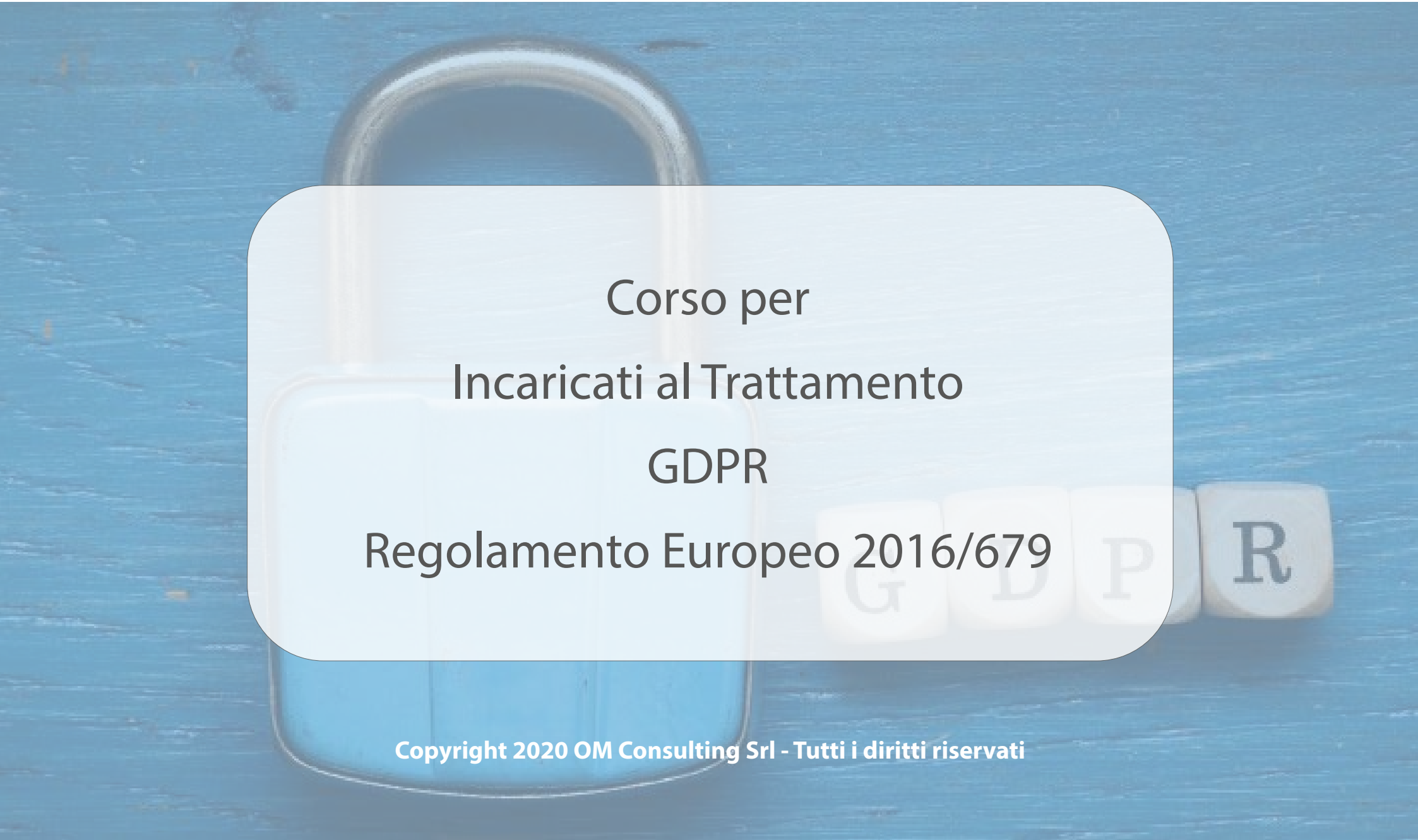
OMCONSULTING
ildigitaleresosemplice

OMACADEMY

TITALIA
Ildigitaleresosemplice



Corso per

Incaricati al Trattamento

GDPR

Regolamento Europeo 2016/679

Sommario

Lezione 1.1 1
Che cos'è il GDPR 1
A cosa serve il GDPR 2

Lezione 1.2 3
Cosa sono i dati personali 3
Cosa si intende per trattamento 4
A cosa servono i dati 5

