il Regolamento 2016/679/EU

General Data Protection Regulation (GDPR)

Cremona, 15 maggio 2018

a cura di: Avv. Marco Longoni

- Principi generali della normativa nazionale in vigore (D. Lgs. 196/2003, c.d. Codice della Privacy)
- Oggetto ed ambito di applicazione

I dati personali

Secondo l'art. 4 comma 1 lett. B) del D. lgs 196/2003, il dato personale è:
«**qualunque informazione** relativa a **persona fisica, persona giuridica, ente od associazione**, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale».

Dato personale può essere anche un'**immagine,** una **informazione** o una **notizia** riferibile a un soggetto determinato o determinabile.

Alcuni esempi

I codici identificativi, ovvero
•Codice fiscale;
•Codici clienti;
ovvero altri codici univoci, attribuiti a una persona in base a criteri predefiniti, sono dati personali.

Dato personale, dunque, è una **qualsiasi informazione riferita a una persona** (**ovvero, che può essere a questa collegata** tramite un codice)

Non sono «dati personali», ad esempio, i dati delle persone giuridiche, degli enti o delle associazioni.

I dati «sensibili»

L’art. 4 comma 1 lett. D) D. lgs 196/2003 definisce **dati sensibili** quei «*dati personali* ***idonei a rivelare l'origine razziale ed etnica****, le* ***convinzioni religiose, filosofiche*** *o di altro genere, le* ***opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni*** *a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale»*

Questa particolare categoria di dati è sottoposta dal Codice Privacy a un **livello di protezione più elevato** di quello previsto per i dati comuni.

Principi generali - 1

Diritto alla protezione dei dati personali

Si tratta della regola fondamentale sancita dall'articolo 1 del D. Lgs. 196/03) che attribuisce ad **ogni individuo il diritto di pretendere che l'uso dei suoi dati personali si svolga nel rispetto dei suoi diritti e libertà fondamentali**, nonché della sua dignità, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Principi generali - 2

Principio di necessità nel trattamento dei dati

Tale principio mira a **limitare le raccolte ed i trattamenti di dati non necessari**: possono essere raccolti solo i dati necessari per il trattamento che si intende realizzare.

L'art. 3 del D. Lgs. 196/03 impone, infatti, di configurare i sistemi informativi e i programmi informatici riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi o attraverso opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Principi generali - 3

Principio di finalità e di autodeterminazione informativa

Il **principio di finalità** richiede il collegamento dell'attività di raccolta dei dati personali con l'uso che di quelle informazioni viene fatto e consiste nell'obbligo posto a carico di chi effettua la raccolta di far conoscere all'interessato – all'atto della raccolta – la ragione per la quale i dati sono raccolti (che ovviamente deve essere legittima, determinata e non incompatibile con l'impiego dei dati).

Il **principio di autodeterminazione** invece riconosce il diritto del soggetto a determinare il perimetro e l'ambito di comunicazione dei dati che lo riguardano.

Principi generali - 4

Principio di liceità e correttezza

Tale principio riguarda la condotta del titolare, del responsabile e dell'incaricato al trattamento che devono comportarsi garantendo **la liceità e la correttezza del trattamento** stesso sia durante la raccolta che durante l'elaborazione dei dati.

Per trattamento **lecito** si intende conforme alla legge, per trattamento **corretto** si intende un trattamento non attuato mediante una raccolta con informazioni ingannevoli o, peggio, mediante il ricorso ad artifizi e raggiri.

Principi generali - 5

Principio di precauzione (o prevenzione)

Tale principio impone la **prevenzione** di ogni forma di illecito utilizzo di trattamento di dati personali (anche per mera superficialità o negligenza) attraverso ogni cautela idonea ad evitare l'accesso o l'utilizzo di dati di cui non sia possibile ricostruirne le modalità di formazione.

DIVIETO DI UTILIZZO DEI DATI

L'art. 11 comma 2 del D. lgs 196/2003 dispone

2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali ***non possono essere utilizzati****.*

Pertanto, se si vogliono prevenire contestazioni, che possono portare al blocco del trattamento dei dati, occorre rispettare tutti i principi normativi ed i provvedimenti del Garante correlati (Linee Guida, provvedimenti consultabili sul sito web istituzionale)

Le figure incaricate del trattamento dei dati

Soggetti del trattamento dei dati personali

La normativa attribuisce specifici poteri di controllo e responsabilità ai seguenti soggetti:

- il **titolare**
- il **responsabile**
- l'**incaricato**
- l'**interessato**
- il **Garante Privacy**
- l'**Autorità Giudiziaria ordinaria**

Soggetti del trattamento dei dati personali

Per **titolare**, il Codice (art. 4 comma 1 lett. F) intende *«la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza».* Quando il trattamento è effettuato da una persona giuridica o da un ente titolare è l'entità nel suo complesso e non la persona fisica che la rappresenta.

Il **responsabile** del trattamento, invece, è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo **preposto al trattamento di dati personali**.

Il responsabile procede al trattamento attenendosi alle istruzioni impartite per iscritto dal titolare al quale spetta la vigilanza sulla puntuale osservanza delle norme e delle istruzioni impartite.

Soggetti del trattamento dei dati personali

Gli **incaricati** del trattamento sono le «*persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile*». Si tratta quindi dei soggetti che possono elaborare i dati personali, ai quali accedono attenendosi alle istruzioni ricevute per iscritto ed in maniera dettagliata dal titolare o dal responsabile.

