GENERAL DATA PROTECTION REGULATION
IL REGOLAMENTO UE 2016/679

Il nuovo regolamento: a chi si rivolge

Il Regolamento si applica solo al trattamento dei dati personali di persone fisiche (definite "interessati" dal Regolamento).

Lo conferma anche la definizione di «impresa»: "la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica".

Le persone giuridiche sono fuori dal regolamento, anche se "contraenti" e anche se destinatarie di marketing via e-mail, sms, mms, fax, ecc.

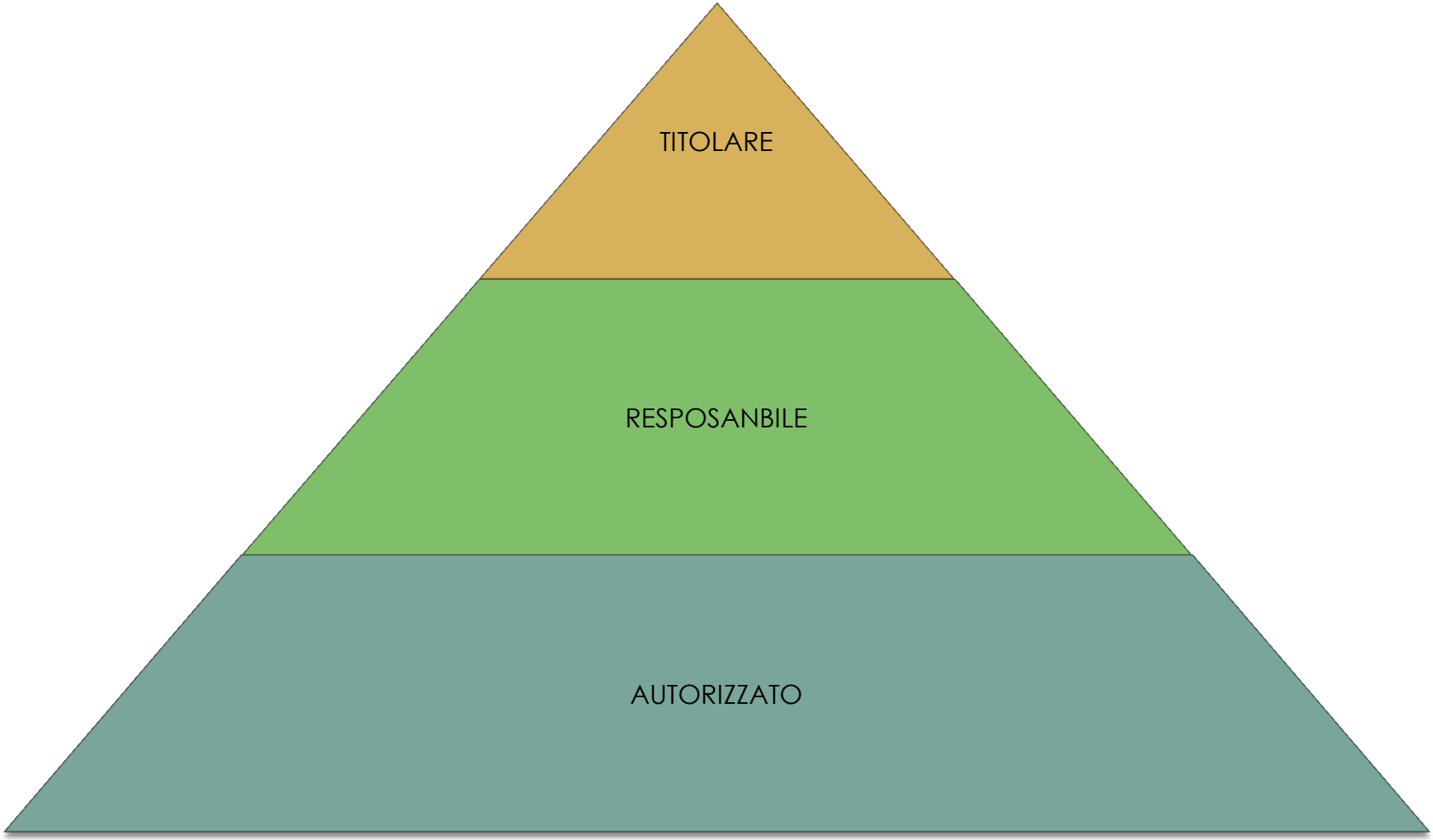
Il Regolamento si applica inoltre:

1) al trattamento di dati personali effettuato da un titolare stabilito nella UE;

ma anche

2) al trattamento di dati personali effettuato da titolari non stabiliti nell'Unione Europea se il trattamento ha ad oggetto dati personali di interessati che si trovano nella UE e riguarda (1) l'offerta di beni o servizi (anche non a pagamento) ai suddetti interessati (2) il monitoraggio del loro comportamento nel territorio dell'Unione Europea.