Lezione 1.3 6
Applicazione del regolamento 6

Lezione 2.1 7
Liceita', correttezza e trasparenza 7

Lezione 2.2 8
Le basi giuridiche 8

Lezione 2.3 10
Categorie particolari di dati personali 10

Lezione 3.1 14
Chi sono gli interessati 14

Lezione 3.2 15
I diritti degli interessati 15

Lezione 3.3 17
Le informative 17

Lezione 4.1 20
Titolare, responsabile, DPO 20

Lezione 4.2 24
Gli obblighi del titolare e del responsabile 24

Lezione 4.3 29
Notifica di data breach 29

Lezione 4.4 30
Valutazione d'impatto e consultazione preventiva 30

Lezione 5.1 31
Trasferimenti di dati 31

Lezione 6.1 32
Chi sono gli incaricati 32
Le istruzioni per gli incaricati 33

Lezione 7.1 36
L'autorita' di controllo italiana 36

Lezione 7.2 38
I ricorsi 38
Le sanzioni amministrative pecuniarie 39

Lezione 1.1
Che cos'è il GDPR

Il **GDPR**, General Data Protection Regulation UE 2016/679, è il Regolamento emanato dalla Commissione Europea nel 2016 atto a **garantire la protezione e la libera circolazione dei dati personali all'interno dell'Unione.**

OBIETTIVO: infondere fiducia nei processi che riguardano i cittadini europei.
Prima del GDPR il principale strumento giuridico dell'Unione europea in materia di protezione dei dati era la Direttiva 95/46/CE, recepita in Italia con il Codice della Privacy (D.Lgs 196/2003), che oggi è stato modificato con il D.Lgs 101/2018.
Attualmente la normativa di riferimento è il GDPR.

Il GDPR è in vigore dal 24 maggio 2016
Il GDPR (e le sanzioni) è applicabile dal 25 maggio 2018

A cosa serve il GDPR

Il Regolamento serve ad **UNIFORMARE la normativa** relativa al trattamento e alla protezione dei dati in tutto il territorio dell'Unione Europea.

In sintesi, serve a **disciplinare il buon uso dei dati personali** affidati alle organizzazioni (aziende), in modo che vengano gestiti correttamente in tutti gli Stati membri dell'UE.

Il GDPR è **direttamente applicabile e vincolante** per tutti gli Stati membri e non richiede una legge di recepimento nazionale.

Al centro del Regolamento non troviamo più l'INTERESSATO (cla persona fisica a cui appartengono i dati), come nella vecchia Direttiva, ma il **TITOLARE DEL TRATTAMENTO** (cioè il rappresentante legale dell'azienda che tratta quei dati).

Lezione 1.2

Cosa sono i dati personali

Sono dati personali, ad esempio:

- Indirizzo email personale (che è anche nome.cognome@azienda.it)
- Targa di un'auto
- Immagine di una persona
- Numero di cellulare
- indirizzo IP di un computer
- Nickname su internet
- Dati biometrici (iride, impronta digitale)
- File audio
- Marcatori temporanei come i TAG

Cosa intende il Regolamento per **DATO PERSONALE**? (Art. 4):

Per **DATO PERSONALE** si intende «qualsiasi informazione riguardante una **persona fisica identificata o identificabile** («interessato»); 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.»

Cosa si intende per trattamento

Un trattamento è qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come:

- la raccolta
- la registrazione
- l'organizzazione
- la conservazione
- l'adattamento o la modifica
- l'estrazione
- la consultazione
- l'uso
- la comunicazione, diffusione o qualsiasi forma di messa a disposizione
- il raffronto
- la limitazione
- la cancellazione o la distruzione.

A cosa servono i dati

I **dati** sono destinati a diventare sempre più la **materia prima** alla base dei **servizi e dei prodotti innovativi**. I **dati** sono un **potenziale motore per lo sviluppo e la fonte di nuovi business ad altissimo valore aggiunto** e servono per:

- Creare prodotti innovativi
- Formulare offerte mirate ai consumatori
- Garantire sicurezza e migliorare efficienza aziendale
- Controllare, profilare e analizzare

Lezione 1.3
Applicazione del regolamento

Il Regolamento si applica ad ogni **trattamento di dati personali contenuti in un archivio**.

