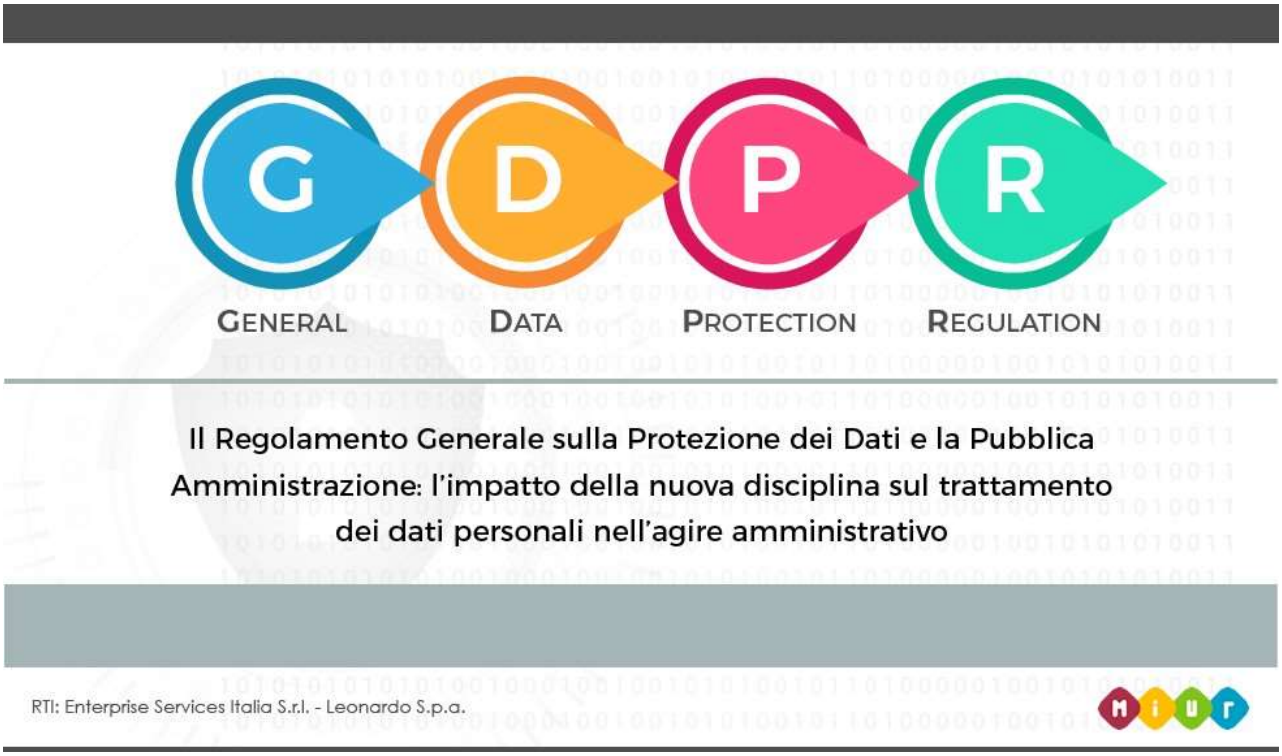
# STORYLINE DEL CORSO

## GDPR --- GENERAL DATA PROTECTION REGULATION

***Il Regolamento Generale sulla Protezione dei Dati e la Pubblica Amministrazione: l'impatto della nuova disciplina sul trattamento dei dati personali nell'agire amministrativo***




## Maggio 2018

# INDICE

# 1. LA DISCIPLINA INTRODOTTA DAL GDPR

## 1.1. DAL CODICE DEL 2003 AL REGOLAMENTO EUROPEO DEL 2016

Il Regolamento UE 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, in materia di protezione dei dati personali (GDPR), che acquista piena efficacia il 25 maggio del 2018, è un'evoluzione e non una rivoluzione, rispetto al Codice della Privacy italiano (D.Lgs. 196/2003), che conteneva già molti dei principi che sono ora ricompresi nella normativa europea. Il Regolamento reca, comunque, alcune rilevanti innovazioni in tema di trattamento di dati personali, e sarà applicabile in maniera generalizzata e immediata in tutta l'Unione europea, sostituendo la Direttiva 95/46/CE.

L'esigenza di una nuova disciplina sorge, soprattutto, da due ordini di ragioni. In primo luogo, come chiarito dal sesto "Considerando [1] ", la rapidità dell'evoluzione tecnologica e la globalizzazione hanno comportato nuove sfide per la protezione dei dati personali, anche perché la condivisione e la raccolta di dati personali è aumentata in modo esponenziale e la tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Il recente caso "Cambridge Analytica", su cui ha aperto un'indagine anche il Garante italiano, è forse la migliore dimostrazione della necessità di una protezione più incisiva e globale.

In secondo luogo, era necessario uno strumento che eliminasse la frammentazione e le diversità normative stratificatesi nei singoli Stati membri. La Direttiva 95/46/CE, infatti, era stata recepita (e applicata) in maniera non uniforme, e ciò ha comportato evidenti conseguenze sia in tema di libera circolazione dei dati personali, che di concretezza e omogeneità della tutela in ambito europeo. Si è pertanto optato per l'adozione di un Regolamento, direttamente applicabile in tutti gli Stati membri, "*al fine di assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione*" (come precisa il decimo Considerando).

Il GDPR, essendo un Regolamento, è direttamente applicabile in tutti gli Stati dell'Unione[2] (self executing), senza bisogno di essere implementato da un'apposita norma nazionale (come è accaduto invece per la direttiva 95/46), e ciò nonostante lascia dei "*margini di manovra*" ai singoli Stati. In particolare, il Legislatore nazionale potrà, con riguardo ai trattamenti di dati effettuati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (e dunque per i trattamenti effettuati da soggetti pubblici), mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione del GDPR.

In Italia, con l'art. 13 della cd. "Legge comunitaria" (L. 25 ottobre 2017, n. 163[3]) si è delegato il Governo a emanare uno o più decreti legislativi per l'adeguamento e l'armonizzazione della normativa nazionale al GDPR. Il Governo, in data 21 marzo 2018, ha approvato il testo preliminare

[1] I "Considerando" costituiscono il preambolo tipico dei testi, anche normativi, dell'Unione europea, e, pur non avendo valore giuridico vincolante, sono di particolare utilità nell'interpretazione e applicazione delle norme stesse.

[2] Ai sensi dell'art. 288, secondo comma, del Trattato sul Funzionamento dell'Unione europea, infatti, il regolamento ha portata generale ed è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

[3] www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2017-10-25;163!vig=.

del decreto legislativo, ma prima della sua approvazione definitiva esso dovrà ricevere i pareri delle commissioni parlamentari e del Garante della Privacy.

Oltre alla normativa primaria, dovranno necessariamente essere aggiornati (o sostituiti) i provvedimenti e le Linee guida del Garante Privacy, che rivestono un'importanza fondamentale in questa materia. Quest'operazione di revisione normativa riguarderà, ovviamente, anche i provvedimenti via via emanati (dal legislatore, dal Ministero e dal Garante) nell'ambito dell'attività del MIUR.

Questo corso costituisce dunque un'introduzione ai principi generali del GDPR (e ai principali cambiamenti in tema di trattamento di dati personali), ma deve necessariamente tenere conto di un quadro normativo ancora fluido e non del tutto assestatosi.

Il Garante Privacy sta svolgendo una apprezzabile attività di divulgazione e semplificazione dei principali adempimenti necessari per la transizione alla nuova disciplina. Tra questi segnaliamo la pagina dedicata al Regolamento (http://www.garanteprivacy.it/regolamentoue), la Guida sintetica (http://194.242.234.211/documents/10160/5184810/Guida+al+nuovo+Regolamento+europeo+in+materia+di+protezione+dati), l'approfondimento sul Data Protection Officer (http://www.garanteprivacy.it/regolamentoue/rpd) e la Scheda informativa - Regolamento 2016/679/UE: le priorità per le PA (http://www.garanteprivacy.it/regolamentoue/formazione/).

### 1.1.1. Sintesi delle principali novità del GDPR

La principale novità del Regolamento è certamente costituita dalla centralità del principio di responsabilizzazione (accountability), previsto dall'art. 5. In forza di questo principio, è rimesso al titolare del trattamento il compito di assicurare, ed essere in grado di comprovare, il rispetto dei principi applicabili al trattamento dei dati personali. Non vi è più una serie predefinita di adempimenti da rispettare, ma dev'essere ciascun titolare, nell'ambito della propria autonomia e previa accurata valutazione dei rischi, a dover individuare le più idonee (e adeguate) misure organizzative e tecniche, e a doverne dimostrare l'applicazione e l'efficacia.

È importante sottolineare la centralità dei profili di sicurezza dei dati. Infatti l'art. 5 del GDPR, che individua i principi generali in tema di trattamento, menziona espressamente l'"*integrità e riservatezza*" dei dati, stabilendo che il trattamento debba avvenire "*in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali*". Si tratta di un principio analogo all'obbligo di sicurezza disciplinato dall'art. 31 del Codice Privacy, ma è significativo che ora sia elencato tra i principi cardine del trattamento.

Altre novità riguardano l'informativa, in ordine alla quale saranno introdotte anche delle icone (uguali in tutta la UE) per esemplificare i contenuti in forma sintetica e renderli di più immediata comprensione a un numero maggiore di persone. In altre parole, quando la Commissione provvederà ad approvarle, sarà possibile avere una prima generale e immediata cognizione circa l'utilizzo dei dati personali, semplicemente attraverso un chiaro sistema di icone.

L'informativa dovrà essere arricchita, in quanto dovranno essere inseriti: i dati di contatto del Data Protection Officer; la base giuridica del trattamento; l'indicazione se sia previsto il trasferimento di dati in Paesi terzi (vale a dire al di fuori dell'Unione europea), e, in caso affermativo attraverso

quali strumenti; il periodo di conservazione dei dati o i criteri stabiliti per determinarne la durata; il diritto di presentare reclamo all'Autorità di controllo e, infine, se il trattamento comporti processi decisionali automatizzati e, nel caso, la logica applicata ai processi decisionali e le possibili conseguenze per l'interessato.

Per quanto riguarda il consenso, analogamente a quanto previsto dall'art. 18 del Codice della Privacy, esso non sarà richiesto se il trattamento (di dati non sensibili) sia "*necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento*" (art. 6, comma 1, lett. e).

Il Regolamento introduce poi significative modifiche in tema di diritti dell'interessato, con una disciplina puntuale del diritto alla cancellazione ("diritto all'oblio"), e con un inedito "diritto alla portabilità del dato" (regolato dall'art. 20). In base a tale diritto, l'interessato gode della facoltà di ricevere i dati personali forniti a un titolare, in formato strutturato, di uso comune e leggibile da un dispositivo automatico, e di trasmettere tali dati a un altro titolare, per le ipotesi di trattamenti effettuati con mezzi automatizzati, basati sul consenso o su un contratto. In pratica, il livello di "signoria" sui propri dati personali arriva al punto di poter migrare liberamente da un titolare all'altro.

Questo innovativo "diritto alla portabilità" non si applica ai trattamenti di dati necessari per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, e quindi non potrà - con ogni probabilità - essere esercitato nei confronti delle pubbliche amministrazioni, quali il MIUR.

Questa breve disamina dei punti cardine del GDPR deve includere anche i concetti di "privacy by design" e "privacy by default", o, per dirla secondo la versione italiana, "protezione dei dati fin dalla progettazione" e "protezione per impostazione predefinita". Si tratta di due importanti presidi, a tutela del corretto trattamento dei dati personali, che devono iniziare a fare parte del bagaglio di cognizioni di chiunque debba realizzare - e utilizzare - sistemi che trattino dati personali.

Un altro importante adempimento è costituito dall'introduzione del Registro delle attività di trattamento, previsto dall'art. 30. Il Registro, che ricorda il "Documento Programmatico di sicurezza" previsto dall'allegato B del Codice della Privacy, non è sempre obbligatorio, ma solo per coloro che abbiano più di 250 dipendenti, ovvero (anche sotto questa soglia) laddove il trattamento possa presentare un rischio per i diritti e le libertà dell'interessato, non sia occasionale o includa il trattamento di categorie "particolari" di dati, individuati nell'articolo 9 paragrafo 1 (già individuato prima), o i dati personali relativi a condanne penali e a reati.

Il Registro deve essere tenuto dal titolare e dal responsabile, il suo contenuto minimo è appunto individuato dall'art. 30.

Il Registro, come visto, non è sempre obbligatorio, ma è sempre utile valutare la sua adozione, soprattutto nell'ottica della responsabilizzazione e della necessità di dover (comunque) dimostrare il rispetto dei principi in tema di protezione di dati personali.

Il Garante infatti ha avuto modo di precisare che "*la tenuta del registro dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema di corretta gestione dei dati personali. Per tale motivo, si invitano tutti i titolari di trattamento e i responsabili, a*

*prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro e, in ogni caso, a compiere un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche – ove già non condotta*"[4].

Completiamo questa breve introduzione con altre tre importanti novità: l'obbligo di notificazione e comunicazione delle violazioni di dati personali (c.d. *data breach*), la valutazione d'impatto e la nomina del Responsabile della protezione dei dati personali, o Data Protection Officer.

Il GDPR introduce infatti l'obbligo di notificazione al Garante dei *data breach,* entro settantadue ore dalla scoperta; obbligo a cui si aggiunge anche la comunicazione agli interessati, laddove ci sia un rischio elevato per i diritti e le libertà fondamentali. Questo impone di dotarsi di sistemi di adeguata segnalazione e reportistica delle intrusioni e delle diffusioni e perdite, anche accidentali, di dati, per essere in grado di adempiere correttamente all'obbligo. Non si tratta di una novità assoluta per le pubbliche amministrazioni, ma certamente la sua portata è molto estesa rispetto al passato, per cui tutti i dipendenti devono essere a conoscenza dell'obbligo di attivarsi in caso di violazioni di dati personali.

Per quanto riguarda la valutazione d'impatto sulla protezione dei dati personali, essa costituisce un processo strutturato di valutazione e gestione del rischio legato ai trattamenti di dati personali, da effettuarsi obbligatoriamente in specifiche situazioni, laddove il trattamento, anche per l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Vi sono delle ipotesi, espressamente individuate dal GDPR, nelle quali la valutazione d'impatto deve essere effettuata: il trattamento su larga scala di categorie particolari di dati o di dati relativi a condanne penali e a reati; la valutazione sistematica e globale di aspetti personali, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici; infine il monitoraggio sistematico di aree pubbliche su vasta scala.