Organigramma della sicurezza



Titolare del trattamento (data controller)

La 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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

È l'entità che in base alla legge o allo statuto ha il potere di decisione autonomo.

Nel caso di persone giuridiche, il "titolare del trattamento" è l'ente nel suo complesso, non il singolo organo decisionale o la persona fisica (o le persone fisiche) che lo rappresentano (così come la responsabilità privacy sarà imputata all'ente in quanto tale).

Contitolarità

Come chiarito dal Parere n. 1/2010 dell' art. 29 Working Party:

La partecipazione alla determinazione delle finalità e dei mezzi congiunta (anche ripartita in modo disomogeneo).

I contitolari devono condividere finalità o strumenti in un insieme di operazioni comuni.

ESEMPIO CONTRARIO

> **Un'agenzia possiede un utenza su un sito di annunci, sul quale anche utenti privati pubblicano a loro volta annunci fornendo i loro dati personali. L'agenzia contatta regolarmente gli utenti privati del sito per proporre possibili acquirenti e richiedendo loro l'incarico. In questo caso, l'agenzia e il sito di annunci sono titolari distinti, ciascuno soggetto agli obblighi di protezione dei dati in relazione al proprio trattamento.**

Il Responsabile del trattamento (data processor)

Il responsabile del trattamento (nel nuovo regolamento europeo data processor) è la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento.

Il titolare del trattamento, quindi, nomina uno o più responsabili.

In base all'art. 28 del nuovo regolamento generale europeo, la nomina deve avvenire tramite contratto o altro "atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento".

Il contratto deve, quindi, essere conforme a quanto stabilito dell'art. 28 del nuovo Regolamento Generale. Col contratto il titolare delega al responsabile la concreta gestione del trattamento, affidandogli uno o più compiti specifici oppure una serie di compiti dettagliati in generale. Il responsabile a sua volta può nominare responsabili di secondo livello, a meno che non sia vietato dalle istruzioni del titolare. E' comunque il responsabile principale a rispondere dell'operato degli altri da lui nominati, di fronte al titolare del trattamento.

Nel caso in cui il responsabile del trattamento ecceda i limiti di utilizzo dei dati fissati dal titolare, il responsabile diventa titolare della gestione illecita dei dati e ne risponde come tale, insieme all'effettivo titolare (in sostanza è come se diventassero contitolari).

Il Responsabile del trattamento: obbligo o facoltà?

Il Regolamento prescrive la obbligatorietà della nomina soprattutto in caso di esternalizzazione del trattamento. È invece del tutto facoltativa la nomina di sub-responsabili da parte del responsabile a ciò autorizzato dal titolare del trattamento.

Il Responsabile del trattamento: considerando 29

Inoltre, il Considerando (29) del Regolamento prevede che il titolare del trattamento deve indicare le persone autorizzate all'interno dello stesso titolare del trattamento, mentre tra i compiti del Responsabile del trattamento (che può per delega del titolare "istruire" tali persone autorizzate) da definirsi con il "contratto" vi è la disciplina che "garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza".

Nella recente Guida al Regolamento UE rilasciata dal Garante per la privacy il 28 aprile scorso, è chiarito che: "le disposizioni del Codice in materia di incaricati del trattamento sono pienamente compatibili con la struttura e la filosofia del Regolamento, in particolare alla luce del principio di "responsabilizzazione" di titolari e responsabili del trattamento che prevede l'adozione di misure atte a garantire proattivamente l'osservanza del regolamento nella sua interezza. In questo senso, e anche alla luce degli artt. 28, paragrafo 3, lettera b), 29, e 32, paragrafo 4, in tema di misure tecniche e organizzative di sicurezza, si ritiene opportuno che titolari e responsabili del trattamento mantengano in essere la struttura organizzativa e le modalità di designazione degli incaricati di trattamento così come delineatesi negli anni anche attraverso gli interventi del Garante in quanto misure atte a garantire e dimostrare "che il trattamento è effettuato conformemente" al regolamento (si veda art. 24, paragrafo 1, del Regolamento)".