Il Regolamento si applica integralmente a **tutte le organizzazioni**, pubbliche e private, situate nel territorio dell'Unione.

Il Regolamento si applica alle imprese situate fuori dall'Unione Europea che **offrono servizi o prodotti a persone che si trovano nel territorio dell'Unione stessa.**

Il Regolamento **NON si applica (Art. 2) ai trattamenti:**

- effettuati da una persona fisica per l'esercizio di attività a **carattere esclusivamente personale o domestico**;
- **effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali**.

Lezione 2.1
Liceita', correttezza e trasparenza

Qualsiasi trattamento di dati personali dovrebbe essere **lecito e corretto**.
Dovrebbero essere **trasparenti le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che li riguardano** nonché la misura in cui i dati personali sono o saranno trattati.
Il principio della **trasparenza** impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano **facilmente accessibili e comprensibili** e che sia utilizzato un **linguaggio semplice e chiaro**.
La trasparenza si applica PRIMA (= alla raccolta), DURANTE (=nel trattamento) e DOPO (eventuale violazione dei dati) il trattamento.

Tale principio riguarda, in particolare, l'informazione degli interessati sull'identità del titolare del trattamento (chi tratta i miei dati) e sulle finalità del trattamento (per quale ragione li tratta).
I dati personali dovrebbero essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento.

Lezione 2.2
Le basi giuridiche

Il trattamento è lecito solo se è basato su una delle seguenti motivazioni (basi giuridiche):

a. l'interessato ha espresso il consenso al trattamento dei propri dati personali (newsletter);
b. 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 (assunzione lavorativa, acquisto di un servizio online);
c. il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento (visita medica obbligatoria, causa legale);
d. il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica (pronto soccorso, interventi medici);

e. 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;
f. 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 un minore.

Le basi giuridiche del consenso e del perseguimento del legittimo interesse del titolare sono quelle considerate più **deboli**: nel caso sia possibile, meglio utilizzarne un'altra.

Lezione 2.3

Categorie particolari di dati personali

Art. 9 – «È vietato trattare dati personali che rivelino **l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale**, nonché trattare **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.»

Quanto sopra **NON si applica** se sussiste una delle seguenti condizioni:

a. l'interessato ha prestato il proprio **consenso esplicito** al trattamento di tali dati personali;
b. il trattamento è necessario per **assolvere gli obblighi** ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in **materia di diritto del lavoro e della sicurezza sociale e protezione sociale**, …in presenza di **garanzie appropriate** per i diritti fondamentali e gli interessi dell'interessato;
c. il trattamento è necessario per **tutelare un interesse vitale** dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
d. il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una, **fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali** …

Quali sono i cosiddetti DATI PARTICOLARI?

Nella vecchia normativa erano chiamati DATI SENSIBILI, e sono sempre dati personali che rivelino:

- l'**origine razziale** o **etnica**
- le **opinioni politiche**
- le **convinzioni religiose** o **filosofiche**
- l'**appartenenza sindacale**
- **dati genetici**
- **dati biometrici** intesi a identificare in modo univoco una persona fisica
- dati relativi alla **salute**
- dati relativi alla **vita sessuale** o all'**orientamento sessuale della persona.**

È VIETATO trattare i dati sopra indicati **A MENO CHE:**

a. l'interessato abbia prestato il proprio **consenso esplicito** al trattamento di tali dati;
b. il trattamento sia necessario per **assolvere gli obblighi ed esercitare i diritti** specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;
c. il trattamento sia necessario per **tutelare un interesse vitale** dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
d. il trattamento sia effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una **fondazione, associazione o altro organismo senza scopo di lucro** che persegua finalità politiche, filosofiche, religiose o sindacali;
e. il trattamento riguardi dati personali **resi manifestamente pubblici dall'interessato**;
f. il trattamento sia necessario per **accertare, esercitare o difendere un diritto** in sede giudiziaria;
g. il trattamento sia necessario per motivi di **interesse pubblico rilevante**;
h. il trattamento sia necessario per finalità di **medicina preventiva o di medicina del lavoro;**

i. il trattamento sia necessario per motivi di **interesse pubblico nel settore della sanità pubblica;**

j. il trattamento sia necessario a fini di **archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici**.