Arriviamo al Data Protection Officer (DPO): si tratta di una figura sostanzialmente nuova, che deve essere nominata obbligatoriamente da enti od organismi pubblici (sia dal titolare che dal responsabile). Per i privati l'obbligo della nomina scatta solo se l'attività principale consiste in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala, oppure se l'attività principale consiste nel trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e a reati.

Il DPO (che può essere sia interno che esterno) è designato in funzione delle qualità professionali, e in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti espressamente individuati dal GDPR. Il DPO deve essere autonomo e non deve subire ingerenze, inoltre, tra i suoi compiti, vi è quello di fornire consulenza e pareri, sorvegliare sul rispetto delle disposizioni del GDPR, cooperare e fungere da punto di contatto con l'Autorità Garante.

I dati di contatto del DPO devono essere, infine, pubblicati sul sito, inseriti nell'informativa e comunicati al Garante (anche nel caso di *data breach*).

[4] http://www.garanteprivacy.it/regolamentoue/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili.

Per concludere, facciamo un cenno all'adesione ai Codici di Condotta e alle certificazioni, considerate dal GDPR come importanti presidi per poter dimostrare il rispetto dei principi e degli obblighi, e alle sanzioni: il GDPR introduce sanzioni amministrative pecuniarie pesantissime, fino a 10.000.000 di euro (o, per le imprese, fino al 2% del fatturato mondiale annuo dell'esercizio precedente, se superiore), per le ipotesi di violazione degli obblighi ricadenti sul titolare, e addirittura fino a 20.000.000 di euro (o, per gli enti privati, fino al 4% del fatturato mondiale annuo dell'esercizio precedente, se superiore) per la violazione, tra l'altro, dei principi del trattamento e dei diritti degli interessati.

Ma, al di là del (legittimo) timore per le sanzioni, la recente vicenda Facebook/Cambridge Analytica dimostra che in molti casi la peggiore sanzione è quella reputazionale, perché oramai il corretto trattamento dei dati personali viene visto come un valore in sé. Mettersi a norma, trattare correttamente i dati e rispettare i diritti degli interessati non è solo un obbligo, ma è un vero e proprio dovere anche e soprattutto per le pubbliche amministrazioni.

### 1.1.2. Termine e roadmap di adeguamento al GDPR

Il GDPR è entrato in vigore il ventesimo giorno successivo alla sua pubblicazione nella Gazzetta Ufficiale dell'Unione europea, avvenuta il 4 maggio 2016. L'art. 99 prevede però che esso si applichi soltanto a decorrere dal 25 maggio 2018.

Erano stati concessi quindi due anni di tempo per rendere i trattamenti conformi ai principi introdotti dal Regolamento, come precisato dal Considerando 171, secondo cui "*il trattamento già in corso alla data di applicazione del presente regolamento dovrebbe essere reso conforme al presente regolamento entro un periodo di due anni dall'entrata in vigore del presente regolamento*".

In questo periodo, si sarebbero dovute anche adattare o modificare sia le decisioni della Commissione, che le autorizzazioni e i provvedimenti delle singole autorità di controllo (per l'Italia, il Garante della Privacy) basate sulla direttiva 95/46/CE. Ed è sempre il Considerando 171 a precisare che esse rimangono in vigore fino a quando non vengono modificate, sostituite o abrogate.

Non bisogna dimenticare però che Il GDPR consente agli Stati membri degli spazi di manovra, soprattutto per quanto riguarda i trattamenti effettuati per finalità di interesse pubblico o da autorità pubbliche: sapremo solo dopo l'emanazione definitiva del decreto legislativo previsto dall'art. 13 della L. 163/2017 quale sarà la fisionomia definitiva dei trattamenti di dati personali nel settore pubblico.

Ma, in ogni caso, poiché il Regolamento è direttamente applicabile (e lo sarà anche in assenza delle norme nazionali di adeguamento), occorre attivarsi immediatamente, a tutti i livelli, per recepire tempestivamente le principali innovazioni.

Il Garante ha individuato, nella sua scheda normativa "Le priorità per le PA"[5] tre adempimenti cruciali, da implementare in via di assoluta urgenza:

1. La designazione del Responsabile della Protezione dei Dati – RPD o DPO, che deve essere coinvolto in tutte le questioni che riguardano la protezione dei dati personali anche nella delicata fase di transizione.
2. L'istituzione del Registro delle attività di trattamento.

   Il Garante sottolinea come sia "*essenziale avviare quanto prima la ricognizione dei trattamenti svolti e delle loro principali caratteristiche (finalità del trattamento, descrizione delle categorie di dati e interessati, categorie di destinatari cui è prevista la comunicazione, misure di sicurezza, tempi di conservazione, e ogni altra informazione che il titolare ritenga opportuna al fine di documentare le attività di trattamento svolte) funzionale all'istituzione del registro.*"

   Tra l'altro, quest'attività di ricognizione è fondamentale per "*verificare anche il rispetto dei principi fondamentali (art. 5), la liceità del trattamento (verifica dell'idoneità della base giuridica, artt. 6, 9 e 10) nonché l'opportunità dell'introduzione di misure a protezione dei dati fin dalla progettazione e per impostazione (privacy by design e by default, art. 25), in modo da assicurare, entro il 25 maggio 2018, la piena conformità dei trattamenti in corso* (Cons. 171)."
3. La notifica delle violazioni dei dati personali (cd. *data breach*).

   La corretta e puntuale attuazione delle nuove misure relative alle violazioni dei dati personali è fondamentale quale risposta alle minacce, sempre più frequenti, di violazione dei dati personali, che spesso riguardano anche sistemi di interesse pubblico. Ciò impone anche alle pubbliche amministrazioni di introdurre efficaci procedure organizzative, che consentano di attivarsi negli strettissimi tempi richiesti dalle nuove disposizioni.

Questi sono dunque i punti cruciali che tutte le pubbliche amministrazioni (e dunque anche il MIUR) devono affrontare nella delicata fase di transizione al GDPR, fase, come detto, da concludersi entro il 25 maggio 2018.

Sviluppando nel dettaglio le indicazioni del Garante, e costruendo una vera e propria roadmap da implementare, possiamo sintetizzare gli adempimenti nei seguenti punti, che dovranno essere posti in essere a tutti i livelli (MIUR, USR, istituti scolastici).

1. Censimento e identificazione dei trattamenti di dati personali, sia automatizzati che non automatizzati, compresi i flussi di scambio di dati, individuando quantomeno la base legale, le categorie di dati, le categorie di interessati e il periodo di conservazione dei dati stessi;
2. Identificazione delle situazioni di eventuale contitolarità dei trattamenti, e regolamentazione delle stesse;
3. Nomina del Responsabile della Protezione dei dati personali;
4. Individuazione dei responsabili esterni del trattamento, e adeguamento dei procedimenti di evidenza pubblica ai principi contenuti nell'art. 28 del GDPR;
5. Verifica, per tutti i trattamenti, dell'adeguatezza delle misure tecniche e organizzative adottate, nonché delle misure di sicurezza;

[5] http://www.garanteprivacy.it/regolamentoue/formazione/.

6. Creazione del Registro dei trattamenti;
7. Implementazione dei processi di privacy by design e privacy by default nei sistemi utilizzati, introducendo questi principi anche nella formulazione dei documenti di gara (bandi e capitolati);
8. Revisione delle informative agli interessati e delle procedure di riscontro alle richieste di questi ultimi;
9. Revisione di tutti i documenti e procedure di governance dei dati personali (regolamenti/direttive/circolari) in maniera tale da conformarli al GDPR;
10. Aggiornamento del Piano di formazione attività formative destinate al personale del MIUR;
11. Verifica (o introduzione) di una procedura specifica per la notificazione delle violazioni di dati personali al Garante e per la comunicazione agli interessati;
12. Effettuazione della valutazione d'impatto sul trattamento dei dati personali, per i trattamenti in ordine ai quali sia necessaria.

### 1.1.3. Ambito di applicazione

Una delle grandi innovazioni del GDPR è la significativa estensione dell'ambito di applicazione della norma, non tanto dal punto di vista della tipologia dei trattamenti, quanto soprattutto per ciò che concerne l'ambito territoriale.

Per quanto riguarda la tipologia dei trattamenti, la disciplina dettata dal Regolamento si applica sia al trattamento automatizzato che al trattamento manuale dei dati personali, se i dati personali sono contenuti o destinati a essere contenuti in un archivio, mentre non rientrano nell'ambito di applicazione i fascicoli non strutturati secondo criteri specifici. Sono esclusi soltanto i trattamenti di dati personali effettuati dalle persone fisiche nell'ambito di attività a carattere esclusivamente personale o domestico e quindi, come precisa il Considerando 18, senza una connessione con un'attività commerciale o professionale.

Per ciò che concerne l'applicazione territoriale, il GDPR si applica innanzitutto al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento[6] da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione europea, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.

La rilevante novità del Regolamento è però legata alla sua "extraterritorialità", ossia l'applicabilità anche a soggetti che non abbiano uno stabilimento nell'Unione europea. Questa espansione dell'ambito di applicazione, già anticipata da alcune sentenze della Corte europea di Giustizia, e in particolare dalla famosissima sentenza "Google Spain" del 2014 [7] , consiste nell'estendere il perimetro delle regole europee anche a soggetti extra-UE, in due specifiche ipotesi.

[6] Lo stabilimento, come precisa il Considerando 22, "implica l'effettivo e reale svolgimento di attività nel quadro di un'organizzazione stabile."

[7] http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=IT.

Il GDPR si applica infatti al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:

A. L'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure,
B. Il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

Per esemplificare, un portale di e-commerce cinese che abbia delle pagine in italiano (o in altra lingua dell'Unione) e offra beni e servizi a cittadini dell'Unione, dovrà necessariamente rispettare le norme europee. Ma non si parla solo di servizi a pagamento, e quindi l'ambito di applicazione è particolarmente esteso, come è stato recentemente riconosciuto addirittura da Mark Zuckerberg, il fondatore di Facebook, che nell'audizione al Congresso del 10 e 11 aprile 2018, dopo lo scandalo Cambridge Analytica, non solo ha mostrato apprezzamento per i principi del GDPR, ma ha anche chiaramente affermato che la sua società si conformerà al Regolamento per quanto riguarda i trattamenti dei cittadini dell'Unione europea.

I principi generali stabiliti dal Regolamento europeo, anche grazie all'applicazione potenzialmente globale, stanno diventando quindi lo standard per la regolamentazione del trattamento di dati personali anche al di fuori dell'Unione europea.

## 1.2. I PRINCIPI INTRODOTTI DAL NUOVO REGOLAMENTO EUROPEO SULLA PROTEZIONE DEI DATI

### 1.2.1. Principio di liceità del trattamento

Il principio di liceità del trattamento è il primo principio menzionato nel quadro del diritto dell'UE e del Consiglio d'Europa (CdE) in materia di protezione dei dati, con formulazione pressoché identica nell'art. 5 della Convenzione n. 108 e nell'art. 6 della Direttiva 95/46/CE. Il GDPR, nell'elencare i principi applicabili al trattamento di dati personali, conferma l'importanza e la centralità di tale principio aprendo l'art. 5 (dedicato ai principi applicabili al trattamento di dati personali) con l'espressione "*i dati personali sono: trattati in modo lecito*" e dedicando alla liceità del trattamento il successivo art. 6. Per comprendere pienamente che cosa significhi trattare i dati personali in modo lecito, e superare così le osservazioni mosse da alcuni sulla natura pleonastica dell'art. 5 par. 1 lett. a), è necessario fare riferimento non solo alla conformità del trattamento alle norme giuridiche, ma al complesso dei valori e principi che il legislatore comunitario ha inteso tutelare nell'ambito di quel bilanciamento che permea l'intero impianto del GDPR.

L'art. 6 GDPR, nel fissare le condizioni di liceità del trattamento, si pone rispetto all'art. 5 par. 1 lett. a) in una posizione di specificità e anche di prodromicità, nel senso che oltre a specificare quando un determinato trattamento può considerarsi lecito (solo se e nella misura in cui ricorra almeno una delle condizioni elencate), è il primo indicatore circa la legittimità di un trattamento. Esso sarà lecito se effettuato in presenza di una delle condizioni ivi indicate (tra le quali anche "*l'esecuzione di un compito di interesse pubblico*").

Pertanto, una volta verificata la presenza dei presupposti di liceità del trattamento in base all'art. 6, bisognerà ancora verificare l'ulteriore profilo di liceità in base all'art. 5 par. 1 lett. a) ovvero valutare se, quel trattamento lecito perché posto in essere in presenza di una (o più) delle condizioni

indicate dall'art. 6, è anche rispettoso del complesso dei diritti e valori in gioco alla luce del loro bilanciamento.

Da ultimo, ma non per importanza, occorre considerare l'art. 9 GDPR in cui sono contenute eccezioni alla regola generale del divieto di trattare le particolari categorie di dati personali (quelle che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, i dati genetici, biometrici o relativi alla salute o alla vita sessuale o all'orientamento sessuale) e le condizioni in presenza delle quali detto trattamento può considerarsi lecito (fra le quali vi sono "*i motivi di interesse pubblico rilevante*"). E infine l'art. 10 GDPR riguardante il trattamento dei dati personali relativi a condanne penali e reati, che impone come condizione di liceità, che lo stesso avvenga sotto il controllo dell'autorità pubblica o previa autorizzazione del diritto dell'unione o degli Stati membri.

In conclusione, è chiaro che il legislatore comunitario ha inteso, con l'emanazione del GDPR, collocare la dimensione individuale accanto a quella collettiva nell'ottica di un bilanciamento in cui rientrano a pieno titolo anche gli interessi della collettività.

### 1.2.2. Principio di correttezza

Accanto al principio di liceità del trattamento, il legislatore comunitario enuncia all'art. 5 par. 1 lett. a) quello della correttezza. Già presente nel D.Lgs. 196/2003, il principio di correttezza è da intendere come buona fede da osservare in tutte le fasi in cui si articola il trattamento dei dati personali.