Autorizzato al trattamento

Autorizzato al trattamento: **chiunque agisca sotto l'autorità del Titolare o Responsabile nell'effettuare trattamenti di dati personali deve ricevere adeguate istruzioni affinché i trattamenti effettuati siano conformi al Regolamento**

Anche se non esplicitamente previsto quale obbligo, appare opportuno che, in analogia con la figura di incaricati del trattamento, le persone autorizzate del trattamento siano designate tramite apposito atto di nomina che vado a dettagliare:

- **l'ambito del trattamento cui sono autorizzati**
- **Istruzioni sulle operazioni di trattamento**
- **Istruzioni sulle misure di sicurezza**
- **I profili autorizzati a livello di sistemi informativi**
- **I corsi di formazione sulla protezione dei dati personali**

Sarebbe opportuno elaborare un manuale per la sicurezza e renderlo disponibile a tutte le persone autorizzate al trattamento

Nel contratto di lavoro deve essere indicato che la persona autorizzata al trattamento è autorizzata a trattare i dati personali nei limiti delle istruzioni ricevute

Principi fondamentali del trattamento

I principi fondamentali applicabili al trattamento dei dati personali codificati dal Regolamento sono considerarsi da rispettare in ogni aspetto del trattamento dei dati personali:

- **Principio di liceità, ovvero rispetto delle disposizioni normative**
- **Principio di correttezza, ovvero il trattamento deve avvenire in modo corretto**
- **Principio di trasparenza, ovvero assicurare la consapevolezza dell'interessato**
- **Principio di limitazione delle finalità, ovvero gli scopi del trattamento devono essere determinati, espliciti e legittimi**
- **Principio di minimizzazione dei dati, ovvero il trattamento deve avere a oggetto dati personali adeguati, pertinenti e limitati a quanto necessario per il raggiungimento della specifica finalità di trattamento**
- **Principio di esattezza, ovvero devono essere predisposte le misure affinché o dati siano esatti e aggiornati e ove necessario sia cancellati o rettificati dati inesatti**
- **Principio di limitazione della conservazione, ovvero i dati devono essere conservati in modo da consentire l'identificazione dell'interessato solo per il periodo di tempo necessario per il raggiungimento della specifica finalità per cui sono oggetto di trattamento**
- **Principio di integrità e riservatezza, ovvero i dati devono essere protetti mediante adozione di misure di sicurezza tecniche e organizzative adeguate da trattamenti non autorizzati o illeciti, dalla perdita, distruzione o danno accidentali**

Principi fondamentali del trattamento

Il Titolare del trattamento è responsabile per il rispetto di tutti i principi fondamentali ed è in grado di provarne il rispetto secondo il c.d. principio di accountability (responsabilizzazione)

Il Regolamento richiama il principio di accountability in una serie di adempimenti richiesti al Titolare del trattamento, quali:

- **Rispetto dei diritti degli interessati**
- **Privacy by design**
- **Privacy by default**
- **Nomina Responsabile del trattamento**
- **Istruzioni agli autorizzati al trattamento**
- **Registro dei trattamenti**
- **Adozione di misure di sicurezza adeguate**
- **Notifica e comunicazione degli eventi di Data Breach**
- **Esecuzione del Privacy Impact Assessment (PIA)**
- **Nomina del Data Protection Officer (DPO)**
- **Trasferimento dei dati in territorio extra-UE**

Privacy by design e privacy by default

Privacy by design: protezione **dei dati personali fin dalla progettazione**, ovvero ridurre al minimo il trattamento dei dati personali mediante l'implementazione di misure tecniche e organizzative quali ad esempio la pseudonimizzazione

Già in fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere loro funzioni, si deve tenere conto degli aspetti privacy, in particolare relativamente al diritto alla protezione dei dati personali, in modo che possano essere adempiuti gli obblighi derivanti dal Regolamento

es. Misure organizzative: Adibire un armadio senza ante per le pratiche e metterlo nella sala di attesa / adibire un armadio chiuso a chiave in un locale accessibile esclusivamente al personale.

Privacy by default: protezione del dato personale **per impostazione predefinita**

Devono essere adottate misure tecniche e organizzative idonee a garantire che siano trattati, per impostazione predefinita, solamente i dati personali necessari a raggiungere le specifiche finalità di trattamento. Tale principio si applica:

- alla quantità di dati raccolti
- al periodo di conservazione dei dati
- all'accessibilità a dati

es. Misure organizzative: assegnare a un singolo dipendente le singole pratiche che è autorizzato a trattare.

Diritti degli interessati (artt.12-22)

DIRITTI DEGLI INTERESSATI

- **Diritto a ricevere trasparente e adeguata informativa**
  - Artt. 12-13-14
- **Diritto di accesso**
  - Art.15
- **Diritto di rettifica**
  - Art. 16
- **Diritto alla cancellazione (c.d. diritto all'oblio)**
  - Art. 17
- **Diritto di limitazione del trattamento**
  - Art. 18
- **Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento**
  - Art. 19
- **Diritto alla portabilità dei dati**
  - Art. 20
- **Diritto all'opposizione al trattamento**
  - Art. 21
- **Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione**
  - Art. 22