L'**interessato** è il soggetto (persona fisica, persona giuridica, ente o associazione) **cui si riferiscono i dati personali**. È quindi il vero protagonista del trattamento.

L'autorità preposta alla tutela della riservatezza dei dati personali è il **Garante** per la protezione dei dati personali. Dal punto di vista generale il Garante è un'autorità amministrativa indipendente.

Le **funzioni principali** del Garante sono controllare la legittimità dei trattamenti, esaminare i ricorsi e le segnalazioni ricevute dagli interessati.

I diritti dell'interessato e la figura del Garante

Gli obblighi previsti e le relative sanzioni

I diritti dell’interessato

ARTICOLO N.7 (**Diritto di accesso ai dati personali** ed altri diritti)

1. L'interessato ha diritto di **ottenere la conferma dell'esistenza** o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.

2. L'interessato ha diritto di ottenere l'indicazione:

a) dell'origine dei dati personali;

b) delle finalità e modalità del trattamento;

c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;

d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;

e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

I diritti dell’interessato - segue

3. L'interessato ha diritto di ottenere:

a) **l'aggiornamento, la rettificazione** ovvero, quando vi ha interesse, **l'integrazione** dei dati;

b) la **cancellazione**, la **trasformazione in forma anonima** o il **blocco** dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;

c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state **portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi**, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

I diritti dell’interessato - segue

4. L'interessato ha **diritto di opporsi**, in tutto o in parte:

a) per motivi legittimi al **trattamento dei dati personali che lo riguardano**, ancorché pertinenti allo scopo della raccolta;

b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Esercizio dei diritti

ARTICOLO N.8

(Esercizio dei diritti)

1. *I diritti di cui all'articolo 7 sono esercitati con* ***richiesta rivolta senza formalità al titolare o al responsabile, anche per il tramite di un incaricato****, alla quale è fornito* ***idoneo riscontro senza ritardo****.*

Tali diritti non possono essere esercitati con richiesta al titolare o al responsabile nei casi di divieto normativo espresso (in materia di sostegno alle vittime di richieste estorsive, per ragioni di giustizia, presso uffici giudiziari di ogni ordine e grado o il Consiglio superiore della magistratura o altri organi di autogoverno o il Ministero della giustizia etc)

Modalità di esercizio dei diritti

ARTICOLO N.9 (Modalità di esercizio)

1. La richiesta rivolta al titolare o al responsabile può essere trasmessa anche mediante lettera raccomandata, telefax o posta elettronica. Il Garante può individuare altro idoneo sistema in riferimento a nuove soluzioni tecnologiche. Quando riguarda l'esercizio dei diritti di cui all'articolo 7, commi 1 e 2, la richiesta può essere formulata anche oralmente e in tal caso è annotata sinteticamente a cura dell'incaricato o del responsabile.

2. Nell'esercizio dei diritti di cui all'articolo 7 l'interessato può conferire, per iscritto, delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da una persona di fiducia.

3. I diritti di cui all'articolo 7 riferiti a dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.

Modalità di esercizio dei diritti

ARTICOLO N.10

(**Riscontro all'interessato**)

1. Per garantire l'effettivo esercizio dei diritti di cui all'articolo 7 il titolare del trattamento è tenuto ad adottare idonee misure volte, in particolare:

a) ad agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili;

b) a semplificare le modalità e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico.

Modalità di esercizio dei diritti

ARTICOLO N.10

(Riscontro all'interessato)

2. I dati sono estratti **a cura del responsabile o degli incaricati** e possono essere **comunicati al richiedente anche oralmente, ovvero offerti in visione mediante strumenti elettronici**, sempre che in tali casi la comprensione dei dati sia agevole, considerata anche la qualità e la quantità delle informazioni. Se vi è richiesta, si provvede alla trasposizione dei dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica.

3. Salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprende tutti i dati personali che riguardano l'interessato comunque trattati dal titolare. Se la richiesta è rivolta ad un esercente una professione sanitaria o ad un organismo sanitario si osserva la disposizione di cui all'articolo 84, comma 1.

(segue: art. 84)

Obbligo di consenso previa informativa

REGOLE ULTERIORI PER PRIVATI ED ENTI PUBBLICI ECONOMICI

ARTICOLO N.23 (Consenso)

1. Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato.

2. Il consenso può riguardare l'intero trattamento ovvero una o più operazioni dello stesso.

3. Il consenso è **validamente prestato solo se è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le informazioni di cui all'articolo 13**.

4. **Il consenso è manifestato in forma scritta quando il trattamento riguarda dati sensibili.**

Misure minime art. 33 e 34 Codice Privacy

L’art. 34 prevede che

Il trattamento di dati personali effettuato con ***strumenti elettronici*** è consentito solo se sono adottate, **nei modi previsti dal disciplinare tecnico contenuto nell'allegato B)**, le seguenti misure minime

a) autenticazione informatica;

b) adozione di procedure di gestione delle credenziali di autenticazione;

c) utilizzazione di un sistema di autorizzazione;

d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;

(segue)

Misure minime art. 33 e 34 Codice Privacy

e) **protezione** degli strumenti elettronici e dei dati **rispetto a trattamenti illeciti di dati**, ad accessi non consentiti e a determinati programmi informatici;

f) adozione di procedure per la **custodia di copie di sicurezza, il ripristino** della disponibilità dei dati e dei sistemi;

[g) tenuta di un aggiornato documento programmatico sulla sicurezza;] (1) ABROGATO

h) adozione di **tecniche di cifratura o di codici identificativi** per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Sanzioni in caso di violazione delle regole

La normativa, in caso di violazione delle regole che disciplinano il trattamento dei dati, prevede alcune sanzioni che possono essere applicate **dal Garante** o dall'**Autorità Giudiziaria** ordinaria.

