

*“Contesto di riferimento e glossario in materia di
protezione dati”*

Sommario

1 CONTESTO DI RIFERIMENTO	2
2 GLOSSARIO	3

1 Contesto di riferimento

La presente introduzione è necessaria al fine di inquadrare sotto un profilo contestuale il Regolamento Europeo n. 679/2016 (General Data Protection Regulation meglio noto come GDPR), entrato in vigore il 24 maggio 2016 ma pienamente applicabile a partire dal 25 maggio 2018, che andrà ad uniformare ed armonizzare le legislazioni dei Paesi Europei con riguardo alla materia di protezione dei dati personali. L'esigenza di una rivisitazione della normativa in materia di protezione dei dati personali si apprezza in relazione al mutato contesto politico, economico e sociale di riferimento del tutto differente rispetto a quello degli anni 90, periodo nel quale l'impatto e la cultura del dato non era così centrale come invece è oggi; ciò è dato dallo sviluppo repentino delle moderne tecnologie (*in primis* mobile devices, smartphone, tablet, social network, ecc.; in seconda battuta strumenti IOT (Internet of things), sistemi di Data Analytics e Big Data, Business Intelligence, ecc.) nemmeno immaginabile negli anni che chiudevano il secolo scorso, grazie alle quali è pensabile e apprezzabile anche il valore economico del dato.

Accanto a questa constatazione di tipo "sociologica" va da sé che il programma di integrazione europeo che vede come base di partenza la creazione di un mercato unico europeo, da realizzarsi inizialmente attraverso la libera circolazione di persone, servizi e merci, non possa non tenere in considerazione anche della libera circolazione del "dato personale" così come puntualmente sottolineato dai "considerando" del Regolamento fino anche alla maggiore rilevanza di questa libertà rispetto alla tutela del dato in sé come diritto soggettivo (considerando nr. 4).

A seguito di questa breve introduzione storica/sociologica ed avviando la riflessione sul terreno giuridico, in prima battuta preme precisare che la scelta di tipologia di intervento del legislatore Europeo risulta alquanto significativa nella misura in cui, con la scelta di un Regolamento, non viene lasciata agli Stati membri alcuna possibilità di intervento (se non in termini di adozione di provvedimenti volti ad armonizzare la normativa nazionale) stante la piena applicabilità del Regolamento a dispetto della presenza, come successo invece in passato in materia di protezione di dati personali, di direttiva europea (95/46) che necessitava di un atto di recepimento (Dlgs. 196/2003, meglio noto come codice della privacy). In riferimento invece ai contenuti della presente legge si sottolinea come l'approccio che propone il Regolamento sia del tutto differente rispetto a quello proposto dal codice privacy nazionale.

Principio fondamentale che impregna l'intera normativa è infatti quello di **accountability** (la capacità di rendere conto delle azioni) il quale illustra, di fatto, una responsabilizzazione dei soggetti coinvolti in materia di protezione di dati personali; questi infatti secondo il dettato normativo non dovranno più ragionare in termini di mero adempimento alla norma di riferimento, come invece accaduto fino ad oggi con riferimento ai dettami del codice della privacy.

In tal senso il principio di accountability deve essere letto sotto un duplice profilo: esso non solo è il principio che ispira l'adeguamento/l'adempimento degli enti alla normativa europea, ma è anche il punto di partenza per **dimostrare** la compliance (il rispetto, l'aderenza) dell'ente/organizzazione alla norma europea. Ciò significa che un ente/organizzazione può disattendere una prescrizione del Regolamento, avendo tuttavia cura di indicare in apposito documento le ragioni in forza delle quali si ritiene di non dover seguire il dettato normativo.

Oltre quindi a lasciare uno spazio di intervento ai soggetti Titolari del trattamento in ordine alla scelta di adozione delle novità introdotte dal GDPR, obbligandoli comunque ad una seria riflessione in ordine alle politiche da adottare per essere conformi al Regolamento, si segnalano a titolo esemplificativo alcuni istituti del tutto lontani dalla logica "burocratica" del Codice Privacy.

