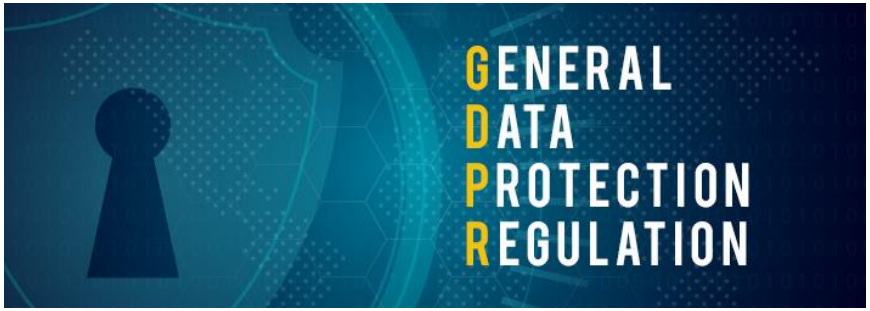
La protezione dei dati per dummies

Non per tecnici!

c.arlati

Indice

- Introduzione
- Che fare?
- I diritti
- Ruoli



Introduzione

Di cosa parliamo?

- Di un Regolamento del Parlamento e del Consiglio UE (2016/679) emanato il 27 aprile 2016 – in attuazione dal **25 maggio 2018**
- Si occupa :
  - Del trattamento dei dati
  - Della **protezione dei dati**
  - Della libera circolazione dei dati
  - Riguarda le persone fisiche

Di cosa parliamo?

- Il Regolamento UE è immediatamente applicativo e non dev'essere recepito da alcuna legge – livello minimo di protezione per i 520 milioni di cittadini europei
- Le nuove regole sono in sostanziale continuità con quanto già previsto dal d.lgs. 196/03 (cd «codice della privacy») – novità limitate ma significative
- Il Regolamento definisce prassi operative che dovrebbero già essere invalse nelle organizzazioni …

Principi generali

- Attenzione : la definizione di **trattamento** dei dati data dal regolamento è molto ampia – riguarda :
  - Raccolta (quindi anche la sola raccolta)
  - Conservazione
  - Operazioni di elaborazione

Principi generali

- Il regolamento prevede che i titolari del trattamento dei dati debbano rispettare i seguenti principi generali (art.5) :
  - Acquisizione dei dati per finalità specifiche (NON per scopi general generici)
  - Trattamento dei dati coerente con la finalità per la quale vengono raccolti (es. non si fa marketing con i dati raccolti per scopi sanitari, a meno che ciò non sia stato autorizzato dall'interessato …)
  - Esattezza dei dati trattati (dunque vanno aggiornati se non esatti)
  - Liceità, correttezza, trasparenza nei confronti della persona a cui i dati si riferiscono
  - Conservazione dei dati limitata nel tempo
  - **Integrità e riservatezza del dato (il Regolamento UE pone molta enfasi su questo principio : il titolare DEVE documentare ogni violazione dei dati personali e le azioni compiute per porvi rimedio –art.32)**

Principi generali

- Quindi : il Regolamento prevede che i titolari dei dati si diano un **sistema gestionale** per trattarli in coerenza con i principi enunciati!
- **Il proprietario dei dati non dev'essere MAI danneggiato dal trattamento degli stessi**
- **Anche se … la protezione dei dati non ne deve impedire la libera circolazione**

Un grande problema …

- Contemperare il trattamento corretto dei dati con il loro libero utilizzo non è semplice
- **Purtroppo è diffusa l'incapacità delle persone a gestire i propri dati (anche in conseguenza della diffusione dell'uso di internet e dei social)**
- Il considerando n.4 del Regolamento cerca di affrontare la questione affermando che : «*il trattamento dei dati personali dev'essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità*»