Le **sanzioni** possono essere di natura:

1. **penale:** comportano l'applicazione di pene detentive o pecuniarie da parte dell'Autorità Giudiziaria;
2. **amministrative:** determinano l'applicazione di sanzioni pecuniarie da parte del Garante o di specifiche limitazioni rispetto al libero trattamento dei dati personali (Garante ha il potere infatti di disporre il blocco del trattamento dei dati).

Sanzioni **penali** - esempi

(Misure di sicurezza) Art. 169

1. Chiunque, essendovi tenuto, **omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni** [o con l'ammenda da diecimila euro a cinquantamila euro.] (1)

2. All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo della sanzione stabilita per la violazione amministrativa. **L'adempimento e il pagamento estinguono il reato**. L'organo che impartisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli articoli 21, 22, 23 e 24 del decreto legislativo 19 dicembre 1994, n. 758, e successive modificazioni, in quanto applicabili (2).

Sanzioni **penali** - esempi

(Trattamento illecito di dati) Art. 167

1. Salvo che il fatto costituisca più grave reato, chiunque**, al fine di trarne per sé o per altri profitto** o di recare **ad altri un danno**, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, **se dal fatto deriva nocumento**, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.

2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, **22, commi 8 [*I dati idonei a rivelare lo stato di salute non possono essere diffusi*]** e 11, 25, 26, 27 e 45, è punito, **se dal fatto deriva nocumento**, con la reclusione da uno a tre anni.

Sanzioni in caso di violazione delle regole

Per l'integrazione del **reato** è necessario dunque che sia accertato un **dolo specifico** «***al fine di trarne per sé o per altri profitto o di recare ad altri un danno***» e che sia dimostrato il «***nocumento***» inteso, secondo la giurisprudenza, come un pregiudizio economicamente apprezzabile.

Sanzioni **amministrative** - esempi

(Omessa o inidonea informativa all'interessato) Art. 161

1. La violazione delle disposizioni di cui all'articolo 13 è punita con la sanzione amministrativa del pagamento di una somma da seimila euro a trentaseimila euro;

(Altre fattispecie) Art. 162

2 La violazione della disposizione di cui all'articolo 84, comma 1, è punita con la sanzione amministrativa del pagamento di una somma da mille euro a seimila euro (2).

2-bis. In caso di trattamento di dati personali effettuato in violazione delle misure indicate nell'articolo 33 o delle disposizioni indicate nell'articolo 167 è altresì applicata in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma da diecimila euro a centoventimila euro. Nei casi di cui all'articolo 33 è escluso il pagamento in misura ridotta (3).

Azioni risarcitorie

La normativa italiana demanda alla **giurisdizione dell'Autorità Giudiziaria Ordinaria** ogni azione volta ad ottenere il risarcimento del danno tanto patrimoniale quanto non patrimoniale derivante dall'illecito trattamento dei dati.

In ogni caso la tutela offerta dal Garante è alternativa a quella dell'Autorità Giudiziaria Ordinaria: infatti il ricorso al Garante non può essere proposto se, per il medesimo oggetto e tra le stesse parti, è stata già adita l'Autorità Giudiziaria.

Azioni risarcitorie

L'interessato che ritiene di aver subito un danno dall'illegittimo trattamento dei dati può chiedere, esclusivamente all'Autorità Giudiziaria, il risarcimento del danno subito.

La normativa prevede quindi una **particolare ipotesi di responsabilità extracontrattuale** per i danni cagionati a seguito di trattamento di dati personali.

Infatti in questi casi si applica la disciplina prevista dal codice civile per l'esercizio di attività pericolose, in base alla quale, **per evitare di essere obbligati al risarcimento occorre dimostrare di aver adottato tutte le misure idonee a evitare il danno.**

Azioni risarcitorie

La normativa prevede inoltre espressamente che, in caso di **violazione della disciplina in materia di modalità del trattamento e requisiti dei dati**, è risarcibile ***anche il danno non patrimoniale***, cioè il danno che non incide direttamente sull'integrità economica dell'interessato.

Peraltro, rimane in ogni caso a carico del danneggiato l'onere di provare l'esistenza del nesso causale fra l'attività di trattamento dei dati personali e l'evento dannoso e la quantificazione del danno

Dal 25 Maggio 2018…

GDPR
General Data Protection Regulation

Nuovo Regolamento 2016/679/UE

del Parlamento Europeo
e del Consiglio

Nuovo Regolamento 2016/679/UE del Parlamento Europeo e del Consiglio

FONDAMENTI DI LICEITA' DEL TRATTAMENTO

Il regolamento conferma che **ogni trattamento deve trovare fondamento in un'idonea base giuridica**; i fondamenti di liceità del trattamento sono indicati all'**art. 6** del regolamento e **coincidono, in linea di massima, con quelli previsti attualmente dal Codice**

(**consenso**, adempimento obblighi contrattuali, **interessi vitali della persona interessata o di terzi**, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati).

CONSENSO

Cosa cambia?

- Per i dati "sensibili" (art. 9 regolamento) il consenso **DEVE** essere "esplicito"; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione – art. 22).

- **NON** deve essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta", anche se questa è modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito" (per i dati sensibili); inoltre, **il titolare (art. 7.1) DEVE essere in grado di dimostrare che l'interessato ha prestato il consenso** a uno specifico trattamento.

