NUOVA NORMATIVA PRIVACY ED IMPATTO SULLE HR

Luisa Parisi
luisa.parisi@ztlex.com

ZAMBELLI TASSETTO
STUDIO LEGALE

Mogliano Veneto, 28 Maggio 2018

"PROTEZIONE DELLE **PERSONE FISICHE** CON RIGUARDO AL **TRATTAMENTO DEI DATI PERSONALI**, NONCHE' ALLA **LIBERA CIRCOLAZIONE DEI DATI**"

- Denominato "**GDPR**" (General Data Protection Regulation);
- pubblicato nella Gazzetta Ufficiale dell'Unione Europea il 04/5/2016;
- è in vigore dal **25/5/18** in Italia come negli altri Stati membri**;**
- immediatamente esecutivo (non necessita di una normativa di recepimento);
- abrogazione della direttiva "madre" (95/46/CE) dal 25/5/18 e prevalenza sul D.Lgs. n. 196/2003 (vecchio Codice) per le parti incompatibili;
- tutela la **SICUREZZA** dei dati personali.

REGOLAMENTI: NOZIONE

- nella gerarchia delle fonti del diritto dell'Unione europea, i regolamenti sono **fonti del diritto derivato** (fondate sui Trattati istitutivi delle Comunità europee e dell'Unione Europea che sono **fonti primarie**);
- atti a **portata generale,** con **efficacia erga omnes;**
- **obbligator**i in tutti i loro elementi per le stesse Istituzioni, per gli Stati membri e per i cittadini;
- **direttamente applicabili** in ciascuno degli Stati membri, senza necessità di una norma interna di recepimento;
- le norme incompatibili del diritto interno non potranno essere utilizzate, mentre quelle compatibili lo potranno.

PERCHE' UN NUOVO REGOLAMENTO?

- evoluzione tecnologica ---> diffusione dati della persona;
- "*governo della rivoluzione digitale*" al fine di proteggere i dati dei cittadini europei, ossia per la protezione dell'umanità, che è diritto fondamentale (così Antonello Soro, Presidente Autorità Garante Protezione Dati, Convegno di Bologna del 24.5.18)
- "*la protezione delle **persone fisiche** con riguardo al trattamento dei dati di carattere personale è un **diritto fondamentale***" (cons. 1): ossia ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano [così è statuito all'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea ("Carta") ed all'articolo 16, paragrafo 1, del Trattato sul funzionamento dell'Unione europea ("TFUE")]
- eliminazione frammentazione applicativa della normativa in materia di protezione dei dati personali;

COSA CAMBIA A GRANDI LINEE

- passaggio da un approccio formalistico ad uno sostanzialistico;
- atteggiamento proattivo;
- principio di accountability intesa anche come capacità di dimostrare di aver adottato ogni misura utile per tutelare i dati della persona;
- passaggio dalle misure minime a misure adeguate;
- minimizzazione dei dati (necessità e proporzionalità);
- pseudonimizzazione;
- massima trasparenza, chiarezza, intellegibilità (vedasi consenso);
- riconoscimento di nuovi diritti (oblio e portabilità).

AMBITO DI APPLICAZIONE

- **AMBITO SOGGETTIVO DI APPLICAZIONE:** si applica a qualsiasi soggetto, pubblico o privato, che tratti dati personali riguardanti una persona fisica

- **AMBITO TERRITORIALE DI APPLICAZIONE:** in relazione a dati personali di **persone fisiche che si trovano nell'Unione Europea**, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione Europea (NB: le norme attuali, invece, richiedono lo stabilimento nell'UE del titolare del trattamento)

PRINCIPALI DEFINIZIONI

- **DATO PERSONALE**: **qualsiasi informazione** riguardante una persona fisica identificata o identificabile

  NB: si considera identificabile una persona fisica quando possa essere individuata mediante un numero identificativo, dati relativi all'ubicazione, identificativo on line o mediante uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale e sociale (C26, C27, C30)

- **TRATTAMENTO:** qualsiasi operazione o insieme di operazioni applicate a dati personali o insiemi di dati personali (per esempio: raccolta, registrazione, organizzazione, conservazione, comunicazione mediante trasmissione, diffusione, ma anche cancellazione e distruzione)

(cont.)