Diritto a ricevere trasparente e adeguata informativa

Anche nelle vigenze del Regolamento, ruolo primario nel trattamento dei dati personali riviste l'informativa da rendere all'interessato al momento della raccolta dei dati personali presso l'interessato o, se i dati sono ottenuti da altra fonte, entro un termine ragionevole, in funzioni delle circostanze del caso

Nel caso in cui non sia possibile indicare nell'informativa all'interessato l'origine dei dati personali in quanto provengono da più fonti deve essere fornita allo stesso un'informativa di carattere generale

Se i dati personali possono essere oggetto di comunicazione a un altro destinatario, l'interessato deve esserne informato nel momento in cui tale soggetto riceve la prima comunicazione dei dati personali

Il Titolare del trattamento, qualora intende trattare i dati personali per una finalità diversa da quella per cui sono stati raccoltati, deve fornire all'interessato prima di tale ulteriore trattamento, le informazioni necessarie relative a tale nuova finalità

L'obbligo di fornitore l'informativa è derogato nel caso in cui l'interessato dispone già delle informazioni, se l'ottenimento o la comunicazione dei dati personali è prevista per legge o se informare l'interessato fosse impossibile o richiederebbe sforzi sproporzionati

Diritto a ricevere trasparente e adeguata informativa
Art. 13 – dati personali raccolti presso l'interessato

INFORMATIVA PER DATI PERSONALI RACCOLTI PRESSO GLI INTERESSATI

- **Identità e dati di contatto del Titolare del trattamento (di suo eventuale rappresentante) e di eventuale DPO**
- **Finalità di trattamento cui sono destinati i dati personali**
- **Destinatari o categorie di destinatari dei dati personali**
- **L'intenzione del Titolare del trattamento di effettuare trasferimenti di dati personali verso Paesi terzi od organizzazioni internazionali e l'esistenza o l'assenza di decisioni di adeguante dalla Commissione o il riferimento a garanzie adeguate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili**
- **Periodi di conservazione dei dati personali o i criteri utilizzati per determinare questo periodo**
- **I legittimi interessi perseguiti dal Titolare del trattamento o da terzi, qualora il trattamento dei dati personali sia basato su un legittimo interesse**
- **L'esistenza dei diritti dell'interessato a poter richiedere al Titolare del trattamento l'accesso, rettifica, cancellazione o la limitazione del trattamento o l'opposizione al trattamento oltre che il diritto alla portabilità dei dati**
- **Qualora il trattamento si basi sul consenso, l'esistenza del diritto di poter revocare il consenso in qualsiasi momento senza pregiudizio sulla liceità del trattamento fino a quel momento effettuato**
- **Il diritto di proporre reclamo all'Autorità Garante**
- **Se la comunicazione di dati personali è un obbligo statuario o contrattuale o precontrattuale e se l'interessato ha l'obbligo di fornire i dati nonché le conseguenze della mancata comunicazione di tali dati**
- **L'esistenza di processo decisionale automatizzato, compresa la profilazione, e indicazioni della logica utilizzata e delle conseguenze per l'interessato previste da tale tipologia di trattamento**

Diritto a ricevere trasparente e adeguata informativa
Art. 14 – dati personali non ottenuti presso l'interessato

INFORMARIVA PER DATI PERSONALI OTTENUTI DA FONTI TERZE

- **Identità e dati di contatto del Titolare del trattamento (di suo eventuale rappresentante) e di eventuale DPO**
- **Finalità di trattamento cui sono destinati i dati personali**
- **Le categorie di dati personali**
- **Destinatari o categorie di destinatari dei dati personali**
- **L'intenzione del Titolare del trattamento di effettuare trasferimenti di dati personali verso Paesi terzi od organizzazioni internazionali e l'esistenza o l'assenza di decisioni di adeguante dalla Commissione o il riferimento a garanzie adeguate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili**
- **Periodi di conservazione dei dati personali o i criteri utilizzati per determinare questo periodo**
- **I legittimi interessi perseguiti dal Titolare del trattamento o da terzi, qualora il trattamento dei dati personali sia basato su un legittimo interesse**
- **L'esistenza dei diritti dell'interessato a poter richiedere al Titolare del trattamento l'accesso, rettifica, cancellazione o la limitazione del trattamento o l'opposizione al trattamento oltre che il diritto alla portabilità dei dati**
- **Qualora il trattamento si basi sul consenso, l'esistenza del diritto di poter revocare il consenso in qualsiasi momento senza pregiudizio sulla liceità del trattamento fino a quel momento effettuato**
- **Il diritto di proporre reclamo all'Autorità Garante**
- **La fonte da cui hanno origine i dati personali con indicazione se trattasi di fonte accessibile al pubblico**
- **L'esistenza di processo decisionale automatizzato, compresa la profilazione, e indicazioni della logica utilizzata e delle conseguenze per l'interessato previste da tale tipologia di trattamento**