Si richiama inevitabilmente quindi al processo di istituzione e conservazione del **registro di trattamenti** in capo ai titolari e responsabili del trattamento che consente quindi di avere una chiara panoramica dei trattamenti di dati personali che vengono effettuati all'interno dell'organizzazione che fa per l'appunto capo al titolare o al responsabile; a ciò si aggiunga l'organizzazione del processo che porta il titolare o responsabile del trattamento in contatto con l'autorità garante e con i soggetti interessati in caso di "violazione di dati" nota anche come **Data Breach**, che come sarà meglio trattato nell'apposito documento non si limita al solo furto di dati.

Ancora, la previsione di una conduzione di **Valutazione di impatto** per quei trattamenti che presentino un rischio elevato per i diritti e le libertà degli interessati. Sotto il profilo dei soggetti attivi e protagonisti, in questo nuovo quadro, viene introdotta la figura del **Data Protection Officer – DPO** (obbligatorio per tutti gli

enti pubblici) il quale si andrà a configurare da un lato come consulente per i Titolari e i Responsabili dei trattamenti, attraverso una continua verifica della *compliance* dell'organizzazione/ente rispetto ai dettami del GDPR, ma anche come punto di riferimento per i soggetti interessati rappresentando per questi ultimi il referente dell'organizzazione con il quale interfacciarsi in materia di protezione dei dati personali.

In conclusione, come già emerso dalla disamina condotta, a mutare è l'atteggiamento della normativa rispetto alla tematica della protezione dei dati personali, esso infatti impone una riflessione preventiva rispetto alla materia *de qua*, che porta quindi ad adattare la propria organizzazione in base alle opportunità che si intendono cogliere, lasciando non solo ampi spazi di autonomia ai soggetti Titolari/Responsabili ma anche abbandonando quell'approccio di mero adempimento richiesto dalla normativa.

In sintesi, non è sufficiente avere "le carte a posto".

2 GLOSSARIO

Definizioni normative di riferimento

Anonimizzazione: tecnica di trattamento dei dati personali tramite la quale i dati personali non possano più essere attribuiti a un interessato specifico, nemmeno attraverso l'utilizzo di informazioni aggiuntive.

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

Autorità di controllo: è l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51.

Cifratura: tecnica di trattamento dei dati personali tramite la quale i dati personali vengono resi non intellegibili a soggetti non autorizzati ad accedervi.

Consenso dell'interessato: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

Contitolare: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, insieme ad altri determina le finalità e i mezzi di trattamento dei dati personali;

Data Breach: è un incidente di sicurezza in cui i dati personali vengono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato o persi accidentalmente.

Dati biometrici: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

Dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

Destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

DPIA: acronimo di Data Protection Impact Assessment (valutazione di impatto sulla protezione dei dati).

Interessato: persona fisica identificata o identificabile. Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il

nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Limitazione di trattamento: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

Misure di sicurezza: misure tecniche ed organizzative adeguate per garantire un livello di sicurezza dei dati trattati adeguato al rischio.

Nuovo trattamento: trattamento di dati personali che comporta l'utilizzo di nuove tecnologie o è di nuovo tipo e in relazione al quale il titolare del trattamento non ha ancora effettuato una valutazione d'impatto sulla protezione dei dati, o la valutazione d'impatto sulla protezione dei dati si riveli necessaria alla luce del tempo trascorso dal trattamento iniziale.

Privacy by-design / by-default: l'incorporazione della privacy a partire dalla progettazione di un processo aziendale, con le relative applicazioni informatiche di supporto. La prima introduce la protezione dei dati fin dalla progettazione per caso specifico, la seconda per impostazione predefinita di una pluralità di casi tra loro omogenei.

Profilazione: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

Pseudonimizzazione: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

Rappresentante: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del regolamento;

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

Responsabile della Conservazione documentale: si tratta della figura preposta alla gestione e supervisione del processo di conservazione dei documenti (digitali o cartacei).

Security Manager: è la figura preposta alla gestione e supervisione del processo di Security Incident Management.

Sub responsabile: persona fisica o giuridica designata dal responsabile del trattamento previa autorizzazione scritta del titolare del trattamento;

Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il Titolare o suo delegato del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

Titolare del trattamento o suo delegato: 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;

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

Violazione dei dati personali: 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.