- **VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)**: violazione della SICUREZZA che comporta ACCIDENTALMENTE o IN MODO ILLECITO la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso a dati personali trasmessi, conservati o comunque trattati (va comunicata **entro 72 ore** all'Autorità di controllo);
- **TITOLARE DEL TRATTAMENTO:** è la persona fisica o giuridica, l'autorità pubblica o altro organismo che DETERMINA----> *i)* FINALITA' E *ii)* I MEZZI del trattamento ed è in grado di comprovare il rispetto del GDPR;
- **RESPONSABILE DEL TRATTAMENTO:** la persona fisica o giuridica, l'autorità pubblica o altro organismo che TRATTA i dati PER CONTO del titolare del trattamento
- **RESPONSABILE DELLA PROTEZIONE DATI (RPD o DPO, "Data Protection Officer"):** figura professionale con particolari competenze in campo informatico, giuridico, di valutazione del rischio ed analisi dei processi

CATEGORIE PARTICOLARI DI DATI PERSONALI (DATI SENSIBILI):

- dati relativi alla salute (o vita o orientamento sessuale)
- dati giudiziari
- dati che rivelino l'originale razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale
- dati genetici
- dati biometrici (relativi alle caratteristiche fisiche, fisiologiche o comportamentali) che consentono di identificare in modo univoco una persona fisica.

TRATTAMENTO DELLE CATEGORIE PARTICOLARI DI DATI PERSONALI:

- **divieto del trattamento** (art. 9), salvi i casi eccezionali di cui al comma 2 dell'art. 9 ossia:
- a) quando l'interessato ha prestato il **consenso**;
- b) quando il trattamento è necessario per assolvere agli **obblighi** ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di lavoro, sicurezza e protezione sociale;
- c) per tutelare un **interesse vitale** dell'interessato o di altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- d) **se il trattamento è effettuato da una fondazione, associazione o altro organismo senza scopo di lucro che persegue finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi membri, ex membri o persone che hanno regolari contatti con l'ente e che i dati non siano comunicati all'esterno senza consenso dell'interessato;**
- e) se concerne dati manifestamente pubblici;
- f) se occorra per accertare, esercitare o difendere un **diritto in sede giudiziaria** o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
- g) trattamento necessario per **motivi di interesse pubblico**, purchè proporzionato;
- h) se necessario per finalità di **medicina preventiva o del lavoro**;
- i) motivi di interesse pubblico nel settore sanità (es. gravi minacce per la salute o garanzia di elevativi parametri di qualità e sicurezza dell'assistenza sanitaria e dei medicinali);
- j) necessario per archiviazione nel pubblico interesse, ricerca scientifica o storica o a fini statistici.
- Gli Stati membri possono mantenere o introdurre ulteriori condizioni o limitazioni riguardo ai dati genetici, biometrici o relativi alla salute.

TITOLARE DEL TRATTAMENTO

- è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o assieme ad altri, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche:
- determina **finalità** e **mezzi** del trattamento dei dati personali;
- **adotta misure tecniche ed organizzative** per garantire il rispetto del regolamento;
- è **in grado di comprovare** che il trattamento è stato effettuato nel rispetto del regolamento.
- **Contitolare del trattamento** (art. 26): accordo interno che delinei gli spazi di competenza e le rispettive responsabilità del titolare e contitolare in merito all'osservanza degli obblighi derivanti dal regolamento

RESPONSABILE DEL TRATTAMENTO (art. 28)

- è la persona fisica o giuridica, l'autorità pubblica o altro organismo che TRATTA i dati PER CONTO del titolare del trattamento e su istruzioni dello stesso (es.: società in outsourcing; consulenti del lavoro, commercialisti, fornitori di servizi telematici, conservatori di documenti informatici).
- Possibilità di nomina di uno o più sub-responsabili purché a ciò autorizzato per iscritto dal titolare del trattamento (c.d. avvalimento a catena). In caso di inadempimento del sub-responsabile, risponde il responsabile.
- NB: obbligatorio il **contratto scritto** o atto giuridico tra titolare e responsabile del trattamento che includa: materia e durata del trattamento; natura e finalità del trattamento; tipo di dati personali; categorie di persone interessate; diritti ed obblighi del responsabile del trattamento; misure di sicurezza; definizione obblighi (correlati ad esempio all'esercizio dei diritti degli interessati; riservatezza dati; assistenza, cancellazione dati alla fine del trattamento)

RESPONSABILE PROTEZIONE DATI (RPD o DPO – artt. 37, 38, 39):