Registro dei trattamenti

Il Registro dei trattamenti è uno documento che contiene la mappatura di tutte le caratteristiche dei trattamenti dei dati personali effettuati dal Titolare del trattamento e dal Responsabile del trattamento

Ha una funzione descrittiva e deve rappresentare la situazione reale in cui sono eseguite le attività di trattamento e, su richiesta, è messo a disposizione dell'Autorità Garante

Possono essere tenuti in forma scritta, anche in formato elettronico

La tenuta del Registro è obbligatoria

- **per le organizzazioni con più di 250 dipendenti**
- **se i trattamenti effettuati possano presentare un rischio per i diritti e le libertà dell'interessato**
- **se i trattamenti di categorie particolari di o ai dati personali relativi a condanne penali e a reati**

Al di la dell'obbligatorietà la tenuta del Registro dei trattamenti è un'occasione per verificare il rispetto dei principi fondamentali, per la liceità del trattamento, per la verifica del rispetto dei principi di privacy by design e privacy di default

Registro dei trattamenti del Titolare

CONTENUTI MINIMO

DEL

REGISTRO

DEI TRATTAMENTI DEL TITOLARE

- **il nome e i dati di contatto del Titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del Titolare del trattamento e del Data Protection Officer**
- **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, compresi i destinatari di paesi terzi od organizzazioni internazionali**
- **ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale e in mancanza di decisioni di adeguatezza, la documentazione circa le garanzie adottate**
- **ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati**
- **ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative implementate**

Registro dei trattamenti del Responsabile

CONTENUTI MINIMO

DEL

REGISTRO

DEI TRATTAMENTI DEL TITOLARE

- **il nome e i dati di contatto del Responsabile o dei responsabili del trattamento, di ogni Titolare del trattamento per conto del quale agisce il Responsabile del trattamento, del rappresentante del Titolare del trattamento o del Responsabile del trattamento e, ove applicabile, del Data Protection Officer**
- **le categorie dei trattamenti effettuati per conto di ogni Titolare del trattamento**
- **ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale e in mancanza di decisioni di adeguatezza, la documentazione circa le garanzie adottate**
- **ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative implementate**

Sicurezza dei dati e valutazione dei rischi

Il Titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

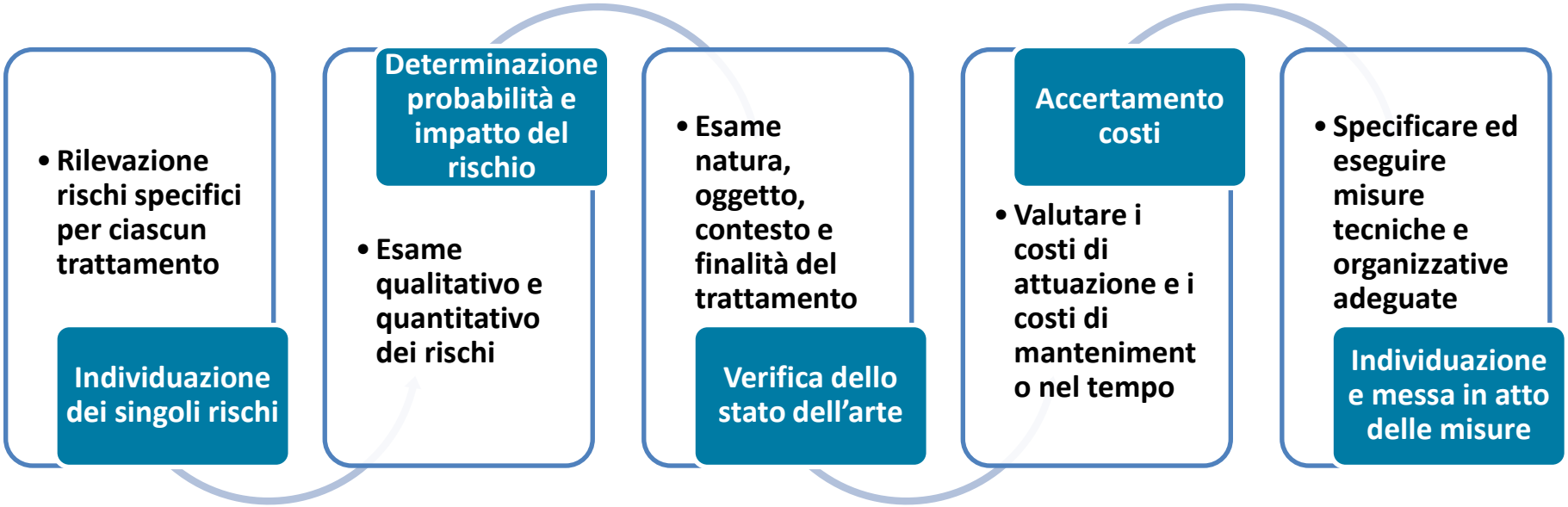
ESEMPI DI MISURE DI SICUREZZA ADEGUATE

- **la pseudonimizzazione e la cifratura dei dati personali**
- **la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento**
- **la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico**
- **una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento**