I diritti – Carta di Nizza

- Dunque la protezione dei dati va contemperata con gli altri diritti fondamentali del cittadino europeo, definiti dalla Carta di Nizza :
  - Diritto alla vita
  - Diritto all'integrità della persona
  - Diritto alla libertà
  - Diritto alla sicurezza
  - Diritto di sposarsi e costruire una famiglia
  - Libertà di pensiero, coscienza e religione
  - Libertà di espressione e informazione
  - Libertà di riunione e associazione
  - Diritto all'istruzione

I diritti – Carta di Nizza

- Diritto di lavorare
- Libertà professionale
- Diritto di proprietà
- Diritto di asilo
- Diritti del minore
- Diritti degli anziani
- Inserimento delle persone con disabilità
- Diritto dei lavoratori alla consultazione e all'informazione nell'ambito dell'impresa
- Diritto di negoziare e ad azioni collettive
- Diritto di accesso ai servizi di collocamento

I diritti – Carta di Nizza

- Tutela in caso di licenziamento ingiustificato
- Condizioni di lavoro giuste ed eque
- Conciliazione tra vita familiare e professionale
- Sicurezza sociale e assistenza sociale
- Protezione della salute
- Rispetto della vita privata e familiare
- Diritto di voto ed eleggibilità alle elezioni
- Diritto a una buona amministrazione
- Diritto di accesso ai documenti
- Diritto di petizione
- Diritto di libera circolazione e soggiorno nell'UE

I diritti – Carta di Nizza

- Diritto ad un ricorso effettivo ad un giudice imparziale
- Presunzione d'innocenza
- Diritto a difendersi se accusati
- Diritto a non essere giudicati o puniti due volte per lo stesso reato

Traduzione «pane e salame»

- Dunque …:
  - tutti i titolari del trattamento dei dati sono legittimati ad utilizzarli, purché lo facciano correttamente
  - sono i titolari del trattamento che devono dimostrare il senso (e la correttezza) di ciò che fanno con i dati altrui
  - i dati possono essere una merce pericolosa, meglio averne lo stretto indispensabile per fare ciò che si deve fare
  - coloro che trattano i dati debbono averne cura come se fossero i loro
  - se le finalità di trattamento sono lecite siamo sulla buona strada!

Che fare?

Dati personali

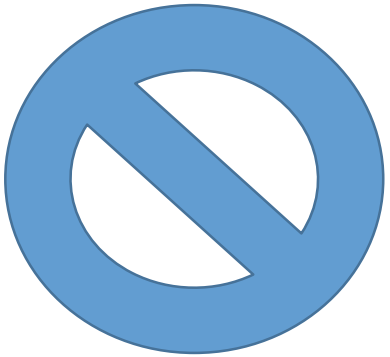
- Esistono diverse tipologie di dato:
  - ***dati personali*** – qualsiasi informazione riguardante una persona fisica identificata o identificabile (definizione molto estesa che riguarda, ad es., il codice fiscale, il codice IBAN, il numero di un documento, l'indirizzo IP assegnato a un dispositivo per la navigazione su internet) – **tutti i dati personali vanno PROTETTI**
  - **quelli che erano definiti «dati sensibili» dal d.lgs. 196/03 ora sono sostituiti tra tre diverse tipologie di dato … - queste categorie di dati necessitano di una PROTEZIONE PARTICOLARE (gli Stati membri possono stringere ulteriormente le maglie es. vietando i dati biometrici nella gestione del rapporto di lavoro)**

Dati sensibili

- ***dati genetici*** – relativi alle caratteristiche genetiche o acquisite di una persona – derivano dall'analisi di campioni biologici (es. sangue)
- ***dati biometrici –*** derivanti da un trattamento tecnico specifico finalizzato a raccogliere informazioni fisiche o comportamentali di una persona – scopo è il riconoscimento univoco della stessa – es. immagine facciale, impronta
- ***dati relativi alla salute*** – attinenti alla salute fisica o mentale di una persona es. cartella clinica