Lezione 3.1
Chi sono gli interessati

Il GDPR si rivolge a tutte le **persone fisiche**, chiamate **INTERESSATI**, a cui si riferiscono i dati personali. L'interessato **può essere solo una persona fisica**, e **non una persona giuridica, un ente o un'associazione**.

Ogni persona fisica gode di una **SERIE DI DIRITTI INALIENABILI**, che sono i seguenti:

- ACCESSO (Art. 15)
- RETTIFICA (Art. 16)
- OBLIO (Art. 17)
- LIMITAZIONE DEL TRATTAMENTO (Artt. 18-19)
- PORTABILITÀ (Art. 20)
- OPPOSIZIONE (Art. 21)
- PROCESSO DECISIONALE AUTOMATIZZATO (Art. 22)
- RECLAMO (Artt. 78)
- CONSERVAZIONE (Art. 15)

Lezione 3.2
I diritti degli interessati

ACCESSO: Ogni interessato ha diritto di avere conferma che sia in corso il trattamento dei suoi dati ed avere accesso agli stessi, dopo essersi fatto identificare **(ottenerne copia)**.

RETTIFICA: Ogni interessato ha diritto di ottenere la **correzione o integrazione** dei suoi dati personali inesatti.

OBLIO : Ogni interessato ha diritto di decidere che **siano cancellati tutti i suoi dati personali** non più necessari alle finalità.

LIMITAZIONE DEL TRATTAMENTO : Ogni interessato ha diritto di richiedere la **sola conservazione** dei propri dati (illiceità del trattamento, mancata correttezza dei dati, particolare necessità dell'interessato) e non più l'utilizzo.

PORTABILITÀ: Ogni interessato ha diritto di **ricevere** i propri dati personali in un **formato strutturato, di uso comune e leggibile** da dispositivo automatico e **richiederne trasmissione ad altro titolare** senza impedimenti (ad esempio, spostare il proprio profilo da Fitbit a Runstarter).

OPPOSIZIONE: Ogni interessato ha diritto di **opporsi** in qualsiasi momento al **trattamento automatizzato** che abbia impatti significativi sulla sua libertà o diritti, compresa la profilazione (chiedere l'intervento umano).

PROCESSO DECISIONALE AUTOMATIZZATO: Ogni interessato ha diritto di **non essere sottoposto** a una decisione basata **unicamente** sul trattamento automatizzato, compresa la profilazione, che **produca effetti giuridici** che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

RECLAMO: Ogni interessato ha diritto di reclamare all'Autorità di Controllo **per ogni presunta violazione** del GDPR.

CONSERVAZIONE: Ogni interessato ha diritto di avere **indicazione delle tempistiche** con le quali il Titolare conserverà i suoi dati.

Lezione 3.3
Le informative

Come può un interessato essere informato su come verranno gestiti i propri dati?
Diventa fondamentale il ruolo dell'**INFORMATIVA**, che è **obbligatoria**.

Chi la redige?
Il Titolare del Trattamento, che deve scriverla «in **forma concisa, trasparente, intelligibile**, con un **linguaggio semplice e chiaro**».

Come e dove deve essere messa a disposizione?
«Le informazioni sono **fornite per iscritto** o con altri mezzi, anche, se del caso, con mezzi elettronici»; in ogni caso, l'informativa deve essere **facilmente accessibile**.

Le informative possono essere relative a dati raccolti presso l'interessato (Art. 13) oppure da un'altra fonte (Art. 14).