### 1.2.3. Principio di trasparenza

I dati personali devono essere trattati non solo in modo lecito e corretto, ma anche in modo trasparente. Il diritto dell'interessato al controllo delle proprie informazioni è ritenuto talmente importante dal legislatore comunitario da inserire, nella rosa dei principi di cui all'art. 5, quello della trasparenza, che si traduce all'atto pratico in una serie di doveri che gravano in capo al titolare del trattamento.

Il principio della trasparenza ritorna all'interno del Capo III, che il GDPR riserva ai diritti dell'interessato e che apre proprio con la Sezione "*Trasparenza e modalità*". Il ragionamento alla base è semplice: per poter consentire al soggetto interessato di avere il controllo sui dati che lo riguardano (a prescindere e prima ancora della valutazione circa la eventuale illiceità del trattamento) e per rendere effettivo tale controllo è necessario fornirgli tutte le informazioni relative ai dati trattati, alle finalità del trattamento, all'identità e ai dati di contatto del titolare, del responsabile del trattamento e del Responsabile della Protezione dei Dati (DPO o RPD), agli eventuali destinatari dei dati, alla possibilità che i dati vengano trasferiti a un Paese extra UE (cfr. artt. 13 e 14 GDPR). Altrettanto importante (e sempre nell'ottica della trasparenza nel trattamento) è informare l'interessato dei diritti che il GDPR riconosce e garantisce e delle modalità attraverso cui esercitarli. La trasparenza nel Regolamento non è una mera enunciazione di principio, ma una garanzia per l'interessato che vuole essere effettiva. E per questo il legislatore europeo ha indicato le modalità attraverso le quali devono essere date all'interessato le informazioni relative ai dati personali. È necessario che siano fornite in forma concisa, trasparente (ecco che il concetto ritorna)

e facilmente accessibile, con un linguaggio chiaro e semplice, idoneo a essere compreso da chiunque, con particolare attenzione alle informazioni fornite ai minori (cfr. art. 12 par. 1 GDPR).

### 1.2.4. Principio di pertinenza

Il principio di pertinenza rientra, insieme a quello di adeguatezza e non eccedenza rispetto alle finalità, in quello più generale e onnicomprensivo della "*minimizzazione dei dati*" di cui all'art. 5 par. 1 lett. c). Con il principio di pertinenza, il legislatore europeo ha voluto prescrivere a colui che effettua il trattamento di limitarlo solo ed esclusivamente a quei dati che siano strettamente connessi alla finalità perseguita. Il dato è pertinente quando la sua trattazione è assolutamente necessaria per il perseguimento della finalità, ossia quando fra dato e finalità vi è un nesso inscindibile e dunque quando la finalità prefissata non si può raggiungere senza il trattamento di quel determinato dato personale.

### 1.2.5. Principio di necessità

Il principio di necessità non rappresenta una novità del GDPR, essendo già presente nel Codice Privacy (all'art. 3), ma, rispetto a tale principio, il legislatore europeo si è posto in un'ottica di continuità. Già nel precedente assetto normativo si era ravvisata la necessità di limitare il trattamento effettuato con sistemi tecnologici a quei dati che fossero strettamente necessari al raggiungimento della finalità perseguita, escludendo quindi il trattamento quando la stessa finalità poteva essere perseguita attraverso dati anonimi od opportuna modalità in grado di condurre all'identificazione dell'interessato solo in caso di necessità.

Il GDPR ha ribadito nell'art. 5 par. 1 lett. c) che i dati personali sono, non solo adeguati e pertinenti, ma anche "*limitati a quanto necessario rispetto alle finalità per le quali sono trattati*" sempre nell'ottica di quella minimizzazione dei dati che impone a colui che effettua il trattamento di ridurre al minimo il trattamento stesso ed evitare che si renda possibile identificare l'interessato tutte quelle volte in cui il raggiungimento della finalità perseguita non lo richieda.

### 1.2.6. Principio di sicurezza

Il principio di sicurezza è enunciato all'art. 5 par. 1 lett. f) del GDPR ma il concetto di "sicurezza" ricorre costantemente in tutto il Regolamento, rappresentando una garanzia per i diritti dell'interessato e un obbligo stringente per coloro che effettuano il trattamento. Tale osservazione fa comprendere quanto la sicurezza dei dati sia uno degli obiettivi più importanti che il legislatore europeo ha voluto realizzare con l'introduzione del GDPR, basando l'intero Regolamento su un approccio proattivo e preferendo apprestare una tutela ex ante dei dati (pur prevedendo quella ex post altrettanto efficace). La lettura della lettera f) dell'articolo -5 - secondo cui "*i dati personali sono trattati in maniera da garantire un'adeguata sicurezza [...] compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali*" - conferma che la sicurezza è principio che permea l'intera attività di trattamento. Un livello di sicurezza che il GDPR definisce "adeguato" al rischio deve essere garantito tanto a livello tecnico-informatico, quanto a livello giuridico e organizzativo ("*misure tecniche e organizzative adeguate*", art. 32 par.1).

Tra le misure che intervengono ex post rispetto alla violazione dei dati personali, ricordiamo la notifica all'Autorità Garante (art. 33) e l'eventuale comunicazione all'interessato (al fine di consentire, come "extrema ratio" che sia egli stesso ad attivarsi al fine di evitare che il rischio elevato per i suoi diritti e libertà si concretizzi.

Da non trascurare tutte quelle misure che riguardano l'aspetto meramente organizzativo, ricordando che qualsiasi realtà in cui si effettua un trattamento è prima di tutto un sistema informativo, ovvero un insieme non solo di apparecchiature, ma anche di persone, che è necessario sensibilizzare e formare e di procedure aziendali, che devono essere scrupolosamente seguite.

### 1.2.7. Principio di responsabilizzazione

Il principio di responsabilizzazione è contenuto nell'art. 5, par. 2 del GDPR. Dopo aver indicato tutti i principi che regolano il trattamento dei dati personali, il legislatore europeo afferma che "*il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo*". Ciò significa che il titolare del trattamento deve rispettare e applicare i principi di cui si è trattato nei precedenti punti e deve essere in grado di dimostrarlo.

Come si è già anticipato in apertura, la c.d. accountability rappresenta una delle novità introdotte dal GDPR, che onera il titolare del trattamento dell'obbligo di dimostrare la *compliance* al Regolamento della propria condotta nell'effettuare il trattamento. Un aiuto in tal senso proviene dalla possibilità per il titolare di aderire ai codici di condotta o a meccanismi di certificazione, che fungono da elementi di positiva valutazione circa la conformità al GDPR.

Il GDPR applica il principio di responsabilizzazione anche al responsabile del trattamento, e questa rappresenta certamente una novità rispetto al precedente panorama normativo. Egli innanzitutto potrà essere individuato come tale soltanto se in grado di apprestare garanzie sufficienti a fare in modo che il trattamento per conto del titolare avvenga in conformità al Regolamento (il che già implica un preciso impegno da parte del responsabile). Il principio si esplica ulteriormente con l'obbligo per il responsabile di attenersi strettamente, nell'attività di trattamento, alle istruzioni impartite dal titolare, che vengono formalizzate in un contratto avente forma scritta e contenente la materia disciplinata, la durata del trattamento, nonché la natura e le finalità, il tipo di dati personali e le categorie di interessati (art. 28). Infine, la tenuta dei registri di trattamento (alle condizioni e con i limiti espressamente indicati dall'art. 30) è prevista anche per il responsabile.

## 1.3. I SOGGETTI

### 1.3.1. L'interessato al trattamento e i suoi diritti

L'interessato al trattamento è la persona fisica alla quale si riferiscono (direttamente o indirettamente) i dati personali e al quale il GDPR riconosce una serie di diritti (indicati negli artt. dal 15 al 22) finalizzati a garantire una trasparenza nei rapporti con il titolare e la possibilità di esercitare un controllo effettivo su tutte le informazioni che lo riguardano nonché delle modalità attraverso le quali le stesse sono trattate.

L'attenzione che il legislatore europeo ha dimostrato nei confronti dell'interessato è resa evidente dalla cospicua serie di obblighi posti in capo al titolare e al responsabile del trattamento, fra i quali campeggiano quelli di informativa. L'aver imposto il rispetto di determinate modalità di comunicazione con l'interessato denota da parte del legislatore europeo l'intenzione di rendere

effettiva la tutela e concreto l'esercizio dei diritti, al di là di una loro enunciazione meramente formale. In tal senso deve essere letto a esempio l'obbligo di modulare il linguaggio tenendo conto delle caratteristiche soggettive dell'interessato, in particolare qualora si tratti di soggetti minori.

DIRITTO ALL'ACCESSO

L'art. 15 del GDPR riconosce all'interessato 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*". Tra le informazioni alle quali l'interessato può avere accesso rientrano le finalità del trattamento, le categorie di dati trattati, i destinatari a cui i dati verranno trasmessi.

Attraverso l'esercizio - gratuito - del diritto di accesso l'interessato è in grado di soddisfare quel controllo sui propri dati personali ed è così, in grado di verificare personalmente la legittimità del trattamento e di intervenire in caso di violazione. Continua a essere previsto, anche con il GDPR, il diritto dell'interessato a ottenere una copia dei dati oggetto di trattamento.

DIRITTO ALL'AGGIORNAMENTO DEI DATI

Il diritto all'aggiornamento dei dati, previsto dall'art. 16 del GDPR, consiste nella possibilità, per l'interessato di ottenere che i suoi dati, oggetto di trattamento, siano costantemente aggiornati da parte del titolare. Questo diritto viene esercitato attraverso una richiesta di rettifica dei dati inesatti o non più attuali e l'integrazione di quelli incompleti. Attraverso l'esercizio di tali diritti si garantisce all'interessato che i propri dati mantengano attualità per tutta la durata del trattamento e nel rispetto della sua identità.

DIRITTO ALLA CANCELLAZIONE (DIRITTO ALL'OBLIO) E LE SUE CONDIZIONI

L'interessato ha (sulla scorta dell'art. 17 del GDPR) il diritto a chiedere la cancellazione dei dati che lo riguardano. All'esercizio di tale diritto consegue l'obbligo in capo al titolare del trattamento di provvedere alla loro cancellazione. Tuttavia tale diritto non ha una portata illimitata, ma è circoscritta al verificarsi di determinate ipotesi. In particolare potrà richiedersi la cancellazione nei casi in cui:

→ I dati non siano più necessari alla finalità per la quale sono stati raccolti o trattati;
→ L'interessato abbia revocato il consenso (nel caso in cui esso sia il solo fondamento di liceità del trattamento);
→ I dati siano stati trattati illecitamente o debbano essere cancellati per adempiere a un obbligo legale cui è soggetto il titolare del trattamento; e infine,
→ I dati siano stati raccolti nell'ambito di servizi offerti dalla società dell'informazione.

Il diritto a ottenere la cancellazione ha, poi, diverse eccezioni, fra le quali rientrano anche l'adempimento a un obbligo legale cui sia soggetto il titolare del trattamento o l'esecuzione di un compito svolto nel pubblico interesse, ovvero per l'esercizio di pubblici poteri.

Per fare un esempio pratico, l'interessato al trattamento effettuato per la formazione di una graduatoria da parte del MIUR non potrà - intuitivamente - chiedere la cancellazione dei suoi dati

personali in essa contenuti, essendo il trattamento svolto nel pubblico interesse, e nei limiti in cui il trattamento sia pertinente a tale compito.

Al contrario, ben potrà essere richiesta la cancellazione qualora gli stessi dati siano trattati illecitamente. Si pensi al caso in cui, erroneamente, la medesima graduatoria predisposta da un ufficio del MIUR, e contenente dati inerenti lo stato di salute (ad esempio poiché da essa si possa rilevare l'appartenenza a categorie protette), venga ad essere diffusa mediante pubblicazione in amministrazione trasparente, senza le dovute cautele. In quest'ipotesi, al di là delle eventuali sanzioni amministrative pecuniarie e della responsabilità civile, ben l'interessato potrà richiedere la cancellazione dei dati trattati.

## DIRITTO DI LIMITAZIONE DEL TRATTAMENTO

Con l'art. 18 il GDPR riconosce all'interessato il diritto di ottenere la limitazione del trattamento dei dati che lo riguardano, al verificarsi di determinate condizioni:

→ L'interessato contesta l'esattezza dei dati;
→ Il trattamento dei dati è illecito e l'interessato stesso si oppone alla loro cancellazione;
→ I dati sono necessari all'interessato per esercitare o difendere un diritto in giudizio benché non più necessari al titolare del trattamento in relazione alla finalità perseguita; e infine,
→ L'interessato si è opposto al trattamento in attesa della verifica circa l'eventuale prevalenza dei motivi legittimi del titolare rispetto ai suoi.

Limitare il trattamento dei dati significa, per l'interessato, poter porre un vincolo sugli stessi che rende quei dati indisponibili e non più utilizzabili, da parte del titolare, per un periodo di tempo limitato e suscettibile di revoca (in tale ultimo caso spetterà al titolare dare preventiva informazione all'interessato).

## DIRITTO ALLA PORTABILITÀ DEI DATI

L'art. 20 del GDPR introduce un'assoluta novità: il diritto alla portabilità dei dati. In base a esso l'interessato ha il diritto di ricevere i dati personali che lo riguardano, in un formato strutturato, di uso comune e leggibile da dispositivo automatico e altresì ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti dal primo titolare qualora ricorrano cumulativamente due condizioni: il trattamento si basi sul consenso (anche in relazione alle particolari categorie di dati di cui all'art. 9) o sia necessario per eseguire un contratto e avvenga con mezzi automatizzati.

Il diritto alla portabilità dei dati realizza un duplice obiettivo: non solo potenziare la tutela dell'interessato ma garantire nel contempo la libera circolazione dei dati. Attraverso l'esercizio di tale diritto infatti viene consentito all'interessato di superare i vincoli che lo legano a un titolare del trattamento, potendo egli "portare con sé" i propri dati nel passaggio a un diverso titolare, senza che ciò comporti oneri di sorta. Allo stesso tempo, come affermato dall'art. 29 WP[8] il diritto alla

[8] Linee guida sul diritto alla portabilità dei dati http://194.242.234.211/documents/10160/5184810/Linee-guida+sul+diritto+alla+portabilit%C3%A0+dei+dati+---+WP+242.pdf.

portabilità dei dati ne facilita il trasferimento e aumenta la competizione tra fornitori favorendo la creazione di servizi innovativi nel mercato digitale. Questo diritto, come già sottolineato, non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, e non può dunque essere esercitato nei confronti delle pubbliche amministrazioni, quali il MIUR.