Dati non trattabili (con eccezioni) – art.9

- origine etnica
- idee politiche
- convinzioni religiose o filosofiche
- **appartenenza sindacale**
- genetici
- biometrici
- relativi alla salute
- relativi alla vita sessuale
- relativi all'orientamento sessuale della persona
- relativi a condanne penali o reati (gestiti unicamente sotto la responsabilità dell'autorità giudiziaria!) – **leggi specifiche** possono imporre che questi dati vengano trasmessi ad altri soggetti in situazioni particolari (es. codice degli appalti, contatto con i minori)



Eccezioni – trattamento dati sensibili

- ✓ consenso dell'interessato per una o più finalità specifiche – revocabile, se non disposto altrimenti da leggi dello Stato
- ✓ se resi manifestatamente pubblici dall'interessato
- ✓ per esercitare diritti specifici o obblighi associati al diritto del lavoro e della sicurezza sociale (anche derivanti da **contratti collettivi**!) – es. versamento contributi destinati alle organizzazioni sindacali
- ✓ se il trattamento è effettuato da un'associazione SENZA scopo di lucro per le sue legittime finalità – ciò vale anche per le **organizzazioni sindacali** a condizione che il trattamento riguardi i membri o gli ex membri – **questi dati NON vanno comunicati all'esterno senza il consenso degli interessati!**
- ✓ per esercitare il diritto di difesa nei tribunali

Eccezioni – trattamento dati sensibili

- ✓ per finalità di medicina preventiva e di **medicina del lavoro** – è possibile, quindi, continuare a trattare i dati relativi alla sorveglianza sanitaria dei lavoratori e delle lavoratrici ex d.lgs.81/08 smi – purché lo faccia il medico competente (come già oggi previsto)
- ✓ per motivi di sanità pubblica es. prevenzione epidemie, vaccinazioni
- ✓ per ricerca scientifica, storica, statistica (proteggendo i dati degli interessati)

Maneggio dati – regole generali – art.9

- Solo con il consenso dell'interessato
- Per uno scopo ben preciso (di cui l'interessato dev'essere a conoscenza)
- In esecuzione di un contratto
- Se obbligatorio per legge (es. l'azienda gestisce dati dei lavoratori per busta paga e sostituto d'imposta)
- Se «salva vita» (es. persona al pronto soccorso priva di conoscenza)
- In esecuzione di interesse pubblico (es. registri tenuti dalle p.a., ma anche centrale rischi bancaria)
- Per legittimi interessi del titolare del trattamento (non in contrasto con i diritti fondamentali dell'interessato)

Informativa all'interessato

- È lo **strumento gestionale** attraverso il quale si comunicano all'interessato le modalità di gestione e trattamento dei suoi dati, chiedendogli l'autorizzazione a farlo (art.13) – **chi tratta il dato DEVE dimostrare che è stato autorizzato a farlo!**
- Quali elementi deve contenere?
  - Identità dell'interessato (a cui i dati si riferiscono)
  - Identificazione titolare e del responsabile del trattamento dei dati – eventuali riferimenti al DPO (*Data Protection Officer*) (a quale mail è possibile contattare il responsabile della protezione dei dati?)
  - Finalità del trattamento (cosa farò di quei dati?) – informare il titolare se il dato sarà utilizzato per ulteriori finalità oltre a quella principale
  - Identificazione degli eventuali altri destinatari dei dati dell'interessato (es. in caso di un'agenzia per il lavoro i dati del disoccupato potranno essere forniti anche alle aziende interessate)
  - Impegno a non trasferire i dati al di fuori dell'UE (nel caso lo si faccia specificare le garanzie di riservatezza adottate)

Informativa all'interessato

- Periodo di conservazione dei dati personali (es. fino a vs richiesta di cancellazione)
- Specificazione del diritto dell'interessato a richiedere l'esercizio di alcuni diritti specifici (cancellazione, rettifica, accesso ai dati personali, limitazione del trattamento, portabilità …)
- Specificazione del diritto a revocare il consenso in qualsiasi momento (indicando le conseguenze del caso es. revoca dell'iscrizione al sindacato, rescissione di un contratto con pagamento di penali …)
- Specificare il diritto a ricorrere all'autorità di controllo (il Garante per la privacy – sarebbe «elegante» inserirne nell'informativa la email per un eventuale contatto)
- Se esiste un processo di decisione automatizzato (es. algoritmo) va precisato (es. nel caso dei *riders* la consegna delle pizze è assegnata da una piattaforma in base a procedimenti automatici) – se non esiste va specificato