- Il **consenso dei minori** è valido **a partire dai 16 anni**; prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.

Cosa non cambia?

- **DEVE** essere, in tutti i casi, libero, specifico, informato e inequivocabile e **NON** è ammesso il consenso tacito o presunto (no a caselle **pre-spuntate** su un modulo).

- **DEVE** essere manifestato attraverso "**dichiarazione o azione positiva inequivocabile**"

L'Informativa

I **contenuti dell'informativa** sono elencati in modo tassativo negli articoli 13, paragrafo 1, e 14, paragrafo 1, del regolamento e in parte sono più ampi rispetto al Codice. In particolare, il titolare deve sempre **specificare i dati di contatto del RPD-DPO** (Responsabile della protezione dei dati - Data Protection Officer), ove esistente, **la base giuridica del trattamento**, qual è il suo interesse legittimo se quest'ultimo costituisce la base giuridica del trattamento, nonché **se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti** (esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; si utilizzano BCR di gruppo; sono state inserite specifiche clausole contrattuali modello, ecc.).

- Il regolamento prevede **anche ulteriori informazioni in quanto "necessarie per garantire un trattamento corretto e trasparente":** in particolare, il titolare deve specificare il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di presentare un reclamo all'autorità di controllo.

- **Se il trattamento comporta processi decisionali automatizzati** (anche la profilazione), l'informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

Esempio di adeguamento al GDPR

SIAE DALLA PARTE DI CHI CREA

CHI SIAMO

DIRITTO D'AUTORE · AUTORI ED EDITORI · UTILIZZATORI · INIZIATIVE E NEWS · SERVIZI ONLINE

- LA SIAE
- I REPERTORI
- LO SPETTACOLO IN CIFRE
- CULTURA E SOLIDARIETÀ
- UFFICI E CONTATTI
- DOCUMENTI E FAQ

FAQ - Cose da sapere

INFORMATIVA RESA AI SENSI DEGLI ART. 13-14 DEL GDPR (GENERAL DATA PROTECTION REGULATION) 2016/679

Secondo la normativa indicata, tale trattamento sarà improntato ai principi di correttezza, liceità, trasparenza e di tutela della Sua riservatezza e dei Suoi diritti.

Ai sensi dell'articolo 13 del GDPR 2016/679, pertanto, Le forniamo le seguenti informazioni:

1. I dati personali (nome, cognome, estremi documento di riconoscimento e copia dello stesso, telefono, indirizzo email, etc), saranno forniti al momento dell'adesione in funzione del tipo di associazione richiesta.

I dati personali forniti saranno oggetto:

a. in relazione ad **obblighi contrattuali**, di **Statuto** e di **Regolamento Generale**:
   i. di trattamento relativo alle funzioni istituzionali esercitate dalla SIAE, ai sensi dell'art. 180 L. 633/41, riguardanti la protezione in genere delle opere dell'ingegno e dei diritti connessi anche con ripartizione dei proventi riscossi a seguito dell'utilizzazione economica delle opere dell'ingegno;

1. I dati personali vengono conservati per tutta la durata del rapporto di associazione e/o mandato e, nel caso di revoca e/o altro tipo di cessazione del rapporto, nei termini prescrizionali indicati nell'art. 19 del D. L.vo 35/2017.

1. Lei potrà, in qualsiasi momento, esercitare i diritti:

a. di accesso ai dati personali;
b. di ottenere la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano;
c. di opporsi al trattamento;
d. alla portabilità dei dati;
e. di revocare il consenso, ove previsto: la revoca del consenso non pregiudica la liceità del trattamento basata sul consenso conferito prima della revoca;
f. di proporre reclamo all'autorità di controllo (Garante Privacy).

L'esercizio dei suoi diritti potrà avvenire attraverso l'invio di una richiesta mediante email all'indirizzo privacy@siae.it.

1. Il Titolare del trattamento dati è la SIAE con sede legale in Roma, Viale della Letteratura 30, 00144 – Roma. Il Responsabile del Trattamento, cui è possibile rivolgersi per esercitare i diritti di cui all'Art. 12 e/o per eventuali chiarimenti in materia di tutela dati personali, in SIAE è raggiungibile all'indirizzo: privacy@siae.it.

IL TITOLARE

Società Italiana Autori ed Editori (SIAE)

ESEMPIO DI INFORMATIVA: Fondazione Studi CDL

INFORMATIVA RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI (ART. 13 REG. UE 2016/679) Ai fini previsti dal Regolamento Ue n. 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, il/la Sig./Sig.ra (interessato) nato a_____ il_____, residente in _____, c.f. _____, è informato che il trattamento dei dati personali dallo stesso forniti ed acquisiti, saranno oggetto di trattamento nel rispetto della normativa prevista dal premesso Regolamento nel rispetto dei diritti ed obblighi conseguenti. a) Titolare del trattamentoIl titolare del trattamento è il Dott._____, con studio in_____, c.f._____, iscritto col n.____ presso l'Albo del Consiglio Provinciale dell'Ordine di_____; b) Responsabile protezione dati (eventuale) Il Responsabile protezione dati (c.d. DPO) è il/la Sig.ra/Dott.ssa_____, Via_____, e.mail:_____;

ESEMPIO DI INFORMATIVA: Fondazione Studi CDL

c) Finalità del trattamento

I dati personali forniti sono necessari ai fini della conclusione e della gestione del rapporto di incarico professionale, per gli adempimenti di legge previsti per lo svolgimento dell'attività di Consulente del Lavoro;
d) Periodo di conservazione dei dati

La conservazione dei dati personali forniti avverrà per tutta la durata dell'incarico professionale conferito e per ulteriori anni ….