Sicurezza dei dati e valutazione dei rischi

Rischi da tenere in considerazione nel valutare l'adeguato livello di sicurezza sono:

- **derivanti dalla distruzione, dalla perdita, dalla modifica dei dati personali**
- **derivanti dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali**



Privacy Impact Assessment

In caso di trattamenti che, alla luce dell'uso di nuove tecnologie, della natura, dell'oggetto, del contesto e delle finalità del trattamento, possono presentare rischii elevati per i diritti e le libertà delle persone fisiche, il Titolare del trattamento effettua, prima di procedere al trattamento, deve effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali

QUANDO LA PIA È OBBLIGATORIA?

- **in caso di valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche**
- **nei trattamenti, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e a reati**
- **il caso di sorveglianza sistematica su larga scala di una zona accessibile al pubblico**

Attesa la redazione, da parte dell'Autorità Garante, di un elenco delle tipologie di trattamenti soggetti al requisito del Privacy Impact Assessment e di un elenco delle tipologie di trattamenti per le quali non è richiesta

Privacy Impact Assessment

CASISTICHE CHE PRESENTANO UN RISCHIO ELEVATO

- **uso di nuove tecnologie**
- **valutazione sistematica e globale di aspetti personali basata su un trattamento automatizzato**
- **profilazione**
- **trattamento su larga scala di particolari categorie di dati**
- **trattamento su larga scala di dati giudiziari**
- **confronto, combinazione di dati**
- **dati riferiti a soggetti vulnerabili**
- **trasferimento di dati all'estero**
- **trattamenti strutturalmente inconsapevoli**

Privacy Impact Assessment

Esempi di trattamento	Criteri pertinenti	PIA
▪ Ospedale che tratta dati genetici e sanitari relativi ai pazienti (sistema informativo ospedaliero)	▪ Dati sensibili o dati di natura estremamente personale ▪ Dati relativi a interessati vulnerabili ▪ Dati trattati su larga scala	▪ SI
▪ Utilizzo di un sistema di videosorveglianza per il controllo del traffico autostradale. Il Titolare prevede di utilizzare un sistema intelligente di analisi delle immagini per l'individuazione dei veicoli e il riconoscimento automatico delle targhe	▪ Monitoraggio sistematico ▪ Utilizzi innovativi o applicazione di soluzioni tecnologiche o organizzative	▪ SI
▪ Azienda che controlla sistematicamente le attività dei dipendenti, compreso l'utilizzo dei terminali informatici, la navigazione su Internet, ecc	▪ Monitoraggio sistematico ▪ Dati relativi a interessati vulnerabili	▪ SI
▪ Un'istituzione che crei un database nazionale di valutazioni creditizie o per finalità antifrode	▪ Valutazione o scoring ▪ Decisioni automatizzate che producono effetti giuridici o incidono in modo analogo sull'interessato in misura significativa ▪ Impedimenti all'esercizio di un diritto o all'utilizzo di un servizio o di un contratto da parte dell'interessato ▪ Dati sensibili o dati di natura estremamente personale	▪ SI
▪ Trattamento di "dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato"	▪ Dati sensibili o dati di natura estremamente personale ▪ Dati relativi a interessati vulnerabili	▪ NO

Privacy Impact Assessment

CONTENUTO MINIMO DELLA PIA

- **Una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal Titolare del trattamento**
- **Una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità**
- **Una valutazione dei rischi per i diritti e le libertà degli interessati**
- **misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione**

Se del caso, il Titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti

Se necessario, il Titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento

Se dalla PIA emerge che il rischio per la protezione dei dati personali non potesse essere ragionevolmente attenuato mediante l'uso delle tecnologie disponibili e per gli elevati costi di attuazione, il Titolare del trattamento deve procedere a consultare l'Autorità Garante prima di iniziare le attività di trattamento

DPIA secondo il WP 29

Il WP 29 ha rilasciato il documento:

Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679

Adottate il 4 aprile 2017

Versione successivamente emendata e adottata il 4 ottobre 2017

DPIA secondo il WP 29

La DPIA è uno strumento importante in termini di responsabilizzazione (accountability) in quanto aiuta il titolare non soltanto a rispettare le prescrizioni del GDPR, ma anche a dimostrare l'adozione di misure idonee a garantire il rispetto di tali prescrizioni.

In altri termini, la DPIA è una procedura che permette di realizzare e dimostrare la conformità con le norme.