In entrambi i casi, il titolare del trattamento fornisce obbligatoriamente all'interessato, nel momento in cui i dati personali sono ottenuti una serie di informazioni:

a. **l'identità e i dati di contatto del titolare del trattamento** e del suo rappresentante;
b. i dati di contatto del DPO, ove applicabile;
c. le **finalità del trattamento** nonché la base giuridica del trattamento;
d. gli eventuali **destinatari** o le eventuali categorie di destinatari dei dati personali;
e. l'intenzione del titolare di **trasferire dati a un paese terzo** o a un'organizzazione internazionale;
f. il **periodo di conservazione** o, se non è possibile, i criteri utilizzati per determinare tale periodo;
g. l'esistenza del diritto dell'interessato di **esercitare i propri diritti** di accesso, rettifica, cancellazione o limitazione e portabilità dei dati e di revoca del consenso (se applicabili Artt. 6 o 9);
h. il diritto di **proporre reclamo** a un'autorità di controllo;
i. le **possibili conseguenze** della mancata comunicazione di tali dati;
j. l'**esistenza di un processo decisionale automatizzato**, compresa la profilazione.

Qualora i dati **NON siano stati ottenuti presso l'interessato (Art. 14)**, il titolare del trattamento fornisce **ANCHE la fonte da cui hanno origine i dati personali**.

Il titolare del trattamento fornisce le informazioni di cui sopra:

a. entro un termine ragionevole dall'ottenimento dei dati personali, **al più tardi entro un mese**, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;

b. nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, **al più tardi al momento della prima comunicazione all'interessato.**

Lezione 4.1
Titolare, responsabile, DPO

IL TITOLARE DEL TRATTAMENTO (Art. 4)

La persona fisica, giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o congiuntamente, **determina le finalità e i mezzi del trattamento**.

Il Titolare del trattamento **mette in atto, riesamina e aggiorna le misure** tecniche e organizzative **adeguate** per **garantire ed essere in grado di dimostrare** che il trattamento è effettuato conformemente al GDPR.

Al Titolare si applica il **PRINCIPIO** di **RESPONSABILIZZAZIONE o ACCOUNTABILITY**.

A lui spetta dimostrare di aver messo in atto tutte le opportune misure di tutela.

IL RESPONSABILE DEL TRATTAMENTO (Art. 28)

Chiunque **tratti** dati personali **per conto del Titolare; non può trattare dati personali** se **non** è **istruito** dal titolare del trattamento.

In particolare, il responsabile deve:

- presentare **garanzie sufficienti** di attuare **misure adeguate di protezione**
- trattare i dati sulla base di un **chiaro rapporto contrattuale** (natura, finalità, durata del trattamento, tipi di dati, categorie di interessati, obblighi e diritti)
- garantire l'impegno o il vincolo alla **riservatezza** degli incaricati
- **mettere a disposizione tutte le informazioni** per comprovare la conformità
- impegnarsi a **cancellare i dati** al termine della prestazione di servizi

Se un **responsabile viola il regolamento**, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento e ne risponde legalmente.

IL DATA PROTECTION OFFICER (artt. 37-39)

Nominato **obbligatoriamente da alcuni** (e **facoltativamente** da tutti i titolari), il DPO si occupa di:

- **considerare i rischi** inerenti al trattamento
- **informare e fornire consulenza** al Titolare
- **sorvegliare** l'osservanza del Regolamento
- **fornire** un **parere** in merito alla **valutazione d'impatto** e sorvegliarne lo svolgimento
- cooperare e **fungere da punto di contatto** con l'autorità di controllo

Ricorre **obbligo di nomina di DPO**:

a. se il trattamento è svolto da **un'autorità pubblica** o da un **organismo pubblico**;
b. se le attività principali consistono in trattamenti che richiedono il **monitoraggio regolare e sistematico di interessati su larga scala**;
c. se le attività principali consistono nel trattamento su **larga scala** di **categorie particolari di dati o di dati personali relativi a condanne penali e reati**.

