsourcing extra EU o relazioni extra EU che comportano trasferimento degli stessi).	Il Titolare del Trattamento deve informare l'Interessato **dell'intenzione,** Sua o del Responsabile del Trattamento, **di trasferire dati personali verso un paese terzo o verso un'organizzazione internazionale.** Deve inoltre comunicare **l'esistenza o l'assenza di una decisione di adeguatezza della Commissione e,** nei casi di trasferimento aventi garanzie adeguate o norme vincolanti di impresa o deroghe in specifiche situazioni, **il riferimento alle garanzie appropriate o opportune ed i mezzi per ottenere copia dei dati o il luogo dove sono ubicati.**

Contesto normativo
Responsabile della Protezione dei Dati

Il Titolare del Trattamento e il Responsabile del Trattamento designano sistematicamente un Responsabile della Protezione dei dati (RPD) ogniqualvolta:

- il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico;
- le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
- le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono nel trattamento, su larga scala.

Il RPR è Incaricato <u>almeno</u> dei seguenti compiti:
- Informare e fornire consulenza al Titolare del trattamento o al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR
- Sorvegliare l'osservanza del GDPR
- Fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati
- Cooperare con l'Autorità di Controllo
- Fungere da punto di contatto per l'Autorità di Controllo per questioni connesse al trattamento

Contesto normativo
Sanzioni in caso di non conformità

Le nuove Disposizioni introducono delle **condizioni generali per infliggere sanzioni amministrative pecuniarie** ex art. 83 GDPR e **sanzioni** più elevate in caso di inadempienza da parte di Titolari e Responsabili:

SANZIONI:

Sanzioni **fino a € 20 M** o il **4% del fatturato** totale globale dell'anno precedente se superiore

Mancato rispetto degli articoli	• **5, 6, 7, 9** (principi base del trattamento, comprese le condizioni del consenso)
	• **12 - 22** (diritti degli interessati)
Inosservanza di un ordine impartito dall'Autorità ex art. 68 par. 2 lett. 1) GDPR	• **44 - 49** (trasferimenti dati personali in un paese terzo/organizzazione internazionale)

ALTRE SANZIONI:

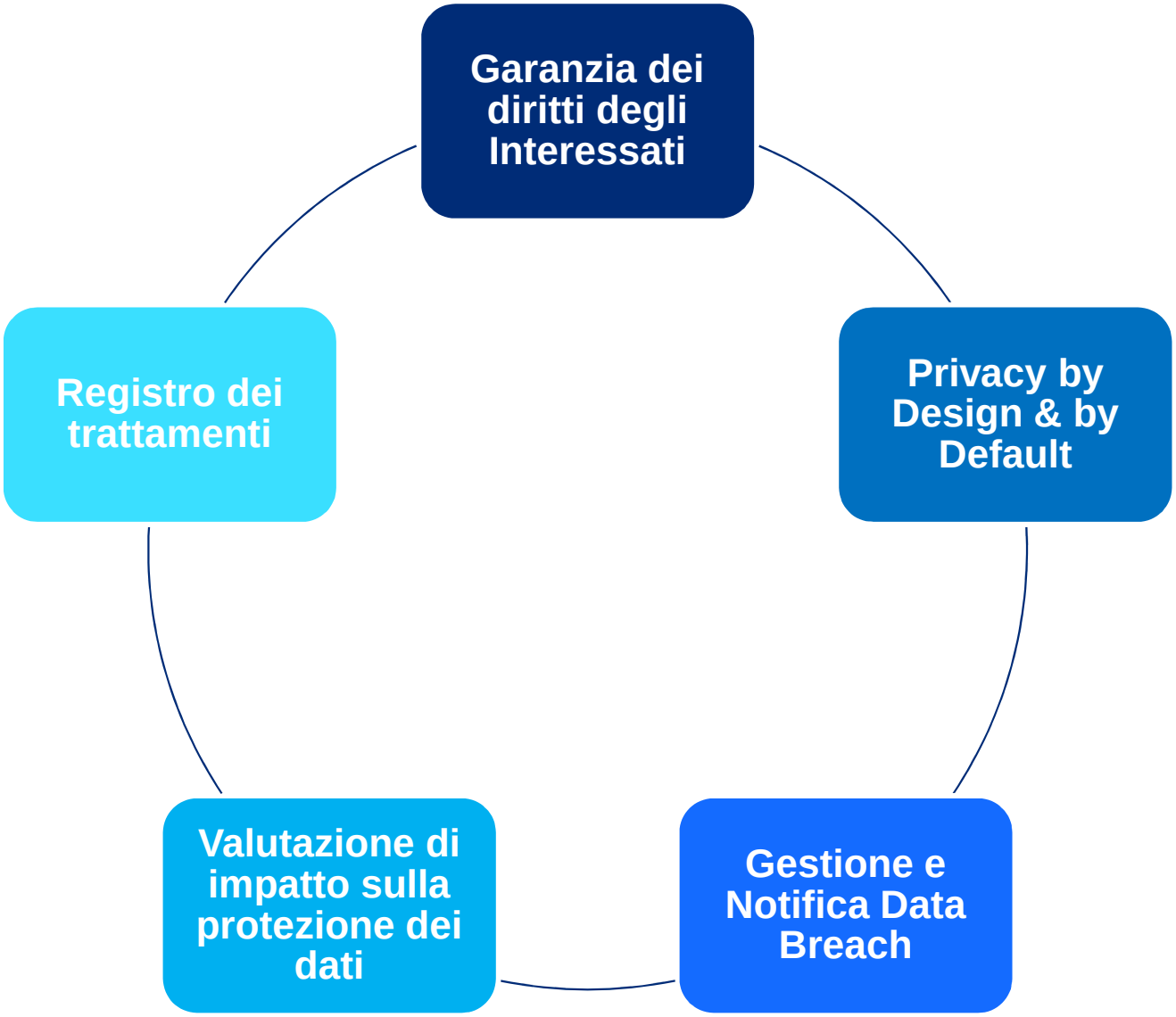
Sanzioni **fino a € 10 M** o il **2% del fatturato** totale globale dell'anno precedente se superiore