ESEMPIO DI INFORMATIVA: Fondazione Studi CDL

e) **Diritti dell'interessato** In relazione ai dati oggetto del trattamento di cui alla presente informativa all'interessato è riconosciuto in qualsiasi momento il diritto di:

-Accesso (art. 15 Regolamento UE n. 2016/679);

-Rettifica (art. 16 Regolamento UE n. 2016/679);

-Cancellazione (art. 17 Regolamento UE n. 2016/679);

-Limitazione (art. 18 Regolamento UE n. 2016/679);

-Portabilità, intesa come diritto ad ottenere dal titolare del trattamento i dati in unformato strutturato di uso comune e leggibile da dispositivo automatico pertrasmetterli ad un altro titolare del trattamento senza impedimenti (art. 20Regolamento UE n. 2016/679);

-Opposizione al trattamento (art. 21Regolamento UE n. 2016/679);

-Revoca del consenso al trattamento, senza pregiudizio per la liceità del trattamentobasata sul consenso acquisito prima della revoca (art. 7, par. 3 Regolamento UE n.2016/679);

-Proporre reclamo all'Autorità Garante per la Protezione dei dati personali (art. 51Regolamento UE n. 2016/679).

ESEMPIO DI INFORMATIVA: Fondazione Studi CDL

L’esercizio dei premessi diritti può essere esercitato mediante comunicazione scritta da inviare a mezzo pec all’indirizzo _____ o lettera raccomandata a/r all’indirizzo _____

Il/la sottoscritto/a dichiara di aver ricevuto l’informativa che precede.

Luogo e data

_____

Art. 35 – la «VIP(D)» o DPIA

Valutazione d'impatto sulla protezione dei dati

1. Quando un tipo di trattamento, allorché prevede 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 effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

Il Responsabile della Protezione dei Dati (RPD) o Data Protection Officer (DPO)

QUALI SONO I REQUISITI?

Il Responsabile della protezione dei dati, nominato dal titolare del trattamento o dal responsabile del trattamento, dovrà:

1. possedere **un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali**, anche in termini di misure tecniche e organizzative o di misure atte a garantire la sicurezza dei dati. Non sono richieste attestazioni formali o l'iscrizione ad appositi albi professionali, anche se la partecipazione a master e corsi di studio/professionali può rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenze.

2. **adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse**. In linea di principio, ciò significa che il RPD non può essere un soggetto che decide sulle finalità o sugli strumenti del trattamento di dati personali;

3. **operare alle dipendenze del titolare o del responsabile oppure sulla base di un contratto di servizio** (RPD/DPO esterno). Il titolare o il responsabile del trattamento dovranno mettere a disposizione del Responsabile della protezione dei dati le risorse umane e finanziarie necessarie all'adempimento dei suoi compiti.

Il Responsabile della protezione dei dati (RPD) o Data Protection Officer (DPO)

IN QUALI CASI E' PREVISTO?

Dovranno designare obbligatoriamente un RPD:

a) **amministrazioni ed enti pubblici**, fatta eccezione per le autorità giudiziarie;

b) **tutti i soggetti la cui** attività principale consiste in **trattamenti che**, per la loro natura, il loro oggetto o le loro finalità, **richiedono il monitoraggio regolare e sistematico degli interessati su larga scala**;

c) **tutti i soggetti la cui attività principale consiste nel trattamento**, su larga scala, **di dati sensibili, relativi alla salute** o alla vita sessuale, genetici, giudiziari e biometrici.

Anche per i casi in cui il regolamento non impone in modo specifico la designazione di un RPD, è possibile una nomina su base volontaria.

Un gruppo di imprese o soggetti pubblici possono nominare **un unico RPD**

Il Responsabile della protezione dei dati (RPD) o Data Protection Officer (DPO)

QUALI SONO I COMPITI?

Il Responsabile della protezione dei dati dovrà, in particolare:

a) **sorvegliare l'osservanza del regolamento**, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità;

b) collaborare con il titolare/responsabile, laddove necessario, nel condurre una **valutazione di impatto sulla protezione dei dati** (DPIA);

c) **informare e sensibilizzare** il titolare o il responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo **agli obblighi derivanti dal regolamento e da altre disposizioni** in materia di protezione dei dati;

d) **cooperare con il Garante** e fungere da punto di contatto per il Garante su ogni questione connessa al trattamento;

e) **supportare il titolare o il responsabile in ogni attività** connessa al trattamento di dati personali, anche con riguardo alla tenuta di un **registro delle attività**

Registro dei trattamenti

Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio (art. 30, paragrafo 5), **devono tenere un registro delle operazioni di trattamento** i cui contenuti sono indicati all'art. 30.

Si tratta di uno strumento fondamentale non soltanto ai fini **dell'eventuale supervisione da parte del Garante**, ma anche allo scopo di **disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda** o di un soggetto pubblico – indispensabile per ogni valutazione e analisi del rischio.

Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

Diritto alla portabilità dei dati

COSA È?

È un diritto innovativo previsto dall'articolo 20 del regolamento (Ue) 2016/679 che consente all'interessato di ricevere i dati personali forniti a un titolare, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, e di trasmetterli a un altro titolare del trattamento senza impedimenti.

QUALI VANTAGGI PUO' OFFRIRE?

- facilitare il passaggio da un fornitore di servizi all'altro;
- consentire la creazione di nuovi servizi nel quadro della strategia dell'Ue per il mercato unico digitale;
- offrire la possibilità di «riequilibrare» il rapporto fra interessati e titolari del trattamento tramite l'affermazione dei diritti e del controllo spettanti agli interessati in rapporto ai dati personali che li riguardano.