- • obbligatorio per:
- □ amministrazioni ed enti pubblici;
- □ tutti i soggetti la cui attività principale consista in trattamenti che, per loro natura, oggetto e finalità richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
- □ tutti i soggetti la cui attività principale consiste nel trattamento, su larga scala, di dati sensibili, relativi alla salute o vita sessuale, genetici, giudiziari, biometrici.
- A titolo esemplificativo, è tenuto alla nomina chi esercita forme di tracciamento e pubblicità comportamentale; servizi di telecomunicazioni; utilizzo di telecamere a circuito chiuso; tracciamento dell'ubicazione da parte di app per dispositivi mobili; reindirizzamento posta elettronica; clientela di compagnia assicurativa; utenti di servizio di trasporto pubblico, fornitori di servizi telefoni e telematici; utenti di servizio di trasporto pubblico, fornitori di servizi telefoni e telematici.

RPD o DPO

- professionista o società di consulenza, interno o esterno all'ente/società, anche in team (ma soltanto un soggetto sarà il referente per l'Autorità/interessati);
- referente per il titolare del trattamento, l'Autorità di controllo (a cui va comunicato il nominativo) e gli interessati, che devono poterlo facilmente contattare;
- figura professionale eclettica che sorveglia l'osservanza del regolamento, ha conoscenze normative (privacy e sicurezza), informatiche e specifiche correlate al settore di riferimento (legale, sanitario, fiscale, commerciale etc);
- rapporto diretto col vertice gerarchico;
- autonomia ed assenza di conflitto di interessi (secondo le Linee Guida dell'Autorità si configura il conflitto di interesse in presenza di organi apicali di vertice quali amministratore delegato, responsabile operativo, responsabile delle risorse umane o sanitario o direttore marketing);
- possibile la designazione di un unico DPO per un gruppo di imprese o enti pubblici;
- formazione continua.

REGISTRI TRATTAMENTI (art. 30):

- parte integrante del sistema di corretta gestione dei dati;
- deve essere messo a disposizione dell'Autorità di controllo, se richiesto;
- obbligatorio solo per imprese o organizzazioni con più di 250 dipendenti oppure se vi possa essere un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento delle categorie particolari di dati (dati sensibili) o dati personali relativi a condanne penali e reati;
- sono 2 i registri: uno del titolare ed uno del responsabile;
- forma scritta, anche in formato elettronico;

(cont.)

- **registro titolare**: deve contenere nome e contatto del titolare e del contitolare, del rappresentante legale del titolare, nonché del responsabile protezione dati (RPD o DPO); finalità del trattamento; categorie interessati e categorie dati personali; categorie dati destinatari; ove applicabile, trasferimento dei dati verso un Paese terzo o un'organizzazione internazionale; descrizione generale misure di sicurezza;
- **registro responsabile**: deve contenere nome e contatto del o dei responsabili, del titolare per conto del quale agisce il responsabile, del rappresentante legale del titolare, del responsabile della protezione dati (RPD o DPO); categorie di trattamenti; ove applicabile trasferimento dei dati verso un Paese terzo o un'organizzazione internazionale; descrizione generale misure di sicurezza tecniche ed organizzative.

PRINCIPI POSTI ALLA BASE DEL TRATTAMENTO DI DATI PERSONALI (ART. 5):

- I dati devono essere:

- trattati secondo “liceità, correttezza e trasparenza”;
- raccolti per finalità determinate, esplicite e legittime;
- adeguati, pertinenti e limitati rispetto alle finalità;
- esatti ed aggiornati;
- limitati nella conservazione;
- trattati garantendo sicurezza ed integrità.

LICEITA' DEL TRATTAMENTO:

- in presenza del **consenso** al trattamento;
- quando 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;
- quando è necessario per adempiere ad un **obbligo legale** cui è soggetto il titolare del trattamento;
- quando è necessario per la salvaguardia **interessi vitali** dell'interessato;
- quando è in esecuzione di un compito di **interesse pubblico** o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
- per il perseguimento **legittimo interesse** del titolare del trattamento o di terzi a condizione che non prevalgano gli interessi o diritti e le libertà fondamentali degli interessati

CONSENSO:

- dimostrabile;
- chiaro;
- richiesto in forma comprensibile, facilmente accessibile, con linguaggio semplice e chiaro;
- revocabile.