Mancato rispetto degli articoli	• **8, 11, 25 - 39** (obblighi del Titolare e del Responsabile del trattamento)
	• **42, 43** (obblighi dell'organismo di certificazione)
	• **41, par. 4** (obblighi dell'Organismo di Controllo)

Programma del corso

- Introduzione
- Principali Definizioni
- Principali impatti
- Contesto normativo
- **Documentazione per l’adeguamento GDPR**

Documentazione per l’adeguamento al GDPR



Procedura «Garanzia dei Diritti degli Interessati»

Articolo di riferimento	• Artt. 15, 16, 17, 18, 20 e 21 GDPR, art. 7 par. 3 e art. 77
Figure coinvolte	• Titolare del trattamento • Responsabile della Protezione dei Dati • Responsabile del Trattamento
Obiettivo	• Attuazione di misure tecniche ed organizzative per favorire e garantire l'esercizio dei diritti ed il riscontro alle richieste presentate dagli Interessati, rispondendo entro 1 mese dalla richiesta pervenuta (anche in caso di diniego), estendibili fino a 3 mesi in caso di particolare complessità
Sintesi dei contenuti	• Tipologia di diritto: - Diritto di accesso - Diritto di rettifica - Diritto alla cancellazione («diritto all'oblio») - Diritto di limitazione di trattamento - Diritto alla portabilità dei dati - Diritto di opposizione - Diritto di revoca del consenso - Diritto di proporre un reclamo all'Autorità di Controllo • Attività di gestione dell'istanza

Procedura «Privacy by Design & by Default»

Articolo di riferimento	• Art. 25 Regolamento 679/2016
Figure coinvolte	• Titolare del trattamento • Responsabile della Protezione dei dati
Obiettivo	• Creare un sistema di protezione dei dati personali fin dalla progettazione e protezione degli stessi per impostazione predefinita, attraverso misure tecniche ed organizzative adeguate così da trattare solo i dati personali necessari per ogni specifica finalità del trattamento, tutelando i diritti degli interessati
Sintesi dei contenuti	• Per ciascun processo aziendale, si procede alla valutazione dell'applicabilità del Principio Privacy by design & by default → caratteristiche del processo: ➢ Change significativo: • Nuovo sviluppo/iniziativa/progetto? • Ampliamento dell' ambito di un processo in essere? ➢ Dati personali: • Presenza di dati personali? • Introduzione di una nuova tipologia di trattamento? ↓ - Controlli by design & by default - Controlli di sicurezza

Procedura «Gestione e Notifica Data Breach»

Articolo di riferimento	• Artt. 33 e 34 Regolamento 679/2016
Figure coinvolte	• Titolare del trattamento • Responsabile della Protezione dei DatI
Obiettivo	• Tale strumento supporta il Titolare nella gestione di Data Breach, indicando i ruoli, le responsabilità, le tempistiche e le modalità di comunicazione di eventuali violazioni di riservatezza dei dati personali all'Autorità di Controllo, ed, ove necessario, a tutti gli interessati oggetto della violazione
Sintesi dei contenuti	• Rilevazione della violazione → segnalazione RPD • Gestione del Data Breach • Notifica della violazione all'Autorità Garante • Comunicazione della violazione all'Interessato a cui i dati personali violati fanno riferimento • Attività successive: - definire le azioni per la mitigazione del rischio, con l'obiettivo di ridurre gli impatti sui diritti e le libertà degli Interessati - valutare gli impatti, per i diritti degli Interessati, causati dall'incidente che ha provocato la violazione dei dati personali • Archiviazione della documentazione relativa alla notifica