DIRITTO DI OPPOSIZIONE

L'art. 21 del GDPR riconosce all'interessato il diritto di opporsi al trattamento dei propri dati personali in qualsiasi momento e per motivi anche non connessi all'eventuale illegittimità del trattamento. Quando l'interessato esercita tale diritto il titolare deve interrompere il trattamento, a meno che non riesca a dimostrare l'esistenza di motivi legittimi in grado di prevalere sugli interessi e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Specifica disciplina è invece prevista per l'ipotesi in cui i dati personali siano trattati per finalità di marketing diretto. In tale ipotesi l'interessato può esercitare il diritto di opposizione in qualsiasi momento e senza essere vincolato al bilanciamento con gli interessi di cui è portatore il titolare, poiché evidentemente, nella concezione del legislatore europeo, la finalità commerciale è sempre subordinata alla volontà dell'interessato di opporsi, che pertanto prevale in ogni caso. In tale caso pertanto il titolare deve obbligatoriamente interrompere il trattamento.

IL TRATTAMENTO AUTOMATIZZATO E LA PROFILAZIONE

L'art. 22 del GDPR, rubricato "*processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione*", sancisce il diritto per l'interessato di non essere sottoposto a una decisione basata unicamente su un trattamento automatizzato, compresa la profilazione, se tale decisione è in grado di incidere sulla sua persona.

La norma in esame non vieta l'adozione di processi automatizzati, né della profilazione (intesa come processo in grado di valutare aspetti personali relativi a una persona fisica al fine di prevederne aspetti riguardanti a esempio le preferenze o gli interessi personali, il comportamento, la situazione economica etc...), ma consente all'interessato di sottrarsi a una decisione che sia basata unicamente su tale modalità di trattamento e che si riverberi sulla sua persona o sia in grado di produrre effetti giuridici che lo riguardano.

Tale diritto non è esercitabile nelle ipotesi in cui la decisione sia necessaria per la conclusione o l'esecuzione di un contratto in cui una delle parti sia l'interessato, quando sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare o si basi sul consenso esplicito dell'interessato. La tutela di quest'ultimo si realizza ancora una volta attraverso la previsione che le deroghe appena indicate sono ammesse laddove il titolare adotti misure adeguate a tutelare i diritti, le libertà e i legittimi interessi dell'interessato.

In altre parole, il GDPR non introduce un divieto assoluto (o la possibilità incondizionata) di opporsi a una decisione che sia basata unicamente su di un trattamento automatizzato (si pensi ai casi di graduatorie elaborate anche attraverso sistemi informatici, quali ad esempio quelle della mobilità del personale docente immesso in ruolo o assunto a tempo indeterminato dal MIUR, sulla base del piano straordinario di assunzioni indetto con l. n. 107/2015).

In primo luogo, la norma si applica laddove la decisione sia **unicamente** basata su trattamento automatizzato, e dunque non può estendersi alle ipotesi ove vi sia un intervento umano. In secondo luogo, come abbiamo visto, anche delle decisioni interamente automatizzate sono ammissibili (per quanto riguarda le pubbliche amministrazioni) qualora laddove vi sia una norma che le autorizza, e che individui anche le misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dei soggetti interessati.

### 1.3.2. Titolare del trattamento (Data controller)

La figura del titolare del trattamento dei dati personali, nel passaggio dall'applicazione della disciplina di cui alla Direttiva 95/46/CE (e quindi del D.Lgs. 196/2003) al Regolamento europeo, muta in minima parte. Il titolare del trattamento (data controller), infatti, non viene designato da nessuno, né la sua qualifica di titolare deve essere formalizzata: la titolarità, in sostanza, discende dal tipo di attività svolte che sono quelle di determinare, singolarmente o insieme ad altri (in caso di contitolarità), le finalità e i mezzi del trattamento dei dati personali (così come previsto dalla definizione di cui all'art. 4 del GDPR).

Il titolare è, perciò, la persona fisica, giuridica, autorità pubblica, servizio o altro organismo che singolarmente o insieme ad altri soggetti governa finalità e mezzi dell'intero trattamento e che disciplina le attività di raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione e, infine, cancellazione o distruzione dei dati personali. In quanto attore principale nella scena del trattamento dei dati personali è proprio in capo a tale figura che incombono tutta una serie di obblighi e responsabilità finalizzate alla protezione concreta ed efficace dei dati personali.

Nell'ottica del principio di responsabilizzazione (accountability), a esempio, dovrà applicare correttamente le norme in materia di trattamento dei dati personali, oltre a dover individuare le misure adeguate tecniche e organizzative a presidio del corretto trattamento e, profilo non meno rilevante, essere in grado di dimostrare - a posteriori e qualora richiesto dall'Autorità di controllo - il rispetto e la conformità del trattamento dei dati personali di cui abbia la titolarità alla normativa in materia.

Di rilievo, a questo punto, osservare che il GDPR - a differenza della previgente disciplina europea - prevede espressamente (art. 26) l'istituto della contitolarità del trattamento (che nella previgente disciplina era stato, comunque, individuato sulla base della prassi). Contitolarità significa, sostanzialmente, che con riferimento al medesimo trattamento di dati personali (relativo, cioè, agli stessi dati personali) vi sono due o più soggetti legittimati a determinarne finalità e mezzi. I contitolari devono (per quanto riguarda le decisioni su finalità e mezzi del trattamento) determinare in modo trasparente, mediante un accordo interno, le rispettive responsabilità circa l'osservanza degli obblighi imposti al titolare dal GDPR e, inoltre, in tale accordo può designarsi un unico punto di contatto per gli interessati. È bene evidenziare, oltretutto, che indipendentemente dai termini di tali accordi interni tra contitolari l'interessato può comunque esercitare i propri diritti nei confronti di ciascun titolare.

Nell'ambito del MIUR sarà necessario individuare, anzitutto, nella scansione dei singoli trattamenti e dei soggetti coinvolti, chi - per ciascun trattamento - possa legittimamente definire finalità e mezzi del trattamento (e quindi chi possa definirsi titolare del trattamento). Qualora tale possibilità di individuare finalità e mezzi del trattamento spetti congiuntamente a più soggetti diversi (ad esempio

MIUR e USR o Istituto scolastico) ci troveremmo di fronte ad un'ipotesi di contitolarità. Sarà, a questo punto, necessario un accordo interno che definisca i ruoli dei diversi titolari con riferimento al medesimo trattamento di dati personali, le rispettive funzioni di comunicazione agli interessati e, in tale documento, dovrà individuarsi un punto di contatto da indicare agli interessati. Tale accordo tra contitolari non sarà necessario nel caso in cui i rapporti tra determinati contitolari sia regolato dal diritto dell'Unione europea o dal diritto nazionale.

Un utile esempio è quello offerto dall'Anagrafe Nazionale Studenti (ANS) che contiene i dati relativi alla carriera scolastica dei soggetti fin dal loro primo ingresso nel circuito scolastico (dal 2013 anche quelli relativi al settore dell'infanzia, ulteriormente implementati nel 2016), rispetto ai quali il MIUR, in base all'ultimo schema di decreto ministeriale che è stato sottoposto al parere del Garante Privacy, si pone come titolare del trattamento[9].

### 1.3.3. Responsabile del trattamento (Data processor)

Il responsabile del trattamento dei dati personali (che nella versione inglese del GDPR è chiamato "Data processor" e che non deve essere confuso con la figura del Responsabile della protezione dei dati o Data Protection Officer) è un soggetto che riveste una posizione predominante nell'impianto del GDPR per la sua funzione - sebbene soggetta alle limitazioni impostegli dal titolare mediante le istruzioni specifiche - di protezione dei dati personali. Il responsabile del trattamento, nella definizione del GDPR, è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Il responsabile del trattamento, a differenza del titolare, non partecipa alla definizione delle finalità e dei mezzi del trattamento ma deve attenersi alle istruzioni del titolare per il trattamento di cui sia stato incaricato da parte di quest'ultimo. Il responsabile del trattamento deve presentare garanzie sufficienti per mettere in atto le misure tecniche e organizzative adeguate alla protezione del dato personale trattato per conto del titolare, e ciò determina la necessità, per il titolare, che già in fase preliminare si accerti della "affidabilità" del responsabile del trattamento. Il responsabile, inoltre, può nominare un sub-responsabile sempre nei limiti delle istruzioni che gli siano state fornite dal titolare.

Le istruzioni al responsabile del trattamento sono conferite dal titolare mediante atto contrattuale in cui sono individuati:

→ Gli obblighi per il responsabile del trattamento;
→ 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, tra l'altro, contiene una serie dettagliata di istruzioni che riguardano, a esempio, la garanzia fornita dal responsabile al titolare che tutti i soggetti autorizzati a trattare i dati personali si

[9] Si veda a tal proposito il parere del Garante Privacy n. 301 del 5 luglio 2017 sullo schema di decreto proposto dal Ministero dell'Istruzione, dell'Università e della Ricerca.

siano impegnate alla riservatezza; la corretta adozione delle adeguate misure di sicurezza tecniche e organizzative; la nomina del Data Protection Officer ove richiesto; notificare al titolare le eventuali violazioni di dati personali. In base all'art. 29, infatti, al responsabile del trattamento sarebbe precluso il trattamento dei dati in assenza di specifiche istruzioni da parte del titolare. L'ultimo comma dell'art. 28 del GDPR disciplina, infine, l'ipotesi del responsabile che diventi "titolare di fatto" (o contitolare di fatto) nel caso in cui, esorbitando dai compiti a lui spettanti, determini finalità e mezzi del trattamento.

Il rapporto tra titolare e responsabile del trattamento non deve, però, indurre a ritenere che il responsabile del trattamento di cui all'art. 28 del GDPR sia una figura omologa a quella conosciuta in Italia nella vigenza del Codice della Privacy. La nuova figura di responsabile del trattamento, infatti, si colloca necessariamente all'esterno dell'ambito organizzativo del titolare e da esso è ben distinto: non è possibile ritenere inquadrabile la vecchia figura di "responsabile interno" nella norma dell'art. 28 del GDPR. A ritenere diversamente, infatti, si determinerebbero una serie di cortocircuiti logici secondo cui, ad esempio, il responsabile "interno" potrebbe nominare un responsabile della protezione dei dati distinto e ulteriore rispetto a quello eventualmente già nominato dal titolare.

Nell'ambito del MIUR, pertanto, si dovrà procedere ad una ricognizione dei soggetti ai quali i titolari (MIUR, USR, Istituti scolastici in primis) conferiscano dei dati personali di cui abbiano la titolarità per l'esecuzione di determinati compiti. Si pensi, ad esempio, alla società esterna alla quale sia affidato il compito di gestire i sistemi informatici e i database dell'Amministrazione.

### 1.3.4. L'incaricato del trattamento

Il GDPR non prevede espressamente la figura dell'incaricato del trattamento. Potrebbe apparire una dimenticanza ma in realtà tale figura può ritenersi ancora esistente anche nell'ottica del GDPR in quanto l'art. 29 prevede anche che i soggetti che si trovino sotto l'autorità del titolare o del responsabile di trattamento possano trattare i dati personali solo se istruiti in tal senso (salvo che sia previsto diversamente dal diritto dell'Unione europea o degli Stati membri). Si tratta di una categoria di soggetti che possono continuare a essere definiti, per semplicità, incaricati (o, meglio, autorizzati) al trattamento dei dati personali da parte del titolare o del responsabile.

Nell'ottica del rispetto del principio di accountability e, soprattutto, della necessità di dimostrare, a posteriori, la conformità al GDPR del trattamento di dati personali effettuato dal titolare o dal responsabile, sarà consigliabile tenere "traccia" sia dell'autorizzazione al trattamento sia delle istruzioni fornite a tali autorizzati. Anche nell'ambito del MIUR tale individuazione dei vari soggetti autorizzati al trattamento dovrà rispettare il principio di accountability e, soprattutto, di minimizzazione dei trattamenti individuando - una volta eseguita la scansione con il registro dei trattamenti - quali soggetti (rientranti nell'organigramma del MIUR o degli USR o del singolo Istituto scolastico) possano essere autorizzati a trattare determinati dati personali al fine di adempiere compiutamente alle mansioni lavorative.

# 2. IL DATO PERSONALE E IL TRATTAMENTO

## 2.1. IL DATO PERSONALE E IL SUO TRATTAMENTO

Nel GDPR è dato personale "*qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato)*". Si tratto di una definizione analoga a quanto previsto dalla Direttiva 95/46/CE e, prima ancora, dalla Convenzione 108/81[10]. Lo stesso dicasi per la definizione di "persona identificabile": ossia la persona fisica che può essere identificata, direttamente o indirettamente, con riferimento a dati identificativi, quali 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, psichica, economica, culturale o sociale e infine, novità introdotta dal GDPR, anche genetica.

Occorre, anzitutto, precisare che sebbene i concetti di dato personale e informazione, nel GDPR, appaiano come sinonimi si tratta di due concetti da tenere distinti: l'informazione è ciò che dal dato personale può ricavarsi. Su tale distinzione si è già espresso[11] in passato il Gruppo di lavoro "Article 29" sottolineando - sulla base della previgente, ma sostanzialmente sovrapponibile, definizione di dati personale - che il concetto di "dato personale" debba essere analizzato scomponendo la definizione nei suoi quattro elementi:

→ "qualsiasi informazione";
→ "concernente" (nel GDPR "riguardante");
→ "persona fisica";
→ "identificata o identificabile".

Pur essendo i concetti di "dato personale" e "informazione" ontologicamente distinti è bene concludere nel senso che "le informazioni tanto oggettive che soggettive su una persona, di qualunque portata, possono essere considerate 'dati personali' al di là del supporto tecnico usato" (così Art29WP).

Che cosa si intende per "**trattamento**"?

Nel GDPR è "*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*". Dalla lettura della definizione, e dall'ampiezza dei comportamenti indicati, si evince che la nozione di trattamento è atta a ricomprendere qualsiasi operazione che abbia a oggetto il dato personale, sia essa singola o plurima, effettuata con strumenti informatici o con altri mezzi (ad esempio cartacei).