INFORMATIVA PRIVACY

- forma concisa, trasparente, intellegibile, facilmente accessibile, con linguaggio semplice e chiaro;

  Deve contenere:
- identità e dati di contatto del titolare del trattamento;
- dati di contatto del responsabile dei dati, ove applicabile;
- finalità del trattamento;
- base giuridica (ossia indicazione delle ragioni di liceità, quali ad esempio: esecuzione del contratto, obbligo legale, consenso espresso etc);
- legittimo interesse (ove il trattamento si fondi su esso);
- destinatari o categorie di destinatari dei dati;
- diffusione dati all'estero o utilizzo di sistemi di profilazione (processo decisionale interamente automatizzato -> possibile ove ci sia il consenso);
- periodo di conservazione dei dati (o criteri per determinarlo);
- diritti dell'interessato (rettifica, cancellazione, limitazione del trattamento, portabilità, oblio, reclamo all'Autorità di controllo)

DIRITTO ALL'ACCESSO (ART. 15)

- L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati personali e dalle seguenti informazioni:

  - finalità del trattamento;
  - categorie di dati personali trattati;
  - destinatari dei dati;
  - periodo di conservazione dei dati personali previsto oppure, se non previsto, i criteri per determinarlo;

ULTERIORI DIRITTI (articoli da 16 a 23):

- riconoscimento del diritto dell'interessato a chiedere al titolare del trattamento:
  - la RETTIFICA dei dati personali ovvero
  - la CANCELLAZIONE dei dati personali ovvero
  - la LIMITAZIONE del trattamento dei dati personali che lo riguardano
  - la PORTABILITA' dei dati personali (ricezione in un formato strutturato, di uso comune e leggibile da dispositivo automatico dei dati personali forniti a un titolare di trattamento e diritto di trasmetterli ad altro titolare di trattamento)
  - di OPPORSI al loro trattamento

DIRITTO ALL' "ALL'OBLIO" - ART. 17

- L'interessato ha il diritto alla cancellazione dei propri dati personali senza ingiustificato ritardo ed il titolare del trattamento ha l'obbligo di cancellare prontamente se:
  - i dati personali **non sono più necessari** per le finalità per le quali sono stati raccolti;
  - in caso di **revoca del consenso o opposizione** dell'interessato e non sussiste alcun legittimo motivo prevalente per procedere al trattamento;
  - se i dati sono **trattati illecitamente**;
  - se è previsto un **obbligo legale** di cancellazione;
  - se i dati sono stati raccolti relativamente all'offerta di servizi ai minori.

- Il titolare, se ha reso pubblici i dati, è **obbligato a cancellarli**, tenendo conto della tecnologia disponibile e dei costi di attuazione.

(cont.)

- LE PREDETTE DISPOSIZIONI SUL DIRITTO ALLA CANCELLAZIONE DEI DATI NON SI APPLICANO SE IL TRATTAMENTO E' NECESSARIO:
  - per l'esercizio del diritto alla libertà di espressione e di informazione;
  - per l'adempimento di un obbligo legale correlato ad un interesse pubblico che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
  - per motivi di interesse pubblico nel settore della sanità;
  - a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici se il diritto all'oblio rende impossibile o pregiudica gravemente il conseguimento degli obiettivi;
  - per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

SANZIONI AMMINISTRATIVE (art. 83)

- **Effettive, proporzionate, persuasive, pari a:**

- Fino a **10 MILIONI DI EURO o**, in caso di impresa, FINO AL **2% DI FATTURATO** totale annuo mondiale dell'esercizio precedente

  Per esempio: in caso di mancata comunicazione dei data breach agli interessati (32), mancata designazione o violazioni correlate all'obbligo di designazione del Data Protection Officer – DPO (37), violazioni della sicurezza del trattamento (30), violazione degli obblighi incombenti sul titolare e responsabile del trattamento.

- Fino a **20 MILIONI DI EURO o**, in caso di un'impresa, FINO AL **4% DEL DI FATTURATO** totale annuo mondiale dell'esercizio precedente

  Per esempio: violazioni in materia di principi base del trattamento, condizioni per il consenso, diritti degli interessati, trasferimento di dati personali all'estero, mancata ottemperanza a un ordine o a una limitazione temporanea o definitiva disposti dall'autorità di vigilanza

- Le sanzioni **penali** potranno essere disposte dai singoli Stati membri.

Q&A

Domande?

Contatti

ZAMBELLI TASSETTO
STUDIO LEGALE

Avv. Luisa Parisi
Studio Legale Zambelli Tassetto
Via Cavallotti 22
30171 Venezia Mestre
luisa.parisi@ztlex.com
www.ztlex.com