Diritto alla portabilità dei dati

COSA PERMETTE DI FARE?

• ricevere dati personali trattati da un titolare e conservarli **su un supporto personale o un cloud privato** in vista di un utilizzo ulteriore per scopi personali, senza trasmetterli necessariamente a un altro titolare (es: recuperare l'elenco dei brani musicali preferiti detenuto da un servizio di musica in streaming, per scoprire quante volte si sono ascoltati determinati brani);

• **trasmettere dati personali da un titolare del trattamento a un altro titolare** del trattamento (es.: un diverso fornitore di servizi). L'esercizio del diritto alla portabilità dei dati non pregiudica nessuno degli altri diritti dell'interessato, che può, per esempio:

• continuare a fruire del servizio offerto dal titolare anche dopo un'operazione di portabilità;

• esercitare il **diritto di cancellazione (o «diritto all'oblio»)** ai sensi dell'art. 17 del regolamento.

L'autorità di controllo capofila e la cooperazione prevista dal meccanismo di "sportello unico" nel regolamento 2016/679

L'autorità di controllo capofila è, in sintesi, **l'autorità dello stabilimento principale o unico nell'Ue del titolare o responsabile del trattamento**, alla quale viene trasferita la competenza da tutte le altre autorità di controllo (definite, in questo caso, "autorità interessate") per quanto riguarda i "**trattamenti transfrontalieri**" di dati personali svolti da quel titolare o responsabile.

L'obiettivo della devoluzione di competenze a favore dell'autorità capofila è **garantire l'esistenza di uno "sportello unico" per i trattamenti transfrontalieri di dati personali**: principio sancito dal paragrafo 6 dell'art. 56 ("L'autorità di controllo capofila è l'unico interlocutore del titolare del trattamento o del responsabile del trattamento in merito al trattamento transfrontaliero effettuato da tale titolare o responsabile").

Notifica violazioni di dati personali (data breach)

A partire dal 25 maggio 2018, **tutti i titolari** – e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene oggi – **dovranno notificare all'Autorità di controllo le violazioni di dati personali e le fughe di dati, di cui vengano a conoscenza, entro 72 ore** e comunque "**senza ingiustificato ritardo**", ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati.

Pertanto, **la notifica** all'Autorità dell'avvenuta violazione non è obbligatoria, essendo **subordinata alla valutazione del rischio** per gli interessati che spetta, ancora una volta, al titolare. Se la probabilità di tale rischio è elevata, si dovrà informare delle violazione anche gli interessati, sempre "senza ingiustificato ritardo"; fanno eccezione le circostanze indicate al paragrafo 3 dell'art. 34, che coincidono solo in parte con quelle attualmente menzionate nell'art. 32-bis del Codice. I contenuti della notifica all'Autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli art. 33 e 34 del regolamento.

Sicurezza dei dati (cyber-security, ma non solo)

La sicurezza dei dati raccolti è garantita dal titolare del trattamento e dal responsabile del trattamento chiamati a **mettere in atto misure tecniche e organizzative idonee per garantire un livello di sicurezza adeguato al rischio** ***(analisi del rischio)***

A tal fine **il titolare e il responsabile** del trattamento garantiscono che chiunque acceda ai dati raccolti lo faccia nel rispetto dei poteri da loro conferiti e dopo essere stato appositamente istruito, salvo che lo richieda il diritto dell'Unione o degli Stati membri (Articolo 32).

A garanzia dell'interessato il Regolamento UE 2016/679 regolamenta anche il caso di trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale (Articolo 44 e ss) e prevede che l'interessato venga prontamente informato in presenza di una violazione che metta a rischio i suoi diritti e le sue libertà (Articolo 33)

LE SANZIONI

previste dal GDPR

SANZIONI DI CARATTERE ECONOMICO

Di seguito sono riportate le sanzioni (c.d. **multe**) previste dal Regolamento Europeo che, ai sensi dell'art. 83, devono avere carattere di effettività, proporzionalità e dissuasività.

La decisione sull'applicazione delle sanzioni spetta all'autorità di controllo (in Italia: l'Autorità Garante per la Protezione dei Dati Personali), che, nella valutazione, tiene conto delle circostanze del singolo caso, ossia:

- della **natura, gravità e durata della violazione**
- del carattere **doloso o colposo** della violazione
- delle **misure adottate per attenuare il danno** subito dagli interessati
- delle **eventuali precedenti violazioni** commesse dal titolare del trattamento
- del grado di **cooperazione con l'autorità di controllo**
- degli eventuali altri fattori aggravanti

SANZIONI DI CARATTERE ECONOMICO

- Inosservanza degli obblighi del titolare e del responsabile del trattamento; inosservanza degli obblighi dell'organismo di certificazione; inosservanza degli obblighi dell'organismo di controllo:
  fino a **10 milioni di Euro**, o per le imprese, fino al **2% del fatturato annuo mondiale** dell'esercizio precedente.
- Inosservanza dei principi base del trattamento; inosservanza dei diritti degli interessati; inosservanza delle disposizioni sul trasferimento dei dati personali in paesi terzi o verso organizzazioni internazionali; inosservanza di un ordine, limitazione provvisoria o definitiva o di un ordine di sospensione dei flussi da parte dell'autorità di controllo:
  fino a **20 milioni di Euro**, o per le imprese, fino al **4% del fatturato** annuo mondiale dell'esercizio precedente.
- Inosservanza di un ordine correttivo dell'autorità di controllo:
  fino a **20 milioni di Euro**, o per le imprese, fino al **4% del fatturato** annuo mondiale dell'esercizio precedente.