[10] La *Convention for the protection of individuals with regard to automatic processing of personal data* definisce dato personale come "*any information relating to an identified or identifiable individual*".
[11] Parere 4/2007 sul concetto di dato personale espresso dall'Art29 Working Party http://194.242.234.211/documents/10160/10704/ARTICOLO+29+-+WP+136.pdf.

### *2.1.1. Categorie di dati personali*

Il Regolamento europeo ha introdotto delle importanti novità per quanto concerne le categorie di dati personali. Abbandonando la tripartizione "dati personali comuni", "dati sensibili" e "dati giudiziari" (presente nel Codice Privacy) il GDPR innova rispetto al passato introducendo le definizioni di "dati genetici", "dati biometrici" e dedicando particolare attenzione al trattamento delle "categorie particolari di dati personali" e a quello dei "dati personali relativi a condanne penali e reati".

In base al GDPR, infatti, rientrano nelle "categorie particolari di dati personali" oltre ai dati atti a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (già "dati sensibili" per il Codice Privacy) anche i dati biometrici e quelli genetici.

Il generale divieto posto dall'art. 9 del GDPR di trattare tali categorie di dati conosce delle eccezioni espressamente e tassativamente previste dal secondo comma del medesimo articolo, tra le quali, si ricorda quella relativa al trattamento necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri (lett. g) e quella relativa al caso in cui l'interessato abbia prestato il proprio consenso esplicito al trattamento di tali dati personali (lett. a).

### *2.1.2. La pseudonimizzazione*

"Pseudonimizzazione" è una definizione di nuovo conio. Il GDPR la definisce come "*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*". La pseudonimizzazione, pertanto, è un trattamento volto a separare i dati dalla persona alla quale si riferiscono: i dati personali vengono trattati, ma non si è in grado di ricondurli direttamente all'interessato.

Il Regolamento precisa altresì le modalità attraverso le quali è possibile ottenere una pseudonimizzazione del trattamento: conservando separatamente le informazioni aggiuntive che consentirebbero di ricondurre i dati alla persona alla quale si riferiscono ed effettuando tale conservazione con misure tecniche e organizzative adeguate ad evitare la riattribuzione. La norma, infatti, prevede tali modalità quali condizioni per la stessa individuabilità della pseudonimizzazione ("*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*").

I dati pseudonimizzati sono pur sempre dati personali (a differenza dei dati anonimi), ma non è possibile ricondurli alla persona fisica alla quale gli stessi si riferiscono e, dunque, risalire immediatamente all'identità della stessa (proprio in virtù di quella conservazione separata delle informazioni aggiuntive).

## 2.2. L'INFORMATIVA

### *2.2.1. I dati personali raccolti (e non) presso l'interessato*

Il GDPR dedica all'informativa gli articoli 13 e 14, indicando rispettivamente quali informazioni il titolare del trattamento debba fornire qualora i dati siano raccolti presso l'interessato e quali fornire qualora non siano stati ottenuti presso lo stesso. Ciò che è rimasto identico rispetto al passato è che l'informativa deve essere fornita all'interessato prima di effettuare la raccolta dei dati (salvo che ci

si trovi in una delle ipotesi di cui all'art. 14), che il titolare deve obbligatoriamente indicare i propri riferimenti e quelli del responsabile del trattamento, che devono essere indicate le finalità del trattamento, i diritti dell'interessato e, infine, quali siano gli eventuali destinatari dei dati.

Il GDPR amplia il novero delle informazioni da fornire agli interessati introducendo: i dati di contatto del DPO-RPD; la base giuridica del trattamento; l'interesse legittimo al trattamento e se questo ne costituisce la base giuridica; l'intenzione di trasferire i dati in Paesi terzi e, in caso affermativo, attraverso quali strumenti; il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione; il diritto per l'interessato di presentare un reclamo all'autorità di controllo (l'Autorità Garante per la protezione dei dati personali). Se il trattamento comporta poi processi decisionali automatizzati (anche la profilazione), è necessario specificare la logica di tali processi decisionali e le conseguenze per l'interessato.

Qualora i dati non siano raccolti presso l'interessato, a tali obblighi informativi (che rappresentano un elenco tassativo) debbono esserne aggiunti altri. L'informativa in questo caso deve essere fornita all'interessato entro un termine ragionevole che non può superare un mese dalla raccolta, oppure al momento della comunicazione dei dati (a terzi o all'interessato).

Nell'ipotesi in cui i dati non siano raccolti presso l'interessato potranno aversi casi di esclusione dell'obbligo di fornire l'informativa, fra i quali quelli in cui la comunicazione delle informazioni prescritte risulti impossibile o tale da implicare uno sforzo sproporzionato[12] e quelli in cui i dati debbano rimanere riservati conformemente a un obbligo di segreto professionale o a un obbligo di segretezza previsto per legge.

Con riferimento, infine, alla forma che l'informativa deve avere si evidenzia come il GDPR, nell'ottica di garantire un rapporto realmente trasparente tra titolare e interessato, prevede che l'informativa sia redatta in forma concisa, trasparente (nel senso che deve trasmettere le finalità e modalità del trattamento da parte del titolare), intelligibile per l'interessato e facilmente accessibile. Oltretutto, nel caso in cui l'informativa sia rivolta a minori, sarà necessario usare un linguaggio chiaro e semplice.

Per quanto concerne la forma in cui l'informativa debba essere resa si nota come - anche al fine di agevolare la possibilità di "dimostrazione" insita nel concetto di accountability - in linea di principio deve essere fornita per iscritto e in formato elettronico. Tuttavia il GDPR ammette anche - se richiesto dall'interessato - che l'informativa sia fornita oralmente ma, in questo caso, dovrebbe pur sempre potersi comprovare l'identità dell'interessato. Potranno, infinte, utilizzarsi forme semplificate di informativa mediante icone standardizzate (identiche in tutta l'UE, che dovranno essere identificate mediante un provvedimento della Commissione europea) in grado di esporre il contenuto dell'informativa in maniera sintetica, ma solo in combinazione con l'informativa estesa.

Il MIUR, e tutti i titolari del trattamento quali USR e Istituti scolastici, dovranno adeguare le proprie informative (anche quelle rese attraverso i siti internet istituzionali) alla nuova disciplina del GDPR. In particolare, accanto alle informazioni già presenti (quali i tipi di dati trattati; i riferimenti del titolare e quelli dell'eventuale rappresentante nel territorio italiano; le finalità e modalità del

[12] la cui valutazione è lasciata alla discrezionalità del titolare stesso, al quale saranno certamente utili i criteri evidenziati nei provvedimenti del Garante, ad esempio: http://www.garante-privacy.it/web/guest/home/docweb/-/docweb-display/docweb/3864423.

trattamento; le conseguenze all'eventuale rifiuto di fornire i dati personali; i diritti dell'interessato; l'eventuale responsabile del trattamento e gli eventuali destinatari dei dati personali oggetto di trattamento) dovranno indicarsi:

→ I dati di contatto del Data Protection Officer;
→ La base giuridica del trattamento;
→ L'indicazione se sia previsto il trasferimento di dati in Paesi extra-UE (e nel caso attraverso quali strumenti);
→ Il periodo di conservazione dei dati (o quantomeno i criteri previsti per stabilire la durata della conservazione);
→ Il diritto di presentare reclamo all'Autorità di controllo (Garante);
→ Se il trattamento comporti processi decisionali automatizzati (e nel caso la logica dei processi decisionali e le possibili conseguenze per l'interessato).

## 2.3. IL CONSENSO E LE ALTRE BASI GIURIDICHE PER LA LICEITÀ DEL TRATTAMENTO

Il consenso è, anche nel GDPR, una delle condizioni per la liceità del trattamento. L'art. 6 apre il paragrafo 1 affermando che "*il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni*" e procede con l'elenco che vede in testa (lett. a) proprio il consenso dell'interessato.

In posizione pariordinata l'art. 6 indica, come altre basi giuridiche, il trattamento necessario: b) all'esecuzione di un contratto di cui l'interessato è parte, c) affinché il titolare possa adempiere a un obbligo legale al quale è soggetto, d) per la salvaguardia di interessi vitali dell'interessato o di un'altra persona fisica, e) per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare e infine f) quello necessario per il perseguimento del legittimo interesse del titolare o dei terzi ma a condizione che non prevalgano gli interessi o i diritti o le libertà fondamentali dell'interessato (in particolare se l'interessato è un minore).

Per quanto concerne la PA, la base legittimante il trattamento deve essere individuata non nel consenso dell'interessato ma nell'adempimento di un obbligo legale, o nell'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, di cui è investita la P.A., la quale agisce sulla base di leggi o regolamenti. Ciò si traduce, in pratica, nella non necessità per la PA di acquisire il consenso da parte dell'interessato qualora i dati siano raccolti e trattati per finalità istituzionali. D'altronde, anche il Codice della Privacy, all'art. 18, comma 4, prevede una norma analoga, e legittima il trattamento dei dati a prescindere dal consenso dell'interessato.

Quando il trattamento avviene sulla base del consenso, il GDPR richiede che esso sia libero, specifico, informato e inequivocabile e, - in relazione alle particolari categorie di dati di cui all'art. 9 -, anche esplicito.

Infine, per quanto concerne il consenso espresso dai minori, il GDPR prescrive all'art. 8 che, qualora lo stesso riguardi i servizi della società dell'informazione (Facebook, Google, Twitter, etc.), lo stesso sia lecito ove il minore abbia compiuto almeno 16 anni. È lasciata alla discrezionalità di ogni singolo Stato membro la facoltà di stabilire un'età inferiore, purché non inferiore ai 13 anni.

## 2.4. IL RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD O DPO, DATA PROTECTION OFFICER);

### *2.4.1. Designazione e caratteristiche*

Il Responsabile della protezione dei dati (RPD), o Data Protection Officer (DPO) - disciplinato dagli artt. 37 e ss. - è, come abbiamo visto, una delle più importanti novità introdotte dal GDPR. È una figura obbligatoria per le autorità pubbliche e gli organismi pubblici[13], ma più autorità pubbliche possono peraltro designare anche un unico DPO, tenuto conto della struttura organizzativa e della loro dimensione.

Si tratta di una scelta che deve essere adeguatamente motivata. Pertanto si potrà, ad esempio, nominare un DPO unico per più titolari (ad esempio USR e istituti scolastici), ma sarà imprescindibile valutare la effettività di tale nomina, sia sulla base delle strutture che delle loro dimensioni, e anche della "facile raggiungibilità" del DPO stesso.

Il DPO potrà essere interno (e dunque un dipendente) o esterno, purché scelto in funzione delle sue qualità professionali, e, in particolare, della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti assegnatigli ai sensi del GPDR.

Qualora si scelga di individuare la figura del DPO in una professionalità interna, occorrerà formalizzarla attraverso un apposito atto di designazione, in ordine a cui il Garante ha reso disponibile schema-tipo[14] per la nomina a "Responsabile per la protezione dei dati". Laddove invece si opti per un soggetto esterno, la designazione dovrà costituire parte integrante del contratto di servizi, redatto conformemente all'art. 37 del GDPR.

Il Garante ha, anche di recente, precisato[15] che il DPO, al quale non sono richieste specifiche attestazioni formali o l'iscrizione in appositi albi, deve possedere un'approfondita conoscenza della normativa e delle prassi in materia di privacy, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento.

### *2.4.2. Posizione e Compiti del Responsabile della Protezione dei Dati*

Il DPO è una figura particolare da coinvolgere tempestivamente e adeguatamente in tutte le questioni riguardanti la protezione dei dati personali, e al quale devono essere garantite le risorse necessarie per operare e per mantenere la propria competenza specialistica. È autonomo nell'esecuzione dei suoi compiti, non può essere rimosso o essere oggetto di provvedimenti discriminatori per la sua attività; riferisce direttamente al vertice gerarchico, e può essere anche direttamente contattato dagli interessati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei diritti.

---

[13] Sul sito del Garante è reperibile una utile pagina informativa sulla figura del DPO --- http://www.garanteprivacy.it/regolamentoue/rpd. L'art. 29 Data Protection Working Party ha pubblicato delle "Guidelines on Data Protection Officers ('DPOs')" - http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048, disponibili anche nella versione italiana.

[14] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7322273.

[15] http://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6826945#1.

Il DPO è, infine, tenuto al segreto, e può svolgere anche altri compiti e funzioni, purché non in conflitto di interessi. Il Garante, nelle sue "Nuove FAQ sul Responsabile della Protezione dei dati (RPD) in ambito pubblico"[16] sottolinea come occorra valutare se le eventuali ulteriori funzioni assegnate non comportino la definizione di finalità e modalità del trattamento dei dati. Secondo l'Autorità, nell'ambito pubblico, oltre ai ruoli manageriali di vertice, può sussistere conflitto di interessi anche rispetto a figure apicali investite di capacità decisionali in ordine alle finalità e ai mezzi del trattamento di dati personali, tra cui il responsabile dei Sistemi informativi e il responsabile dell'Ufficio di statistica.

I compiti del DPO sono indicati analiticamente dall'art. 39 del GDPR, secondo cui questa figura deve:

1. Informare e fornire consulenza al titolare o al responsabile nonché ai dipendenti in merito agli obblighi derivanti dal GDPR e dalle altre disposizioni rilevanti, anche con riguardo alla tenuta del Registro dei trattamenti;
2. Sorvegliare sull'osservanza del GDPR e delle altre disposizioni rilevanti, e delle politiche adottate dal titolare o dal responsabile in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e agli audit;
3. Fornire, se richiesto, un parere in merito alla valutazione d'impatto e sorvegliarne lo svolgimento;

Sempre l'art. 39 inserisce alcuni compiti del DPO di natura quasi più pubblicistica che privatistica. Il DPO deve infatti:

4. Cooperare con il Garante;
5. Fungere da punto di contatto per il Garante per questioni connesse al trattamento ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Si tratta quindi di una figura centrale per il corretto trattamento di dati personali, dotato di incisivi poteri di controllo, di spiccata autonomia, che si spinge al punto da dover prestare cooperazione alle attività dell'Autorità Garante. In questo contesto, la scelta accurata di un DPO competente e preparato sarà fondamentale anche per garantire il miglior livello possibile di protezione dei dati personali.