Linee Guida «Valutazione di impatto sulla protezione dei dati»

Articolo di riferimento	• Art. 35 GDPR
Figure coinvolte	• Titolare del trattamento • Responsabile della Protezione dei dati • Responsabile del Trattamento
Obiettivo	• A seguito di Risk Assessment, se il trattamento presenta un rischio elevato per i diritti e le libertà degli Interessati, prima di procedere al trattamento, si esegue obbligatoriamente la valutazione dell'impatto sulla protezione dei dati. E' richiesta: - nella valutazione sistematica e globale di aspetti personali dell'Interessato basata su un trattamento automatizzato e sulla quale si fondano decisioni aventi effetti giuridici od incidono significativamente - nel trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e a reati - nella sorveglianza sistematica di una zona accessibile al pubblico
Sintesi dei contenuti	• Definizione del livello di criticità dei trattamenti • Identificazione dei trattamenti critici • Identificazione della tipologia di trattamento • Valutazione controlli • Definizione del livello di Rischio Residuo • Identificazione trattamenti rischiosi

Registro dei trattamenti

Articolo di riferimento	• Art. 30 Regolamento 679/2016
Figure coinvolte	• Titolare del trattamento • Responsabile del Trattamento • Responsabile della Protezione dei dati → redigono e supportano nella redazione del registro delle attività e dei trattamenti effettuati
Obiettivo	• Strumento fondamentale, sia in formato cartaceo che in formato elettronico, per l'eventuale supervisione da parte del Garante e per la disposizione di un quadro aggiornato dei trattamenti in essere all'interno dell'azienda e per ogni valutazione ed analisi del rischio (adempimento obbligatorio per le imprese o organizzazioni con più di 250 dipendenti)
Sintesi dei contenuti	• il nome e i dati di contatto del titolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati • le finalità del trattamento • una descrizione delle categorie di interessati e delle categorie di dati personali • le categorie di destinatari a cui i dati personali sono stati o saranno comunicati • i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale • i termini ultimi previsti per la cancellazione delle diverse categorie di dati • una descrizione delle misure di sicurezza tecniche e organizzative

Riservatezza

Le industry nelle quali operano i nostri Clienti sono estremamente competitive. La riservatezza di piani, dati ed informazioni delle Società nostre Clienti è critica; Marsh Risk Consulting si impegna a proteggere tali piani, dati ed informazioni. In maniera analoga, il Risk Management Consulting è una industry competitiva. Ciò posto, resta inteso che tutti i diritti di proprietà Intellettuale (incluso, in particolare, il diritto d'autore) relativi ai contenuti delle nostre proposte, presentazioni, metodologie e tecniche di analisi, nonché più in generale al materiale distribuito (il "Materiale") rimangono di esclusiva proprietà di Marsh Risk Consulting.

Marsh Risk Consulting Vi concede licenza non esclusiva perpetua irrevocabile di utilizzare il Materiale per esclusivo uso interno. E' fatto pertanto espresso divieto di rivendere o modificare il Materiale, o quanto in esso contenuto, in tutto o in parte.

Voi non dovrete rendere disponibile il Materiale a terzi, per nessun motivo, e non divulgarne i contenuti senza aver ricevuto da Marsh Risk Consulting apposita comunicazione scritta, a meno che il rilascio di tali informazioni venga effettuato a seguito di una richiesta da parte di enti di controllo o di vigilanza o per altro obbligo di legge.

Resta inteso che In nessun modo ed in nessuna circostanza, Marsh Risk Consulting potrà mai essere considerata responsabile nei confronti di terzi che utilizzino, a qualsiasi titolo, il Materiale o quanto in esso contenuto.

MARSH RISK CONSULTING

Marsh Risk Consulting Services S.r.l. - Sede Legale: Viale Bodio, 33 - 20158 Milano - Tel. 02 48538 1 - www.marsh.it

Cap. Soc. Euro 10.400,00 i.v. - Reg. Imp. MI - N. Iscriz. e C.F.: 10027410157 - Partita IVA: 10027410157 - R.E.A. MI - N. 1338125

Società con socio unico soggetta al potere di direzione e coordinamento di Marsh S.p.A., ai sensi art. 2497 c.c.