DPIA secondo il WP 29

Coerentemente con l'approccio basato sul rischio che informa l'intero GDPR, lo svolgimento di una DPIA non è obbligatorio per ogni singolo trattamento.

La DPIA è necessaria solo se il trattamento "può comportare un rischio elevato per i diritti e le libertà delle persone fisiche"

(art. 35, paragrafo 1).

DPIA

La valutazione contiene almeno:

- **una descrizione sistematica** dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
- **una valutazione della necessità e proporzionalità** dei trattamenti in relazione alle finalità;
- **una valutazione dei rischi per i diritti e le libertà** degli interessati di cui al paragrafo 1; e
- **le misure previste per affrontare i rischi**, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Data Breach

Definizione di 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 personali trasmessi, conservati o comunque trattati**

In caso di Data Breach, il Titolare del trattamento notifica la violazione all'Autorità Garante senza ingiustificato ritardo e, ove possibile, 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 delle persone fisiche. Qualora la notifica all'Autorità Garante non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

L'eventuale Responsabile del trattamento informa il Titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione

CONTENUTO DELLA NOTIFICA ALL'AUTORITÀ GARANTE

- **descrizione della natura violazione occorsa e categorie e numero interessati coinvolti**
- **dati di contatto del DPO, se nominato, o di un altro punto di contatto cui rivolgersi per avere più informazioni**
- **descrizione possibili conseguenze**
- **descrizione delle contromisure adottate/che si intende adottare**

Il Titolare del trattamento deve tenere un registro delle violazioni occorse e non oggetto di notifica in cui siano documentate le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

Data Breach

Nel caso di Data Breach che presentino rischi elevati per i diritti e le libertà delle persone fisiche, il Titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo indicando con un linguaggio semplice e chiaro la natura della violazione dei dati personali.

CONTENUTO MINIMO DELLA COMUNICAZIONE AGLI INTERESSATI

- descrizione della natura violazione occorsa e categorie e numero interessati coinvolti
- dati di contatto cui rivolgersi per avere più informazioni
- descrizione possibili conseguenze
- descrizione delle contromisure adottate/che si intende

NON È RICHIESTA LA COMUNICAZIONE ALL'INTERESSATO SE

- il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura
- il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati
- detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia

Data Protection Officer

Il Data Protection Officer è una nuova figura (almeno in Italia) prevista dal Regolamento all'interno del c.d. Organigramma Privacy.

Il Titolare del trattamento e il Responsabile del trattamento devono designare un Data Protection Officer quando:

- **il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali**
- **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, di categorie particolari di dati personali o di dati relativi a condanne penali e a reati**

Il Data Protection Officer è designato in funzione delle qualità professionali, in particolare deve possedere conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati e la capacità di assolvere i compiti attribuiti al ruolo.

Il Data Protection Officer può essere un dipendente del Titolare del trattamento o del Responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.

Il Titolare del trattamento o il Responsabile del trattamento pubblica i dati di contatto del Data Protection Officer e li comunica all'Autorità Garante.

Art. 4 S.L. - Impianti audiovisivi e altri strumenti di controllo (nuovo testo riformato dal Jobs Act)

1. **Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo gli impianti e gli strumenti di cui al periodo precedente possono essere installati previa autorizzazione della Direzione territoriale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più Direzioni territoriali del lavoro, del Ministero del lavoro e delle politiche sociali.**

2. **La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.**

3. **Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196.4 S.L.**

Installazione di impianti audiovisivi

Sindacale	Amministrativa
Accordo aziendale stipulato con RSU o RSA ovvero con le OOSS più rappresentative sul piano nazionale da parte se si tratta di unità ubicate in diverse province o diverse regioni	Autorizzazione dell'Ispettorato Territoriale del Lavoro o dell'Ispettorato Nazionale se si tratta di unità ubicate nel territorio di competenza di più DTL

L'accordo sindacale o l'autorizzazione amministrativa devono intervenire PRIMA dell'installazione (nota Min. Lav. n. 11241 del 1.6.2016)

Controlli con altri strumenti tecnologici di lavoro o di registrazione degli accessi e delle presenze

Non è richiesta la preventiva procedura di concertazione con i sindacati ma al lavoratore va fornita adeguata informazione circa le modalità d'uso degli strumenti e l'effettuazione dei controlli (pena l'inutilizzabilità dei dati raccolti).

Sentenza Cassazione n. 10955/2015

Legittimo il controllo occulto attuato mediante la creazione di un falso profilo femminile da parte del Responsabile del Personale che, intrecciata un'amicizia virtuale con il dipendente, lo coinvolgeva in lunghe chat in orario di lavoro, per poi licenziarlo.