### *2.4.3. La pubblicità dei dati di contatto del DPO*

Il DPO deve essere sempre "*facilmente raggiungibile*" (il GDPR indica questo requisito per i gruppi imprenditoriali, ma è facilmente estendibile anche alle pubbliche amministrazioni, qualora sia nominato un solo DPO per più amministrazioni distinte), e, soprattutto, deve essere agevolmente contattabile sia dagli interessati che dai dipendenti, oltre che, naturalmente, dall'Autorità Garante.

Per queste ragioni, è previsto che dei dati di contatto (e, in alcuni caso, anche del nominativo) del DPO sia data ampia pubblicità. I dati di contatto del DPO devono infatti essere pubblicati sul sito

[16] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7322110.

dell'Ente, comunicati all'Autorità Garante[17], e riportati nell'informativa. Non solo: il nome e i dati di contatto vanno comunicati all'Autorità Garante e all'interessato in caso di *data breach*, e sempre all'Autorità Garante nelle ipotesi di consultazione preventiva ex art. 36 del GDPR.

Tutti i dipendenti, devono quindi essere a conoscenza dell'esistenza di questa figura e delle sue funzioni, quantomeno per due ordini di ragioni. In primo luogo poiché è fondamentale che i dipendenti possano agevolmente contattare il DPO qualora abbiano dei dubbi in ordine all'applicazione del GDPR, o all'interpretazione delle politiche del titolare in tema di trattamento di dati personali. Ad esempio, se un dipendente del MIUR avesse delle perplessità in ordine alla liceità di una pubblicazione online, o di una comunicazione, o sull'accesso alle immagini di un sistema di videosorveglianza, potrà chiedere il parere del DPO.

In secondo luogo, i dipendenti devono essere consapevoli del fatto che il DPO debba essere prontamente coinvolto in tutte le questioni relative al trattamento di dati personali, e debba sorvegliare sul rispetto delle norme e dei principi del GDPR. Questa sorveglianza (fondamentale nell'ottica dell'accountability) deve essere resa effettiva anche e soprattutto con la cooperazione di tutti i dipendenti, che trattano dati personali, e con la previsione di idonei flussi informativi che consentano al DPO di esercitare i propri compiti in maniera efficace.

## 2.5. REGISTRI DELLE ATTIVITÀ DI TRATTAMENTO

Tra gli obblighi ai quali il titolare del trattamento e il responsabile del trattamento sono soggetti in base al GDPR spicca senza dubbio quello relativo alla tenuta dei registri delle attività di trattamento. L'art. 30, a essi dedicato, indica analiticamente quali informazioni debbano essere contenute nei registri, tra le quali ricordiamo:

→ Il nome e i dati di contatto del titolare del trattamento (o del responsabile) e quelli del DPO;
→ La finalità del trattamento (non prevista per il responsabile per ovvie ragioni);
→ Una descrizione delle categorie di interessati e dei dati personali trattati;
→ I trasferimenti di dati verso Paesi terzi;
→ I termini ultimi previsti per la cancellazione dei dati (ove possibile); e infine,
→ Una descrizione generale delle misure di sicurezza adottate a tutela dei dati.

Le informazioni individuate dall'art. 30 rappresentano il contenuto minimale dei registri, ma nulla vieta al titolare (e al responsabile), nella propria autonomia, di inserire ulteriori contenuti, che siano funzionali alla corretta gestione dei trattamenti. Può essere utile il confronto con i modelli di registro che sono già stati rilasciati da alcune Autorità di controllo, tra cui l'Autorità Belga[18].

I registri delle attività di trattamento devono essere tenuti in forma scritta, anche in formato elettronico (quest'ultima modalità di tenuta può rivelarsi particolarmente utile per realtà complesse e strutturate - si pensi all'implementazione o aggiornamento di dati).

[17] Il Garante ha già messo a disposizione un modulo per tale comunicazione --- http://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7322292.
[18] https://www.privacycommission.be/fr/canevas-de-registre-des-activites-de-traitement.

Sono esonerati dall'obbligo di tenuta di tali registri le imprese e le associazioni con meno di 250 dipendenti, a meno che il trattamento effettuato possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o riguardi le categorie particolari di dati (i "dati sensibili" del Codice Privacy) o dati relativi a condanne penali o reati.

L'importanza della tenuta dei registri delle attività di trattamento è da inquadrare nell'ottica generale di accountability ed è strettamente connessa alla tutela del dato personale. Lo strumento è fondamentale infatti per i titolari e i responsabili che vogliano dimostrare la conformità dei trattamenti a quanto previsto dal legislatore comunitario ed è indispensabile nell'attività di cooperazione con l'autorità di controllo (la quale potrà pertanto chiedere che detti registri vengano messi a disposizione su richiesta). Non è da sottovalutare, infine, che accanto al valore prettamente probatorio, la tenuta dei registri è altresì un utile strumento per la gestione e il monitoraggio del "ciclo di vita" dei dati personali trattati.

È quindi fondamentale porre la massima attenzione non soltanto alla redazione iniziale del registro dei trattamenti, ma anche alla sua alimentazione e aggiornamento.

# 3. LA SICUREZZA INFORMATICA E IL TRATTAMENTO DEI DATI PERSONALI

## 3.1. DATA PROTECTION "BY DESIGN" E "BY DEFAULT"

I concetti di protezione dei dati "by design" e "by default" (nella versione italiana "protezione dei dati fin dalla progettazione" e "protezione per impostazione predefinita"), contemplati dall'art. 25 del GDPR, sono espressione del principio di minimizzazione del trattamento, ossia di quel principio in base al quale il trattamento deve limitarsi ai soli dati personali necessari al soddisfacimento dello scopo legittimo per cui i dati personali siano, volta per volta, trattati. Si tratta di due importanti presidi a tutela del corretto trattamento dei dati personali, che devono iniziare a fare parte del bagaglio di cognizioni di chiunque debba realizzare - e utilizzare - sistemi destinati al trattamento di dati personali.

Per quanto riguarda la privacy by design, il GDPR prevede che l'adeguatezza delle misure (quali ad esempio la pseudonimizzazione, che abbiamo già esaminato) tecniche e organizzative (necessarie ad attuare in modo efficace i principi di protezione dei dati e integrare nel trattamento le necessarie garanzie per soddisfare il rispetto del regolamento oltre che tutelare i diritti degli interessati) debba essere attentamente considerata sia al momento di individuare gli strumenti attraverso i quali i dati saranno trattati, sia all'atto del trattamento stesso. I parametri che il titolare o il responsabile devono valutare al fine della individuazione delle misure tecniche e organizzative più adeguate al caso di specie sono: stato dell'arte e i costi di attuazione; natura, ambito di applicazione, contesto e finalità del trattamento; nonché i rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

La privacy by default consiste nella predisposizione di misure tecniche e organizzative adeguate, in modo da garantire che, per impostazione predefinita, vengano trattati soltanto i dati necessari per ogni specifica finalità del trattamento. L'obbligo si estende alla quantità dei dati personali raccolti, alla portata del trattamento, al periodo di conservazione e all'accessibilità. In particolare, dette misure devono garantire che, per impostazione predefinita, i dati personali non siano resi accessibili a un numero indefinito di soggetti, senza l'intervento di una persona fisica. In altre parole, i sistemi devono essere configurati in modo da trattare soltanto i dati strettamente necessari, e in maniera tale da non essere diffusi automaticamente, se non in forza di un intervento umano.

Anche in questo ambito si può notare il rilievo centrale che assume il concetto di accountability (o responsabilizzazione). Il GDPR, infatti, non descrive analiticamente le misure tecniche e organizzative che titolare e responsabile devono adottare, ma ne indica alcune (come, a esempio, la pseudonimizzazione o la cifratura) che il titolare o il responsabile potrebbero - valutati i rischi che incombono, volta per volta, sui dati personali oggetto di trattamento; lo stato dell'arte delle misure tecniche e organizzative disponibili; i costi di attuazione delle misure; la natura, ambito di applicazione, contesto e finalità del trattamento - caso per caso stabilire come "adeguate" al trattamento eseguito.

Ovviamente, come tutte le norme che hanno l'obiettivo di prevenire un rischio, anche il GDPR è ben consapevole della impossibilità di assicurare una sicurezza assoluta dei dati personali contro la miriade di rischi che sul loro trattamento incombe. Ciò nonostante, la disciplina è orientata a far sì che ai dati personali, in qualsiasi fase del loro trattamento, siano assicurate le migliori cautele per evitare, attenuare o ridurre il rischio di un trattamento illecito.

## 3.2. LA VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)

Il GDPR individua nel titolare del trattamento il soggetto su cui incombe il compito di individuare le più adeguate misure tecniche e organizzative al fine di garantire il rispetto della disciplina e dei principi in materia di trattamento di dati personali. Nell'impianto del Regolamento, dunque, la responsabilizzazione del titolare è centrale, mentre l'intervento (autorizzatorio o di controllo) dell'Autorità Garante si inserisce in genere in una fase successiva o eventuale. E, a questo principio non fanno eccezione la valutazione d'impatto sulla protezione dei dati e la consultazione preventiva.

La valutazione d'impatto sulla protezione dei dati (DPIA[19]) è un processo che ha la funzione di descrivere un trattamento di dati personali, valutarne la necessità e la proporzionalità, nonché contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti da esso, valutando detti rischi e determinando le misure per affrontarli.

### *3.2.1. Quando è necessaria*

La DPIA è un adempimento che non va posto in essere sempre e comunque, ma deve essere preventivamente effettuato in specifiche ipotesi, previste dal GDPR e in particolare quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Ancora una volta, dunque, è il rischio a essere centrale, e per la valutazione se tale rischio sia elevato o meno, si possono applicare i criteri individuati nelle specifiche linee guida dell'"Art. 29 Working Party"[20].

Nelle Linee guida, si identificano nove fattori rilevanti, per operare tale valutazione:

1. Valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di "*aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato*";
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente;
3. Monitoraggio sistematico;
4. Dati sensibili o dati aventi carattere altamente personale;
5. Trattamento di dati su larga scala;
6. Creazione di corrispondenze o combinazione di insiemi di dati, ad esempio a partire da dati derivanti da due o più operazioni di trattamento svolte per finalità diverse e/o da titolari del trattamento diversi secondo una modalità che va oltre le ragionevoli aspettative dell'interessato;

[19] Acronimo di "Data Protection Impact Assessment".

[20] http://194.242.234.211/documents/10160/0/WP+248+--+Linee-guida+concernenti+valutazione+impatto+sulla+protezione+dati.

7. Dati relativi a interessati vulnerabili (es. minori);
8. Uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative;
9. Quando il trattamento in sé "*impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto*".

Se sussistono almeno due tra questi fattori (la cd. "regola del due") allora, secondo le Linee guida, diventa necessario effettuare la valutazione d'impatto.

Oltre a questa ipotesi generale, il GDPR individua tre ipotesi specifiche, per le quali la valutazione è richiesta. Tali ipotesi sono:

1. Una 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 sulle persone stesse;
2. Il trattamento, su larga scala, di categorie particolari di dati personali (dati sensibili e dati biometrici), o di dati relativi a condanne penali e a reati;
3. La sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Il Garante dovrà rendere pubblico un elenco di trattamenti per i quali si renderà necessaria la valutazione d'impatto, e potrà anche redigere un elenco che, in negativo, individui le tipologie di trattamento per le quali non sarà richiesta alcuna valutazione. Ulteriori eccezioni sono previste per le ipotesi in cui un trattamento sia effettuato per adempiere a un obbligo legale, ovvero sia necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, abbia una base giuridica nel diritto dell'Unione o nel diritto interno di uno Stato membro, sia disciplinato il trattamento specifico e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nel contesto dell'adozione di tale base giuridica.

Non saranno probabilmente molte le ipotesi (salvi casi particolari) nei quali gli enti pubblici saranno tenuti a svolgere una valutazione d'impatto privacy, ma comunque la prassi applicativa, e soprattutto la pubblicazione degli elenchi da parte dell'Autorità garante, potranno fugare futuri dubbi.

Non è però da escludere che, visto il costante e continuo progresso tecnologico, ci si debba confrontare con una valutazione d'impatto: si pensi, ad esempio, all'introduzione da parte del MIUR o di un USR, di sistemi biometrici (scansione dell'impronta digitale o dell'iride) per il controllo delle presenze dei dipendenti. L'introduzione di tali sistemi, che prima sarebbe stata soggetta alla verifica preliminare da parte del Garante, ai sensi dell'art. 17 del Codice Privacy[21], renderebbe adesso necessaria la valutazione d'impatto da parte del titolare del trattamento.

Per fare un altro esempio, si potrebbe pensare all'Anagrafe nazionale degli studenti, la cui normazione secondaria è stata recentemente soggetta a riordino con il Decreto del MIUR n. 692 del 25 settembre 2017. Essa costituisce certamente un trattamento su larga scala, che riguarda anche soggetti minori, e che contiene, sia pure in una partizione separata, i dati indispensabili a rivelare lo stato di disabilità degli alunni.

[21] L'uso della biometria, a esempio, nell'ambito pubblico, era stata oggetto di alcuni provvedimenti da parte del Garante - http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/2641563.

Ragionando in termini generali, sembrerebbero sussistere tutti i requisiti perché questo trattamento debba essere soggetto a una valutazione d'impatto sulla protezione dei dati. Esso però trova il suo fondamento in una base giuridica, che disciplina anche il trattamento specifico, e gli atti di normazione secondaria sono stati soggetti anche a plurimi pareri da parte dell'Autorità Garante. Si potrebbe dunque ritenere che rientri in una delle eccezioni previste dall'art. 35 del GDPR. Anche in questo caso, però, il Regolamento lascia un margine alla normativa nazionale (che, come abbiamo visto, non è ancora intervenuta).

Il contenuto e la procedura della valutazione sono disciplinate dall'art. 35 del GDPR, e possono essere così sintetizzati:

→ Descrizione del trattamento previsto;
→ Valutazione della necessità e della proporzionalità;
→ Misure previste per dimostrare la conformità;
→ Valutazione dei rischi per i diritti e le libertà;
→ Misure previste per affrontare i rischi;
→ Documentazione;
→ Monitoraggio e riesame.

Sul punto possono essere molto utili anche le recenti "*Guidelines for privacy impact assessment*", contenute nello standard ISO/IEC 29134:2017.