Informativa all'interessato

- Se i dati sono stati raccolti attraverso quanto reso pubblico dai social o altre fonti di pubblico dominio va specificato

- **TUTTE queste informazioni vanno fornite all'interessato entro un mese dall'ottenimento dei dati personali** (salvo eccezioni es. l'interessato dispone già delle informazioni, in caso di ricerca scientifica)

I diritti

I diritti dell'interessato

- Quali **diritti** ha l'interessato, il proprietario dei dati?
  - *richiedere al titolare del trattamento del dato informazione sui suoi dati (che lo riguardano singolarmente)* : finalità del trattamento, dati in gestione, altri destinatari eventuali dei dati, periodo di conservazione, origine dei dati se non raccolti presso l'interessato
  - *tempi di risposta certi da parte del titolare del trattamento dei dati* (max 1 mese – oltre i 2 mesi possibile ricorso al Garante) – per richieste infondate, eccessive, ripetitive il titolare del trattamento del dato può chiedere all'interessato un contributo economico alle spese (purché «ragionevole») o rifiutare di soddisfare la richiesta (sconsigliato! l'onere della prova incombe su chi tratta il dato …)

I diritti dell'interessato

- *rettifica del dato* : l'interessato ha il diritto di ottenere l'integrazione dei dati incompleti, fornendo una dichiarazione integrativa
- *limitazione al trattamento* : diritto esercitabile in caso di dati errati, se il trattamento è illecito, se è in atto una controversia sull'uso dei dati, se i dati debbono comunque essere conservati per l'esercizio della difesa o di un diritto in sede giudiziaria – l'UE riconosce l'*opt in*, ovvero : l'interessato deve autorizzare preventivamente l'uso dei suoi dati (in USA vale l'*opt out* : se l'interessato non si oppone possono essere utilizzati)
- *non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato che produca effetti giuridici sulla sua persona* – es. il merito creditizio non può essere generato unicamente da un algoritmo

I diritti dell'interessato

- *portabilità :* l'interessato ha diritto di trasferire ogni informazione si generi all'interno di un rapporto contrattuale o di servizio es. passare ad altre società di servizi significa che quelle che ho utilizzato prima devono essere in grado di trasferire tutti i miei dati ai soggetti che ho scelto ora – necessaria inter-operabilità tra sistemi (non vale per la carta) – DIRITTO ONEROSO PER LE ORGANIZZAZIONI
- *oblio :* il titolare del trattamento dei dati deve cancellare senza ritardo i dati non più necessari rispetto alle finalità autorizzate dal titolare (es. dati di ex dipendenti di aziende o ex iscritti al sindacato), in caso di revoca del consenso, nel caso l'interessato si opponga ad uso dei dati per motivi di marketing non autorizzato, se i dati sono trattati illecitamente, per adempiere ad un obbligo legale (es. protezione dei minori) – PROBLEMA DELLA NATURA DI INTERNET (NON DIMENTICA)

I diritti dell'interessato

- *revoca* : l'interessato deve poter essere posto nelle condizioni di revocare il consenso con la stessa facilità con cui l'ha fornito – attenzione : il diritto di revoca ha a che fare con la genuinità del consenso al trattamento – per evitare problemi EVITARE DI RACCOGLIERE IL CONSENSO PER UNA PLURALITA' DI FINALITA' – finalizzare la raccolta ai dati strettamente necessari