Lezione 4.2

Gli obblighi del titolare e del responsabile

Gli obblighi previsti per i Titolari e per i Responsabili si possono riassumere in **9 requisiti da attuare e saper comprovare**, così schematizzabili:

- Privacy by design e by default
- Registro Attività di Trattamento
- Adozione di misure adeguate
- Notifica di Data Breach
- Procedura di Audit
- Istruzioni di trattamento

→ **REQUISITI VALIDI PER TUTTE LE AZIENDE**

- Nomina del DPO
- Valutazione di Impatto
- Consultazione Preventiva

→ **REQUISITI VALIDI PER ALCUNE AZIENDE**

PRIVACY BY DESIGN E PRIVACY BY DEFAULT

PRIVACY BY DESIGN = FIN DALLA PROGETTAZIONE, SU MISURA
Il Titolare, PRIMA di iniziare un qualsiasi trattamento di dati personali, mette in atto misure tecniche e organizzative adeguate ed integrare nel trattamento le necessarie garanzie al fine di tutelare i diritti degli interessati

PRIVACY BY DEFAULT = PER IMPOSTAZIONE PREDEFINITA
Il Titolare del trattamento mette in atto **misure tecniche e organizzative adeguate** per garantire che siano trattati, **per impostazione predefinita**, solo i dati personali **necessari** per **ogni specifica finalità** del trattamento.
Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità.

MISURE ADEGUATE

Secondo l'Art. 24, **il Titolare deve mettere «in atto misure tecniche e organizzative adeguate** per **garantire**, ed **essere in grado di dimostrare**, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono **riesaminate e aggiornate** qualora necessario.»

Nella sua valutazione, il Titolare deve tenere conto:

- della **natura del trattamento**
- dell'**ambito di applicazione**
- del **contesto**
- delle **finalità** del trattamento, ma soprattutto dei **RISCHI** aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

IL LIVELLO DI SICUREZZA DEVE ESSERE ADEGUATO AL RISCHIO

IL REGISTRO DEI TRATTAMENTI

Il **Registro dei Trattamenti** contiene le seguenti informazioni obbligatorie:

a. **il nome e i dati di contatto** del titolare del trattamento e, ove applicabile, del rappresentante e del DPO;
b. le **finalità** del trattamento;
c. una descrizione delle **categorie di interessati** e delle **categorie di dati personali;**
d. le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
e. ove applicabile, i **trasferimenti** di dati personali verso un paese terzo o un'organizzazione internazionale;
f. ove possibile, i **termini ultimi previsti per la cancellazione**;
g. ove possibile, una **descrizione generale delle misure di sicurezza tecniche e organizzative**.

L'Autorità Garante della Privacy s**uggerisce l'adozione del Registro dei Trattamenti a tutte le organizzazioni ed obbligatoriamente** a, ad esempio non esaustivo:

- esercizi commerciali, esercizi pubblici o artigiani con almeno un dipendente (bar, ristoranti, officine, negozi, piccola distribuzione, ecc.) e/o che trattino dati sanitari dei clienti (es. parrucchieri, estetisti, ottici, odontotecnici, tatuatori ecc.);
- liberi professionisti con almeno un dipendente e/o che trattino dati sanitari e/o dati relativi a condanne penali o reati (es. commercialisti, notai, avvocati, osteopati, fisioterapisti, farmacisti, medici in generale);
- associazioni, fondazioni e comitati ove trattino "categorie particolari di dati" e/o dati relativi a condanne penali o reati (i.e. associazioni a tutela di soggetti malati, persone con disabilità, ex detenuti ecc.; associazioni che perseguono finalità di prevenzione e contrasto delle discriminazioni di genere, razziali, basate sull'orientamento sessuale, politico o religioso ecc.; associazioni sportive con riferimento ai dati sanitari trattati; partiti e movimenti politici; sindacati; associazioni e movimenti a carattere religioso);
- il condominio ove tratti "categorie particolari di dati" (es. delibere per interventi volti al superamento e all'abbattimento delle barriere architettoniche; richieste di risarcimento danni comprensive di spese mediche relativi a sinistri avvenuti all'interno dei locali condominiali)

Lezione 4.3

Notifica di data breach

Un "data breach" è una violazione di sicurezza, accidentale o illecita, che causa **la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati** personali trasmessi, conservati o trattati.

Ogni **violazione dei dati personali** dell'interessato (Data Breach) **DEVE** essere registrata.
Se la violazione può **presentare un rischio elevato** per i diritti e le libertà delle persone fisiche, il titolare **comunica la violazione** all'interessato **senza ingiustificato ritardo e al Garante per la Privacy.**

La comunicazione va effettuata **entro 72 ore** dal momento in cui **se ne viene a conoscenza**.