Qualora la valutazione d'impatto indichi che il trattamento presenti un rischio residuo elevato, e dunque le misure adottate dal titolare del trattamento per attenuare il rischio non siano sufficienti, allora si dovrà procedere alla consultazione preventiva con l'Autorità Garante, secondo il procedimento delineato dall'art. 36 del GDPR.

## 3.3. SICUREZZA INFORMATICA NEL TRATTAMENTO DEI DATI PERSONALI

Tutte le pubbliche amministrazioni vivono oggi in una dimensione digitale in cui l'intera azione amministrativa, le informazioni, i documenti e i dati trattati si caratterizzano, appunto, per una gestione digitale dall'inizio alla fine. Lo stesso documento amministrativo, quindi, nasce come originale informatico, viene sottoscritto digitalmente, viene trasmesso telematicamente, viene trattato con gli strumenti informatici e viene, infine, conservato digitalmente. Il passaggio dalla dimensione cartacea alla dimensione digitale, inoltre, ha comportato una serie di necessari adattamenti per far fronte ai nuovi rischi e adattarsi a quelli che esistevano anche nella "dimensione cartacea".

L'azione della PA è, pertanto, orientata a garantire - sia pur nelle varie declinazioni e peculiarità - che le informazioni siano trattate nel rispetto delle norme dell'agire amministrativo. Esigenza primaria è, quindi, quella di garantire che dati, documenti e informazioni siano trattati assicurandone - ove richiesto - disponibilità, confidenzialità e integrità. Questi tre elementi rappresentano il fulcro e l'obiettivo della sicurezza. Ovviamente i rischi che incombono sulla sicurezza dei dati trattati variano anche con il variare degli strumenti utilizzati per il medesimo trattamento: i rischi che incombono sui dati trattati dalla PA in una dimensione cartacea differiscono, per molti aspetti, rispetto ai rischi che incombono sui medesimi dati trattati, però, in una dimensione digitale.

È per questo motivo che il tema della sicurezza informatica riveste un'importanza fondamentale e strategica affinché la Pubblica Amministrazione possa operare correttamente e senza soluzione di continuità. E ciò è ancor più evidente e stringente se si considera il costante aumento delle violazioni (più o meno rilevanti) ai sistemi informatici o le perdite di dati e informazioni dovute a comportamenti negligenti o imprudenti dei dipendenti pubblici o, ancora, a malfunzionamenti dei sistemi informatici o telematici. In tal modo può certamente constatarsi un incremento, costante nel tempo, dei rischi che incombono sulle informazioni della Pubblica Amministrazione (ma che interessano - quasi indistintamente - oltre che le pubbliche amministrazioni anche privati e aziende).

Con il GDPR si assiste a un netto cambio di prospettiva che riguarda, innanzitutto, una presa di coscienza della inutilità della predisposizione di un catalogo di misure minime di sicurezza. È proprio per tale motivo che il fuoco dell'attenzione viene spostato sull'esigenza di avere una rinnovata responsabilizzazione degli attori principali del trattamento dei dati personali (titolare e responsabile del trattamento), costringendoli a prendere effettiva cognizione della necessità di attivarsi concretamente per garantire una efficace protezione dei dati personali che non sia più limitata a un asettico recepimento di una serie di obblighi preconfezionati di sicurezza (leggasi: misure minime di sicurezza).

Con il GDPR, in pratica, occorre prestare maggiore attenzione sulla sicurezza ragionata ed efficace, abbandonando così quella meramente apparente. Questo cambio di direzione è da ricondursi essenzialmente, come già accennato, alla evoluzione tecnologica (e va di pari passo rispetto ai rischi incombenti sui dati in considerazione del sempre più diffuso utilizzo degli strumenti informatici), nel periodo ultraventennale che separa la precedente direttiva privacy dal GDPR.

Ed è proprio per questo motivo che la sicurezza informatica - in quanto materia fluida e in costante evoluzione - è elemento essenziale al rispetto della disciplina del GDPR. La sicurezza informatica, infatti, ha lo scopo di minimizzare i rischi che incombono sulle informazioni digitali (non solo sui dati personali in essi contenuti) andando a perseguire il raggiungimento di tre obiettivi: la confidenzialità, l'integrità e la disponibilità delle informazioni. La triade composta da confidenzialità, integrità e disponibilità delle informazioni (in inglese indicata con l'acronimo CIA, per *Confidentiality, Integrity* e *Availability*) rappresenta, quindi, il fulcro della sicurezza.

La "confidenzialità" si riferisce a quell'insieme di regole che consentono di mantenere il controllo sull'accesso a determinate informazioni escludendo i soggetti non legittimati. Con il concetto di "integrità", invece, ci si riferisce alle regole finalizzate a far sì che le informazioni i dati e documenti siano trattati in modo da prevedere, prevenire e ripristinare i sistemi informatici a seguito di eventi accidentali o volontari in grado di compromettere o alterare indebitamente i sistemi o i dati in esso contenuti. La "disponibilità", infine, si riferisce alle regole e agli accorgimenti attraverso i quali mantenere i sistemi informatici e telematici costantemente operativi, affidabili, funzionali e accessibili.

### *3.3.1. Dalle misure di sicurezza minime e idonee alle misure adeguate tecniche e organizzative*

Si è già osservato che con il GDPR si abbandonano definitivamente quelle che, nella vigenza del Codice della Privacy, erano definite le "misure minime di sicurezza" (previste dagli articoli 33 e seguenti del Codice) e che consistevano in un numero chiuso di misure che il titolare del trattamento doveva necessariamente adottare per garantire un livello minimo di protezione ai dati

personali. L'insieme delle misure minime era racchiuso nel disciplinare tecnico, il cosiddetto "Allegato B" al Codice della Privacy.

Accanto alle "misure minime", il Codice della Privacy prevedeva le "misure idonee" (art. 31 del Codice) che, a differenza delle prime, non erano racchiuse in un numero chiuso e alla loro violazione non conseguiva una sanzione penale ma, eventualmente, una responsabilità di tipo risarcitorio. In modo analogo a quanto avviene con le misure adeguate di sicurezza previste dal GDPR, le misure "idonee" del Codice devono essere individuate dal titolare sulla base di alcuni fattori precisi: il progresso tecnico, la natura dei dati e le specifiche caratteristiche del trattamento. Si può osservare, tuttavia, che le misure "adeguate" previste dal GDPR non limitano il loro ambito di applicazione agli aspetti tecnici ma si estendono anche agli aspetti organizzativi del titolare o del responsabile del trattamento. In altri termini, le misure adeguate del GDPR hanno un ambito applicativo ben più ampio rispetto a quello delle misure idonee di sicurezza che erano previste dal Codice.

Ciò che il GDPR prevede debba valutarsi, in una continua attività di ricerca e di adattamento e adeguamento, al fine di individuare le misure tecniche e organizzative adeguate (art. 32 del GDPR) al rischio incombente sui dati personali trattati da titolare o responsabile, sono i seguenti elementi:

→ Stato dell'arte e costi di attuazione delle misure;
→ Natura, oggetto, contesto e finalità del trattamento;
→ Rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

L'art. 32 del GDPR, inoltre, individua, a titolo chiaramente esemplificativo, alcune misure che il titolare o il responsabile possono dover adottare nel loro approccio al rischio. Queste misure (che non rappresentano esaustivamente le misure che gli obbligati possono dover, volta per volta, prendere in considerazione) sono:

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

Considerando che la finalità ultima nell'approntare le misure adeguate tecniche e organizzative è quella di garantire confidenzialità, integrità e disponibilità dei dati personali trattati, allora si comprende come questa attività non possa essere limitata al momento iniziale (ossia a quello della loro implementazione), ma si debbano costantemente testare e verificare anche in considerazione delle mutevoli "condizioni tecnologiche" (ad esempio nel momento in cui venga individuata una qualche vulnerabilità al software utilizzato per il trattamento dei dati personali) e organizzative (al mutare del personale, delle mansioni o - in genere - dell'organigramma ci si dovrà preoccupare di testare la "tenuta" del sistema di gestione del rischio che incombe sui dati personali).

L'adesione a codici di condotta o a meccanismi di certificazione (che devono essere approvati secondo le modalità previste dal GDPR), possono essere utilizzati per dimostrare l'adempimento dell'obbligo di sicurezza.

L'obbligo di sicurezza, inoltre, comporta la necessità di considerare anche un altro fattore di rischio: il fattore umano. In base al GDPR, infatti, il titolare e il responsabile hanno l'onere di assicurarsi che tutte le persone che trattano dati personali per loro conto, lo facciano attenendosi alle istruzioni del titolare stesso[22]. In altre parole, anche sotto la vigenza del GDPR, spetta al titolare (e al responsabile) verificare che soltanto soggetti specificatamente incaricati e istruiti (autorizzati) possano trattare i dati personali, e che gli stessi si attengano alle istruzioni ricevute.

Per individuare quali siano in concreto le misure (tecniche e organizzative) "adeguate" possono essere di supporto le norme e gli standard internazionali (ad esempio la norma UNI CEI ISO/IEC 27001:2014 – Tecnologie informatiche – Tecniche per la sicurezza – Sistemi di gestione per la sicurezza delle informazioni – Requisiti - traduzione della ISO 27001/2013), che individuano proprio i presupposti per adottare, attuare, mantenere e migliorare in modo continuo un sistema di gestione per la sicurezza delle informazioni all'interno di un'organizzazione, comprendendo anche i requisiti per valutare e trattare i rischi concernenti la sicurezza delle informazioni, adattati alle peculiarità dell'organizzazione stessa.

Può risultare utile, in tal senso, anche una corretta implementazione dei "controlli essenziali di cybersecurity" individuati dal Research Center of Cyber Intelligence and Information Security dell'Università La Sapienza di Roma, del Laboratorio Nazionale CINI (Consorzio Interuniversitario Nazionale per l'Informatica) nel recente documento "2016 Italian Cybersecurity Report - Controlli Essenziali di Cybersecurity".

[22] Salvo dove diversamente disposto dal diritto dell'Unione o degli Stati membri --- si pensi per esempio a un dipendente che debba comunicare dei dati all'autorità giudiziaria o alla polizia giudiziaria.

### *3.3.2. Rapporti tra GDPR e Direttiva (UE) 2016/1148 in ambito di sicurezza informatica e data breach*

Con la Direttiva 2016/1148, detta anche Direttiva NIS[23] (Network and Information Security) nel 2016 si introduce, a livello europeo, un nuovo tipo di approccio globale in materia di cyber-security. Gli scopi della direttiva NIS sono quelli di: (A) migliorare le capacità, da parte dei settori strategici (operatori di servizi essenziali e fornitori di servizi digitali), di affrontare i rischi derivanti dall'uso delle tecnologie; (B) predisporre e attuare un'effettiva cooperazione tra gli Stati Membri sul tema della sicurezza informatica; e, (C) imporre ai settori critici l'impiego di misure effettive (oltre all'obbligo di segnalazione delle violazioni più rilevanti) sotto il punto di vista informatico e telematico.

La direttiva, in particolare, si rivolge a due categorie di soggetti:

→ Operatori di servizi essenziali[24];

→ Fornitori di servizi digitali[25].

È importante rilevare che, in base all'art. 5, comma 3, della Direttiva NIS, ogni Paese membro dovrà, con il recepimento (che deve avvenire entro il 9 maggio 2018) della direttiva in questione, istituire un elenco dei servizi essenziali per il mantenimento di attività sociali e/o economiche fondamentali. È possibile, pertanto, che svariati sistemi informatici pubblici vengano ricompresi, dalla legge di recepimento della Direttiva NIS, tra i servizi essenziali e, quindi, si estendano anche a esse gli obblighi previsti dalla medesima Direttiva. Lo scorso 8 febbraio 2018 il Consiglio dei Ministri ha approvato, in esame preliminare, lo schema di decreto legislativo di recepimento della Direttiva NIS il cui testo[26], al momento[27], non è stato ancora pubblicato in Gazzetta Ufficiale. In questo testo si evidenzia che "*il trattamento dei dati personali in applicazione del presente decreto è effettuato ai sensi del decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni*". Ciò significa che tutte le disposizioni che il decreto di recepimento della Direttiva NIS dovesse introdurre dovrebbero comunque armonizzarsi con il GDPR nel senso di ritenere comunque applicabili le norme del GDPR.

In ogni caso l'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, con un documento del 13 settembre 2017[28], consiglia da un lato di applicare le stesse regole previste dalla Direttiva NIS a tutte le amministrazioni pubbliche, "*considerato il loro ruolo nella società e*

[23] Ossia la direttiva (UE) 2016/1148, adottata il 6 luglio 2016 e in vigore dall'8 agosto dello stesso anno.

[24] Sono essenziali (ai sensi dell'allegato 2 della Direttiva NIS) i servizi dei settori energia, trasporti, bancario, infrastrutture dei mercati finanziari, sanitario e di fornitura e distribuzione di acqua potabile. Le categorie sono soggette a un ulteriore incremento da parte degli Stati membri, i quali potranno istituire un elenco dei servizi ritenuti essenziali sulla base dei criteri previsti dall'art. 5 della medesima direttiva.

[25] Sono definiti, invece, fornitori di servizi digitali qualsiasi persona giuridica che fornisca un servizio digitale, ossia qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi ovvero un servizio di mercato online, motore di ricerca online o di cloud computing.

[26] http://documenti.camera.it/apps/nuovosito/attigoverno/Schedalavori/getTesto.ashx?file=0520.pdf&leg=XVII#pagemode=none.

[27] 12 aprile 2018.

[28] https://ec.europa.eu/transparency/regdoc/rep/10101/2017/EN/JOIN-2017-450-F1-EN-MAIN-PART-1.PDF.

*nell'economia*", e dall'altro di erogare una formazione specifica, alle pubbliche amministrazioni, sui temi della sicurezza informatica.

Gli obblighi previsti dalla Direttiva NIS si dividono in due categorie principali:

1) Obbligo di adozione di "*misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi*"; e,
2) Obbligo di notificare, senza ritardo, all'autorità competente (individuata nella legge di recepimento) o al CSIRT[29] gli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali prestati.