App per rilevazione presenze (provvedimento del Garante n. 350 del 8.9.2016)

Possibile installare una app sullo smartphone privato dei lavoratori per registrarne le presenze in servizio.

Requisiti:

a. **I dati dell'app non possono essere usati a fini diversi dalla rilevazione della presenza (no a fini disciplinari)**
b. **va effettuata la notifica preventiva al Garante**
c. **I lavoratori devono essere idoneamente informati sul funzionamento dell'app e le sue finalità**
d. **L'app non puo' avere accesso agli altri dati sul telefono, deve essere accesa/spenta dal lavoratore, deve segnalare quanto è attiva**
e. **i dati di geolocalizzazione dei lavoratori possono essere trattati ma devono essere subito cancellati. i dati di localizzazione della sede di lavoro e di timbratura (data e orario) possono essere conervati in linea con l'obbligo di tenuta del LUL (5 anni);**

Mail (provv. Garante Privacy italiano n. 456 del 30.7.2015)

Possibile controllare la posta elettronica aziendale del lavoratore se si è indicato preventivamente e chiaramente le modalità d'uso corrette e i controlli effettuati

Diversamente il lavoratore ha una legittima aspettativa di confidenzialità della corrispondenza

E' opportuno che l'azienda:

- **renda disponibili anche indirizzi condivisi tra più lavoratori (es. contabilità@ente.it)**
- **inserisca avvisi automatici inerenti la natura aziendale delle comunicazioni**
- **preveda, in caso di assenza del lavoratore, messaggi di risposta automatica con le coordinate di altri lavoratori cui rivolgersi**
- **preveda la delega a verificare il contenuto dei messaggi in caso di assenza prolungata o imprevista e/o di improrogabili necessità aziendali**

Cessazione del rapporto di lavoro

In caso di mail aziendale contraddistinta dal nome del lavoratore, il datore deve:

- **disattivare e rimuovere l'account dell'ex dipendente**
- **adottare sistemi automatici volti a informare i terzi e fornire indirizzi alternativi ove proseguire le comunicazioni con l'azienda**

Social network

Trattamento dei dati dei candidati:

Ammesso quando il profilo è utilizzato dal candidato per finalità lavorative e/o lo stesso è necessario e rilevante per l'esecuzione della prestazione lavorativa cui la domanda del candidato è rivolta.

Trattamento dei dati dei dipendenti/collaboratori:

Ammesso quando effettivamente occorre per verificare il corretto adempimento delle obbligazioni derivanti dal rapporto di lavoro in corso (es.: per il WP29 il datore di lavoro può avere un legittimo interesse a monitorare il profilo Linkedin dell'ex dipendente con patto di non concorrenza per verificarne il rispetto)

Norme disciplinari in tema di Social Network

L'accesso a social network in orario di servizio è consentito solo se previamente previsto, autorizzato e regolamentato per eventuali attività di customer care e customer satisfaction.

I dipendenti che accedono a social network durante l'orario e sul posto di lavoro danneggiano la prestazione contrattualmente dovuta poiché sottraggono tempo all'attività lavorativa e possono altresì provocare problemi di sicurezza al sistema.

In ogni caso – anche fuori dall'ambiente e/o orario di servizio - i lavoratori devono astenersi dal pubblicare su social network notizie, commenti e/o immagini che per il loro contenuto possono ledere l'immagine e reputazione aziendale ovvero dei colleghi e/o superiori e/o clienti dell'Azienda. A tale proposito si rileva che l'uso di espressioni denigratorie e lesive della reputazione del datore di lavoro e/o colleghi e/o clienti dell'Azienda su social network integra gli estremi della diffamazione in ragione del contesto pubblico, della conoscenza da parte di più persone e della possibile incontrollata diffusione tra i partecipanti alla rete del social network.

SIM aziendali

Garante Privacy provv. n. 3 del 11.1.2018

Ammissibile l'analisi dei consumi telefonici dei dipendenti in possesso di SIM aziendale,:

- **limitatamente al specifiche voci di spesa a carico della società in funzione della tipologia di tariffazione prescelta;**
- **tempi di conservazione dei dati limitati ad un massimo di 6 mesi,**
- **il datore di lavoro deve informare adeguatamente i dipendenti e adottare un disciplinare interno per regolamentare le condizioni di uso delle SIM**
- **a fronte di consumi anomali la società invita il dipendente, tramite suo superiore, a limitare i costi, esclusa l'adozione di misure disciplinari**
- **In caso di addebito al lavoratori di telefonate non aziendali i numeri di telefono chiamati non devono essere raccolti e deve essere predisposto un sistema di addebito a tariffazione**
- **i dati di fatturazione per effettuare le analisi devono essere resi anonimi e non consentire l'identificazione del lavoratore**

GRAZIE PER LA VOSTRA ATTENZIONE

Avv. Matteo Pagani