Lezione 4.4

Valutazione d'impatto e consultazione preventiva

Quando un tipo di trattamento, allorché preveda **in particolare l'uso di nuove tecnologie**, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un **rischio elevato per i diritti e le libertà delle persone fisiche**, il titolare del trattamento deve sempre effettuare, prima di procedere al trattamento, una **valutazione dell'impatto dei trattamenti** previsti.

In alcuni casi specifici, che presentino un rischio elevato, è prevista dal Regolamento la **consultazione preventiva** del Garante per la Privacy

Lezione 5.1
Trasferimenti di dati

Nel caso in cui i dati personali oggetto di un trattamento debbano essere **trasferiti verso un paese terzo o un'organizzazione internazionale**, il Titolare del trattamento e il Responsabile devono rispettare clausole specifiche al fine di assicurare la protezione dei dati trattati, ad esempio:

- Trasferimento sulla base di una decisione di adeguatezza dell'UE;
- Trasferimento soggetto a garanzie adeguate (Autorizzazioni specifiche di un'Autorità di controllo, codici di condotta, certificazioni, etc);
- Norme vincolanti d'impresa, «Binding Corporate Rules».

Lezione 6.1
Chi sono gli incaricati

Il GDPR non prevede espressamente la figura dell'incaricato, ma non ne esclude la nomina, facendo riferimento a **persone autorizzate al trattamento dei dati sotto l'autorità diretta** del Titolare o del Responsabile (art. 4, n. 10 GDPR).

Incaricato, o autorizzato, è il soggetto persona fisica che effettua materialmente le operazioni di trattamento sui dati personali.
L'autorizzato può essere sia un dipendente del Titolare che dell'eventuale Responsabile, se viene nominato.
Gli autorizzati possono essere organizzati con diversi livelli di delega.

E' fondamentale fornire agli autorizzati le **istruzioni operative** (art. 29 GDPR), compresi gli obblighi inerenti le misure di sicurezza, e che sia fornita loro la **necessaria formazione**.

Lezione 6.2
Le istruzioni per gli incaricati

Le istruzioni per gli incaricati:

- Operare sulla base delle **Istruzioni** indicate nel Documento Programmatico Privacy al punto 7.5 (riportate nella slide 41);
- **Sorvegliare** che il trattamento sia effettuato nei termini e nei modi stabiliti dal Regolamento 2016/679 in materia di dati personali, con particolare attenzione alle misure di sicurezza (art. 32);
- Impegnarsi alla **riservatezza** e alla **non divulgazione** dei dati oggetto del trattamento;
- Partecipare alla **formazione annuale** relativamente al Sistema Privacy adottato in Azienda.

L'autorizzato deve **attenersi strettamente** alle istruzioni ricevute.
La normativa non prevede requisiti quantitativi per essere considerati autorizzati, per cui anche la semplice **presa visione di un dato personale** (es. il magazziniere che consulta la bolla di consegna) **si qualifica come trattamento**.

Le **istruzioni per gli incaricati**, in sintesi:

- **Diritto di accesso:** una volta identificata la persona fisica, l'organizzazione provvede senza ingiustificato ritardo a fornire le informazioni.
- **Diritto di rettifica:** una volta identificata la persona fisica, si procederà con l'integrazione dei dati personali incompleti o inesatti, il riscontro al richiedente senza ingiustificato ritardo, entro massimo un mese.
- **Diritto all'oblio (cancellazione):** una volta identificata la persona fisica, si procederà con la valutazione della fattibilità tecnica della richiesta, la fattibilità legislativa della richiesta (ad esempio, a fronte dell'obbligo di mantenere le registrazioni contabili per 10 anni), la valutazione dell'interesse legittimo della società (ad esempio, a fronte di possibili contenziosi) e si darà riscontro al richiedente.
- **Diritto di limitazione:** Qualora l'interessato ritenga di aver diritto alla limitazione dei propri dati si procederà a trattare tali dati esclusivamente per accertamento, esercizio o difesa di diritto in sede giudiziaria.