SANZIONI CORRETTIVE

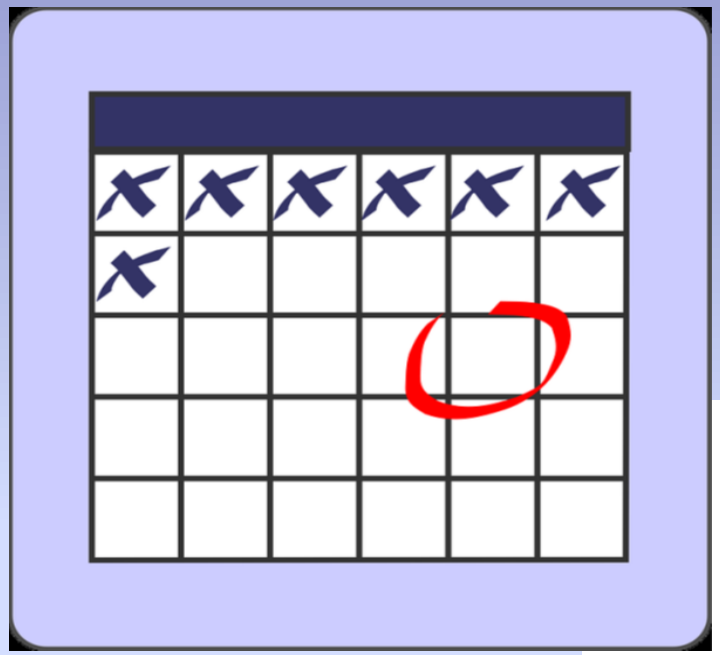
Le sanzioni correttive sono connesse ai **poteri** dell'Autorità di controllo. Essi consistono nel:

- **Rivolgere avvertimenti** al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono violare il GDPR
- **Rivolgere ammonimenti** al titolare e del trattamento o al responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del GDPR
- **Ingiungere** al titolare del trattamento o al responsabile del trattamento **di soddisfare le richieste**dell'interessato di esercitare i relativi diritti
- **Ingiungere** al titolare o al responsabile del trattamento **di conformare i trattamenti alle disposizioni del GDPR**, anche specificando in che modo ed entro quale termine
- **Ingiungere** al titolare del trattamento **di comunicare all'interessato una violazione** dei dati personali

Segue: SANZIONI CORRETTIVE

- **Imporre una limitazione** provvisoria o definitiva al trattamento, incluso il divieto di trattamento
- **Ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento** e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali
- **Revocare la certificazione** o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti
- **Infliggere una sanzione amministrativa pecuniaria** in aggiunta alle presenti misure (v. sopra)
- **Ordinare la sospensione dei flussi** di dati verso un destinatario in un paese terzo o un'organizzazione internazionale

Save the date: 25 maggio 2018



La brutta notizia è che il tempo vola.

La buona è che il pilota sei tu.

Michael Altshuler

Cosa Cambia?

Modifiche	Novita'
Modifica di definizioni esistenti	Estensione ambito territoriale
Specificazione dei ruoli e compiti di Titolare e Responsabile	Nuove definizioni (profilazione, dati biometrici, ecc.)
Informativa rafforzata	Il Responsabile della protezione dei dati (c.d. "Data Protection Officer")
Il consenso	Il Registro dei trattamenti
Specificazione di diritti	La valutazione preventiva d'impatto
Inasprimento sanzioni	Notifica dei data breach Diritto all'oblio e a Portabilità dei dati
	Privacy *by design* – privacy *by default*

Possibiità per le aziende:

	Applicazione diretta del regolamento	Applicazione del Codice di Condotta	Certificazione
Caratteristica	Obbligatorio	Volontario	Volontario
Possibili Sanzioni 4% fatturato	SI	NO	NO
Evidenza Immediata di Conformità al regolamento	NO	NO	SI

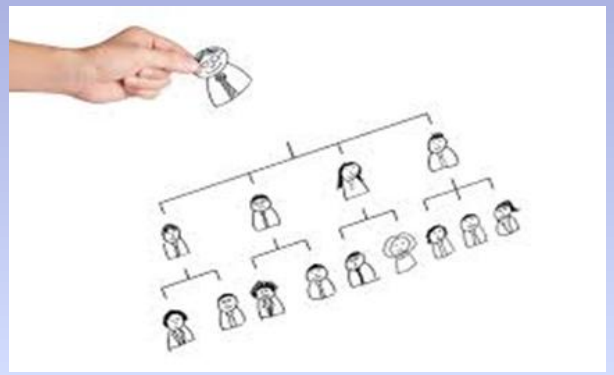
I nuovi imperativi:

1) Tratta meno dati che puoi

2) Distribuisci le responsabilità e documenta i trattamenti

3) Favorisci l’anonimizzazione e la pseudonimizzazione.

Quali sono le milestones per applicare il regolamento?