Ruoli

Ruoli

- **Titolare del trattamento del dato :** decide come il dato viene trattato, con quali finalità e con quali misure di protezione – per le persone giuridiche è l'organizzazione in quanto tale, non il legale rappresentante – le richieste di risarcimento la riguardano direttamente – le organizzazioni possono rivalersi sui dipendenti responsabili di dolo o colpa grave nel trattamento del dato – i titolari possono far riferimento a standard gestionali tipo ISO/IEC 27001 e 27002 e codici di condotta per dimostrare il rispetto degli obblighi
- **Rappresentante/incaricato** : è chi rappresenta nell'UE un titolare del trattamento del dato con stabilimento al di fuori dell'UE, con esclusione di trattamenti occasionali e delle autorità pubbliche

Ruoli

- **Responsabile:** è persona fisica o giuridica che tratta dati personali per conto del titolare del trattamento – la figura viene notevolmente rinforzata dal Regolamento UE, in particolare :
  - deve esserci un contratto tra titolare e responsabile che deve prevedere determinati limiti per il responsabile : sui dati e le finalità di loro uso, sulla riservatezza, sull'adozione di misure di sicurezza, sulla gestione di eventuali violazioni dei dati, sui sub-responsabili (deve esisterne un elenco!), sull'obbligo di cancellare tutti i dati a sua disposizione al termine della prestazione, sull'obbligo di essere pro-attivo e segnalare al titolare le criticità
  - se il responsabile affida ad altre organizzazioni il trattamento di dati (es. selezione del personale, gestione biste paga, gestione sistemi informatici), deve informarne il titolare
  - deve dotarsi di procedure specifiche – registro violazioni, sicurezza informazioni previo valutazione rischi ex ISO 31000, registro delle attività di trattamento (per le aziende con più di 250 dipendenti o in caso di trattamenti con particolari rischi), **nomina DPO (non obbligatoria, se non in alcuni casi limitati e specifici, ma caldeggiata dal Garante)**

Ruoli

- **DPO (*data protection officer*) :** è l'oggetto misterioso del nuovo Regolamento – alcune specificazioni su questo ruolo :
  - è un «professionista», il cui profilo non è chiaro (quale formazione? per ora non vi sono obblighi in questo senso …) – deve comunque conoscere l'attività aziendale, i sistemi informativi, la loro sicurezza
  - deve comunque essere esente da conflitti d'interesse ed essere indipendente (NON può avere funzioni operative nell'organizzazione che tratta i dati) – può essere un consulente esterno
  - deve essere vincolato alla riservatezza
  - non è il responsabile in caso di inosservanza del regolamento – è il titolare del dato che continua ad essere responsabile del corretto trattamento dei dati! – dev'essere coinvolto in tutte le attività di trattamento dei dati (art.38)
  - deve essere dotato delle risorse economiche e logistiche necessarie

DPO compiti (art.39)

Consulenza al responsabile del trattamento	**Informa i dipendenti dell'organizzazione sul trattamento dei loro dati (es. videosorveglianza)**	Formatore
Verifica rispetto regolamento	Segnalare anomalie e non conformità al responsabile del trattamento	Fornire un pare sulla valutazione d'impatto (se richiesto)
	Fungere da punto di contatto con l'autorità garante	

Ruoli

- **Il DPO NON è obbligatorio se non in determinate fattispecie – è possibile nominare un unico DPO per gruppo imprenditoriale**
- **Il DPO, se presente, va pubblicizzato sui siti delle organizzazioni – art.37 (chi è? e-mail? telefono? i dipendenti sono a conoscenza di chi sia?)**
- Obbligo presenza DPO :
  - Per autorità pubbliche e aziende che offrono servizi pubblici
  - Per attività che richiedono raccolta dati o monitoraggio degli stessi su larga scala (es. banche, assicurazioni, compagnie telefoniche)
  - Per le attività che trattino dati sensibili e dati di cui all'art.9 c.1 (tra cui i dati sindacali e sanitari)

Come procedere?