- **Diritto alla portabilità dei dati:** Per i trattamenti automatizzati, l'interessato ha il diritto di ricevere i propri dati in un formato strutturato, di uso comune e leggibile da un dispositivo automatico. In tale caso la persona responsabile, dopo aver verificato l'identità della persona fisica, provvederà all'invio di tali dati senza ingiustificato ritardo, entro un massimo di un mese.
- **Diritto di opposizione:** L'interessato ha diritto di opporsi in qualsiasi momento al trattamento dei dati che lo riguardano se tali dati sono basati sul consenso o su un contratto oppure se raccolti per finalità di marketing diretto, compresa la profilazione. L'organizzazione verificherà la mancanza di impedimenti (ad esempio l'esistenza di motivi legittimi prevalenti dimostrati) ed in seguito comunica all'interessato l'aggiornamento dei propri dati personali sulla base della richiesta ricevuta.

Tutte le attività devono essere svolte **senza ingiustificato ritardo, entro massimo un mese.**

Lezione 7.1
L'autorita' di controllo italiana

Ogni Stato membro dell'Unione europea ha la sua Autorità di controllo.
L'autorità di controllo è **competente per la gestione dei reclami** ad essa proposti o per eventuali violazioni del regolamento europeo e delle norme nazionali in materia di protezione dei dati.

Il Garante per la protezione dei dati personali (Garante Privacy) è l'autorità di controllo nazionale italiana, un'autorità amministrativa indipendente istituita dalla legge sulla privacy (legge 31 dicembre 1996, n. 675), in attuazione della direttiva comunitaria 95/46/CE.

Il Garante si occupa di:

- **verificare la conformità alla legge dei trattamenti** e prescrivere ai titolari le misure da adottare;
- **esaminare i reclami**;
- **limitare, sospendere o vietare i trattamenti** in violazione delle norme;
- adottare le **autorizzazioni** generali;
- **promuovere codici di deontologia** e buona condotta (es. in materia di giornalismo);
- partecipare alle attività comunitarie e internazionali (anche quale componente dell'EDPB);
- **irrogare sanzioni correttive.**

L'Autorità di controllo interviene principalmente **successivamente alle valutazioni del Titolare del trattamento**, che ha quindi una responsabilità maggiore.

L'attività ispettiva viene svolta in collaborazione con il **Nucleo speciale privacy della Guardia di Finanza** sulla base di un piano di controlli semestrale.

L'Autorità di controllo decide anche le eventuali sanzioni pecuniarie:
«**Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie** inflitte in relazione alle violazioni del GDPR **siano in ogni singolo caso effettive, proporzionate e dissuasive.**»

Lezione 7.2
I ricorsi

"**Chiunque subisca o ritenga di aver subito un danno materiale o immateriale** causato da una violazione del presente Regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento"

Il **Titolare risponde del danno causato**.

Il **Responsabile** ne risponde **solo se** non ha adempiuto agli obblighi del GDPR o **ha violato** le istruzioni del trattamento fornite dal titolare.
Qualora più titolari o responsabili siano coinvolti, essi sono **responsabili in solido**.

Le sanzioni amministrative pecuniarie

Le sanzioni si dividono in due grandi ambiti con differenti limiti alle sanzioni comminabili. Per alcune inadempienze in ambito Privacy sono previste anche sanzioni penali e non solo pecuniarie, come disciplinato dal D. Lgs 101/2018.

- **OBBLIGHI DEL TITOLARE**
- **OBBLIGHI DEL RESPONSABILE**
- **FIGURE DELLA PROTEZIONE DEI DATI**
- **TRATTAMENTI RELATIVI AI MINORI**
- **PRINCIPI BASE DEL REG (CONSENSO)**
- **DIRITTI DEGLI INTERESSATI**
- **TRASFERIMENTO DATI**
- **INOSSERVANZA PROVVEDIMENTI DI AUTORITA' GARANTE**

FINO A **10 milioni di EURO** O,
PER LE IMPRESE, FINO **AL 2%** DEL FATTURATO MONDIALE DELL'ESERCIZIO PRECEDENTE, SE SUPERIORE ai 10 milioni di Euro.

FINO **A 20 milioni di EURO** O,
PER LE IMPRESE, FINO AL **4%** DEL FATTURATO MONDIALE DELL'ESERCIZIO PRECEDENTE, , SE SUPERIORE ai 20 milioni di Euro.