Definizione di ruoli, compiti e regole

Risultato finale e' che il **Rischio Residuo** sia minore del Rischio Accettabile

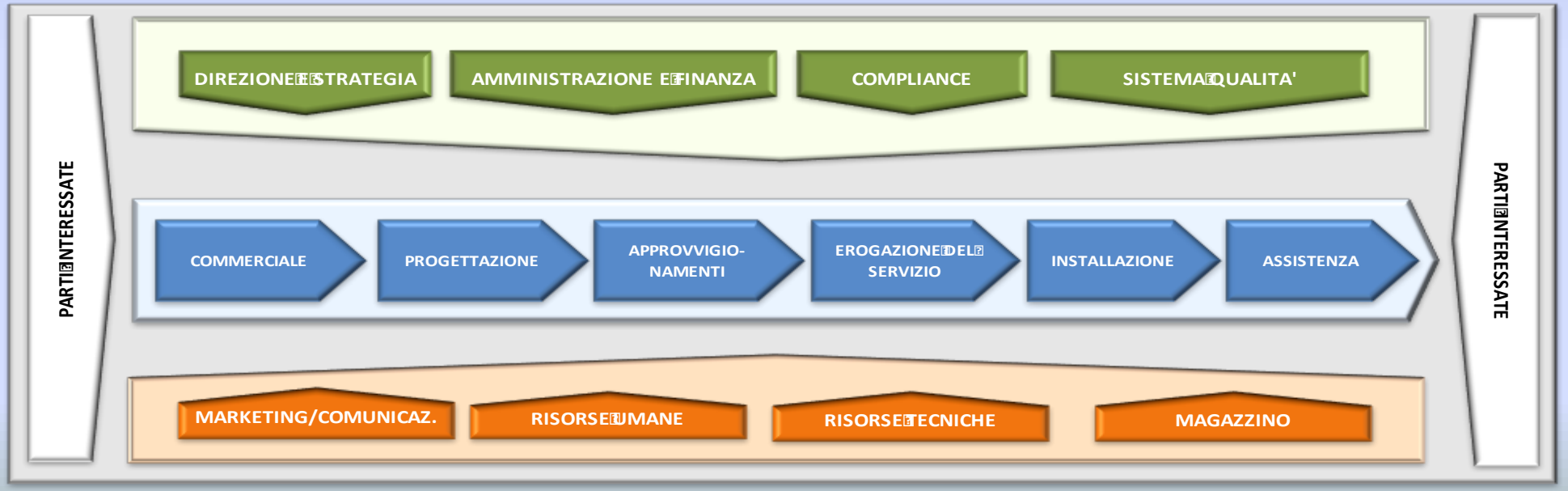
Integrazione delle norme

GDPR è una parte del TUTTO

Accountability / Responsabilizzazione

Ai Titolari e ai Responsabili del trattamento viene affidato il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali → **STRATEGIA**

Rispetto delle disposizioni normative e di alcuni criteri specifici indicati nel regolamento attraverso l'adozione di misure «ad hoc» → **DIREZIONE**



Data protection by default and by design

- L'art. 25 del Regolamento introduce la necessità di **configurare il trattamento** prevedendo fin dall'inizio le garanzie indispensabili al fine di soddisfare i requisiti normativi e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

- Tutto questo deve avvenire **a monte, prima di procedere al trattamento dei dati** vero e proprio e richiede, pertanto, un'analisi preventiva con una serie di attività specifiche e dimostrabili.

Privacy by default e privacy by design

Processo	*Sottoprocesso*	*Obiettivi*
Risorse Umane	Recruiting	Individuare la persona fisica che può ricoprire la funzione aziendale vacante

Contesto interno	*Trattamento*	*Contesto esterno*	*Interessati (dati raccolti)*
Funzione HR, Area di collocazione	Raccolta, condivisione, elaborazione e conservazione dei dati attraverso la sezione «Lavora con noi» del sito web, i report dell'agenzia esterna e le risposte all'annuncio sui quotidiani	Webmaster, Redazione quotidiano, Agenzia ricerca personale, Consulenza, ecc.	Candidati e neo assunti (CV, note colloquio, cellulare, stato famiglia, casellario giudiziario, IBAN, sindacato, ecc.)

Valutazione di impatto

Rischio	*Contromisura*
Informativa web incompleta	Redigere l'informativa seguendo passo passo quanto indicato nell'art. 13
Mancanza evidenza informativa web letta dall'interessato	Aggiungere un controllo sullo scroll dell'informativa che soltanto al termine della stessa renda cliccabile la check-box di conferma di lettura
Consenso web generico	Aggiungere check-box di accettazione per ogni singolo trattamento che lo richieda
CV contenente dati sensibili	Aggiungere disclaimer «non inserire CV contenenti dati sensibili» e specificare cosa succederà in caso si ricevessero CV non conformi
…	…

Cosa comporta l'applicazione del Regolamento

1. **Data Mapping** (Definizione di tutte le tipologie di trattamento, finalità di raccolta, responsabilità, ubicazione)
2. Definizione del Registro dei Trattamenti, eventuale nomina DPO
3. Analisi del rischio
4. Valutazione impatto e minimizzazione del rischio
5. Definizione ruoli e responsabilità (Titolare del trattamento, Responsabile, Incaricati interni ed esterni, ecc.)
6. Definizione di procedure tecniche (Ad es. policy, prove di leggibilità, backup, disaster recovery, data breach, ecc.)
7. Definizione di procedure organizzative (modalità di raccolta del consenso, clausole contrattuali, regolamento utilizzo PC e rete ...)
8. Formazione interna
9. Audit interni ed esterni legati alla gestione dei dati

*La «**data protection**» sarà sempre di più un **fattore competitivo** e favorirà le aziende che capiranno che non si tratta più solo di una serie di adempimenti da gestire ma di **un processo organizzativo aziendale** che ha **natura produttiva** e **non solo normativa.***

Grazie per l'attenzione.

a cura di: Avv. Marco Longoni