1. **Valutazione documentata dei rischi a cui potrebbe essere soggetto il trattamento dei dati personali in quella specifica organizzazione**
2. **Previsione piano di prevenzione delle violazioni** es. identificativi univoci assegnati ai dipendenti, nuovo sistema di controllo degli accessi alla sede e alla rete aziendali, uso di tecnologie di cifratura e identificazione del personale, anonimizzazione del dato, minimizzazione del dato (quali dati realmente necessari?)
3. **Protezione del dato** es. resilienza dei sistemi (es. *back up* dei dati frequente, piano di gestione delle emergenze), capacità di ripristino dei dati in tempi limitati in caso di incidenti, procedure di *testing*
4. **Emersione dei *data breach* :** gli attacchi di pirati informatici o le azioni maldestre NON vanno nascoste in caso di perdita, modifica, divulgazione non autorizzata del dato – le violazioni vanno documentate e portate a conoscenza del Garante!

Come procedere?

5. **Tenere i registri delle attività di trattamento :**
   - Obbligatorio in ogni caso per le organizzazioni con più di 250 dipendenti,
   - Per quelle con meno addetti, ma che trattino dati che possano presentare rischi per la libertà dell'interessato – DIFFICILE DA STABILIRE
   - Per le organizzazioni che trattino dati sensibili e i dati per i quali vi sono limitazioni al trattamento (art.9c.1), tra i quali : iscrizioni al sindacato
6. **Valutare l'impatto sulla protezione dei dati dei trattamenti previsti (in riferimento all'uso delle tecnologie telematiche)** :riguarda i dati «a rischio elevato» per la libertà del titolare (difficile da stabilire) - sicuramente ricompresi i dati sensibili , quelli ex art.9c.1 del Regolamento (es. dati iscrizioni sindacali), quelli relativi alla videosorveglianza – cosa comporta la valutazione? Il titolare del trattamento deve farsi alcune domande …

Le domande della valutazione d'impatto

- Sono in grado di descrivere sistematicamente i trattamenti previsti e le finalità degli stessi?
- Sono in grado di giustificare la necessità e la proporzionalità del trattamento dei dati in relazione alle finalità che mi propongo?
- I dati che tratto mettono in pericolo la libertà e la sicurezza degli interessati?
- Sto conservando i dati nel rispetto dei principi della riservatezza, integrità e disponibilità (all'interessato)?
- Le misure di sicurezza che ho messo in campo per proteggere i dati sono adeguate?
- Sono in grado di gestire un'emergenza/minaccia? Ho un piano?

(se del caso la valutazione d'impatto può essere svolta sentendo gli interessati o loro associazioni e nel rispetto di specifici codici di condotta)

I Registri (cenni)

- I registri sono mantenuti sotto la responsabilità del titolare del trattamento – costituiscono la documentazione di ciò che è stato fatto
- Necessari due registri distinti : per il titolare e per il responsabile – da tenere per iscritto e in forma elettronica – su richiesta disponibili alle autorità di controllo
- Nei registri sono inseriti:
  - i dati del titolare del trattamento
  - i dati del responsabile della protezione dei dati ove previsto
  - le finalità del trattamento dei dati
  - descrizione delle categorie degli interessati i cui dati sono raccolti
  - descrizione delle tipologie di dati trattati
  - descrizione dei riferimenti dei soggetti terzi a cui i dati verranno messi a disposizione (es. per un'agenzia per il lavoro sono le aziende)
  - i termini per la cancellazione dei dati (ove possibile) (ad es. i dati dei dipendenti si conservano per tutta la durata del rapporto di lavoro, i dati relativi alla videosorveglianza dei dipendenti si conserveranno per …)
  - descrizione delle misure di sicurezza attuate per proteggere i dati (vedi)

Traduzione «pane e salame»

- Le informative date all'interessato debbono essere complete ed esaurienti
- I diritti all'oblio e alla portabilità richiedono sistemi informatici adeguati
- Individuare chiaramente il responsabile del trattamento dei dati tra i partner e i fornitori per fare chiarezza
- Fare la valutazione dei rischi e assumere le decisioni conseguenti!
- Registrare gli incidenti, non rimuoverli!
- Formare i dipendenti alla tutela del dato è fondamentale!
- Il DPO non è qualcuno su cui scaricare la responsabilità, ma una risorsa per applicare le norme

(a cura di C.Arlati)