Per quanto riguarda, in particolare, l'obbligo di notifica degli incidenti ("incident report") si deve considerare che un analogo tipo di segnalazione è già prevista, in Italia - anche per soggetti non espressamente ricompresi tra i destinatari designati dalla Direttiva NIS - in virtù della circolare n. 2/2017 dell'AgID e, per quanto ci riguarda, del Regolamento europeo n. 2016/679 che, come detto, disciplina i "*data breach*" che coinvolgano dati personali. Si può osservare, pertanto, che tutti i procedimenti di gestione del rischio informatico e i tipi di cautela volta per volta individuati dalle norme in tema di prevenzione del rischio seguono costantemente misure analoghe e parametrate a quelle che possiamo definire le "*best practices*" (migliori pratiche) nell'ambito della sicurezza informatica.

### *3.3.3. Profili di sicurezza informatica*

Per concludere, la sicurezza è un processo in continua evoluzione e adeguamento, che deve tenere in considerazione quantomeno i seguenti elementi:

1. L'analisi del rischio (fatta in considerazione del fatto che le misure di sicurezza sono individuate sulla scorta dello stato dell'arte e dei costi d'attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento);
2. La valutazione del rischio (sia in ordine alla gravità dei rischi che alla probabilità della loro verificazione);
3. L'individuazione delle misure adeguate (anche in relazione a quelle indicate, a titolo esemplificativo, dall'art. 32 del GDPR);
4. Le istruzioni ai soggetti che trattino i dati personali per conto del titolare (o del responsabile) e secondo le sue istruzioni (in modo che i soggetti non espressamente autorizzati non siano in grado di effettuare alcuna operazione);
5. Il monitoraggio e la valutazione dell'adeguato livello di sicurezza (che deve considerare i rischi di distruzione, perdita, modifica, divulgazione non autorizzata, accesso accidentale o illegale, in tutte le fasi del trattamento, compresa trasmissione e conservazione);
6. L'implementazione di azioni correttive.

[29] Gruppi di intervento per la sicurezza informatica in caso di incidente (Computer Security Incident Response Team) che, in Italia, è rappresentato da CERT-PA (Computer Emergency Response Team Pubblica Amministrazione) - www.cert-pa.it.

### *3.3.4. La cifratura*

Una delle tecniche più efficaci da impiegare per evitare gli accessi indebiti (e l'eventuale diffusione illecita degli stessi) è rappresentata dall'uso della cifratura. Attraverso l'uso di tecniche di cifratura dei dati si assicura l'accesso ai dati contenuti nel supporto di memorizzazione esclusivamente ai soggetti legittimati e in possesso delle relative credenziali di autenticazione (password, autenticazione biometrica o altro), necessarie per decifrare i contenuti in questione.

L'utilizzo della cifratura era già prevista quale misura minima di sicurezza dall'allegato B del D.Lgs. 196/03 nel punto in cui prevedeva che gli organismi sanitari e gli esercenti le professioni sanitarie dovessero effettuare il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità tali da minimizzare il trattamento, ossia trattare disgiuntamente tali tipi di dati rispetto alle altre informazioni personali che consentissero di identificare direttamente gli interessati. In particolare si prevedeva che nei casi in cui tali dati personali, in formato elettronico, dovessero essere trasportati all'esterno dei locali riservati al loro trattamento i dati medesimi dovessero essere cifrati. In tal modo, anche in caso di smarrimento o furto del supporto di memorizzazione portatile. Le informazioni necessarie a individuare le modalità di cifratura dei dati potranno essere contenute tra le istruzioni organizzative interne che il titolare o il responsabile fornisce ai soggetti autorizzati a trattare i dati personali per conto del titolare o dell'interessato.

### *3.3.5. Il ripristino dei dati in caso di incidente*

Le operazioni di backup nella vigenza del D.Lgs. 196/03 rappresentavano una misura minima atta a contrastare le ipotesi di perdita o alterazione (per qualsivoglia ragione) dei dati contenuti in un sistema informatico. Il backup consiste, infatti, nella memorizzazione di una copia di sicurezza del supporto da preservare. Nelle ipotesi in cui il sistema originario dovesse essere compromesso o alterato sarebbe possibile, in base alla copia di backup, ripristinare il medesimo sistema allo stato in cui si trovava al momento in cui era stata estratta la copia di backup.

Tale misura anche con il GDPR ha una sua importanza centrale. L'art. 32 del GDPR, infatti, impone a titolare e responsabile di individuare, tra le misure tecniche e organizzative adeguate, anche quelle che abbiano lo scopo e la capacità di "*ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico*". Il procedimento di backup rappresenta, pertanto, una delle misure di prevenzione (posto che deve essere eseguita prima del verificarsi di un disastro informatico e, nel caso in cui la violazione si manifesti, consente di ripristinare il sistema) più efficaci e diffuse. Con il procedimento di backup, quindi, il titolare assicura la possibilità che un computer compromesso possa essere ripristinato mediante la copia di backup. Per tale ragione è importante che le copie di backup siano regolarmente eseguite e - in genere effettuate a intervalli non inferiori a una settimana.

Ovviamente, affinché un sistema di backup possa dirsi efficace, dovrebbe prevedere:

1. La conservazione dei backup in un luogo sicuro e distinto dal supporto originario (nel caso in cui, ad esempio, scoppiasse un incendio nell'aula contenente sia il sistema informatico che il suo backup, andrebbero irrimediabilmente perdute tutte le informazioni);
2. La verifica periodica dei dati di backup (occorre considerare, infatti, che i supporti di memorizzazione dei backup potrebbero essere esposti essi stessi a danneggiamenti, eventi catastrofici o, comunque, deterioramento).

## 3.4. NOTIFICA IN CASO DI VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

La notificazione e comunicazione delle violazioni dei dati personali, prevista dagli artt. 33 e 34 del GDPR, non è in realtà una novità assoluta[30]: il Codice della Privacy disciplina già le comunicazioni dei *data breach* riguardanti i fornitori di servizi telefonici e di accesso a Internet e ci sono altre due ipotesi, previste da specifici provvedimenti del Garante. Il primo provvedimento [31] riguarda l'obbligo (sia per gli enti privati che per quelli pubblici) di comunicare al Garante, entro ventiquattr'ore dalla conoscenza del fatto, tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui sistemi biometrici installati o sui dati personali custoditi.

Il secondo provvedimento [32] , pubblicato nel 2015, riguarda invece soltanto le pubbliche amministrazioni, e prevede che esse siano tenute, entro 48 ore dalla conoscenza del fatto, a comunicare al Garante (mediante uno specifico modello, allegato al provvedimento) tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali contenuti nelle proprie banche dati.

Se dunque l'istituto non è una novità, il GDPR prevede comunque una disciplina più specifica, introducendo un obbligo sostanzialmente generalizzato di notificazione al Garante, e, soprattutto, un obbligo (a determinate condizioni) di comunicazione delle violazioni agli interessati.

### *3.4.1. Riconoscere la natura del data breach*

Il GDPR introduce (nell'art. 4, par. 12), la definizione di violazione dei dati, come "*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*". La disciplina del *data breach*, pur essendo inquadrabile nell'ambito del *risk management*, riguarda chiaramente la gestione ex post degli eventi pregiudizievoli. In altre parole, mentre finora gli adempimenti esaminati riguardavano la gestione e minimizzazione del rischio di eventuali violazioni, il *data breach* parte dal presupposto che una violazione si sia già verificata, e si occupa di attivare le contro-misure finalizzate a minimizzarne le conseguenze.

Il *data breach*, per definizione, consiste in una qualsiasi violazione che vada a incidere sugli aspetti della confidenzialità, integrità o disponibilità dei dati personali.

Si deve considerare il fatto in sé, indipendentemente dalla sua imputabilità, o dalle sue cause. È irrilevante, ai fini dell'obbligo di notificazione o comunicazione, che l'evento sia imputabile ad azioni di terzi (ad esempio un criminale informatico che abbia violato i sistemi dell'ente o della società) o sia invece meramente accidentale (si pensi allo smarrimento di un supporto usb, oppure a un evento naturale che comporti la distruzione degli strumenti informatici). È dunque la mera violazione di sicurezza a generare, unitamente agli altri requisiti che andremo ad analizzare, l'applicabilità degli obblighi di cui agli artt. 33 e 34 del GDPR.

---

[30] Il Garante ha elaborato una sintetica ma precisa infografica, reperibile su http://194.242.234.211/documents/10160/0/Violazioni+di+dati+personali+-+Gli+adempimenti+previsti+%28infografica%29.pdf.

[31] Provvedimento n. 513 del 12 novembre 2014.

[32] Provvedimento n. 392 del 2 luglio 2015.

L'art. 29 Working Party ha rilasciato delle Linee Guida sulla notificazione in caso di violazione dei dati personali[33], linee guida che sono state recentemente aggiornate.

### *3.4.2. Notifica all'Autorità di controllo*

L'obbligo di notifica al Garante è previsto in tutte le ipotesi di violazione dei dati personali, salvo qualora sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche. Solo in quest'ultimo caso non occorre procedere alla notifica. Per fare un esempio, può pensarsi allo smarrimento (o alla sottrazione) di un computer, uno smartphone o un supporto usb. Laddove questi supporti contengano dati personali, e non siano protetti da idonea cifratura, saremo certamente di fronte a un *data breach*. Qualora al contrario i sistemi (o i supporti) siano adeguatamente cifrati, allora si potrà eventualmente ritenere improbabile la sussistenza di rischio.

La notifica deve essere effettuata senza ingiustificato ritardo, e comunque entro settantadue ore dal momento in cui si è venuti a conoscenza della violazione. Se la notifica non è tempestiva, occorre esplicitare i motivi del ritardo.

La norma prevede anche che il responsabile del trattamento informi il titolare "*senza ingiustificato ritardo*" e individui il contenuto minimo della notifica stessa, che deve contenere:

A. La descrizione della natura della violazione, compresi, ove possibile, le categorie e il numero approssimativo di interessati nonché le categorie e il numero approssimativo di record coinvolti;
B. La comunicazione del nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
C. La descrizione delle probabili conseguenze della violazione;
D. La descrizione delle misure adottate (o di cui si propone l'adozione) per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

Laddove non sia possibile fornire tutte le informazioni contestualmente, le stesse possono essere anche fornite in fasi successive, ma sempre senza ulteriore ingiustificato ritardo.

Vi è, infine, un ulteriore onere a carico del titolare, il quale deve documentare qualsiasi violazione di dati personali, ivi comprese le circostanze, le conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione è finalizzata alla verifica della *compliance* da parte dell'autorità di controllo (e dunque del Garante).

Il termine per la notificazione è dunque brevissimo (settantadue ore dalla scoperta) e ciò impone alle pubbliche amministrazioni di adottare, entro il venticinque maggio, quantomeno due importanti cautele: in primo luogo la messa in atto di adeguate procedure informatiche e organizzative per la tempestiva scoperta, e per l'immediata raccolta delle informazioni a seguito delle violazioni di sicurezza, e in secondo luogo specifiche istruzioni a tutti i dipendenti, in ordine alla sussistenza di questo nuovo obbligo, e alle responsabilità conseguenti.

[33] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

### *3.4.3. Ipotesi di comunicazione agli interessati*

All'obbligo di notifica al Garante l'art. 34 del GDPR aggiunge (e questa è una novità assoluta per le pubbliche amministrazioni) l'obbligo della comunicazione del *data breach* anche all'interessato solamente nei casi in cui la violazione dei dati personali rappresenti un rischio elevato per i diritti e le libertà delle persone fisiche. La comunicazione è da effettuarsi "*senza ingiustificato ritardo*", e deve descrivere la natura della violazione con un linguaggio chiaro e preciso.

Anche in questo caso la comunicazione (che deve essere finalizzata al *data breach* e non inserita, ad esempio, in una newsletter o in altre comunicazioni periodiche) ha un contenuto minimo, costituito (oltre che dalla descrizione della natura della violazione) da:

A. Nome e dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
B. Descrizione delle probabili conseguenze della violazione;
C. Descrizione delle misure adottate (o di cui si propone l'adozione) per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

Questa comunicazione non deve però essere sempre effettuata, e infatti essa può essere omessa qualora:

→ Il titolare ha messo in atto misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare laddove siano state implementate quelle misure destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
→ Il titolare ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
→ La comunicazione richiederebbe sforzi sproporzionati. In quest'ultimo caso si deve comunque procedere a una comunicazione pubblica o altra misura simile.

La comunicazione può essere anche richiesta dall'Autorità Garante, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato.

Questi obblighi impongono comunque particolare attenzione, e l'adozione di strumenti capaci non solo di prevenire ma anche di rilevare le violazioni di dati personali e di acquisire tutte le informazioni necessarie, in modo da essere in grado, nei tempi stretti imposti dalle norme, di approntare in maniera corretta la notifica e, se del caso, la comunicazione agli interessati. E, in ogni caso, tutte le attività vanno scrupolosamente documentate, se del caso istituendo (pur non essendo un obbligo) un registro delle violazioni, ove documentare tutti gli eventi, comprese quelle violazioni di sicurezza che si è ritenuto di non notificare o non comunicare.

# 3.5. PROTEZIONE DEI DATI PERSONALI E TRASPARENZA AMMINISTRATIVA

### *3.5.1. Il rapporto tra trattamento di dati personali e pubblicazioni online*

Le pubbliche amministrazioni sono soggette, oramai da più di un decennio, a una serie cospicua di obblighi di pubblicazione di dati e documenti sul proprio sito, per finalità sia di pubblicità legale (l'albo pretorio) sia per finalità di trasparenza (soprattutto a seguito del cd. "Decreto Trasparenza", il D.Lgs. 33/2013). Molto spesso queste pubblicazioni contengono anche dati personali: si pensi ad esempio ai curricula presenti nella sezione amministrazione trasparente del MIUR, degli USR o delle scuole, oppure alle graduatorie in albo pretorio. Occorre quindi chiedersi entro che limiti tali pubblicazioni siano lecite.

Alla pubblicazione di informazioni sul sito Internet di un ente consegue infatti la diffusione del contenuto pubblicato, vale a dire la messa a disposizione delle medesime informazioni a una collettività tendenzialmente indeterminata.

Il Regolamento europeo prescrive, all'art. 86, che i dati personali contenuti in documenti ufficiali in possesso di un'autorità pubblica o di un organismo pubblico o privato per l'esecuzione di un compito svolto nell'interesse pubblico possano essere comunicati "*conformemente al diritto dell'Unione o degli Stati membri cui l'autorità pubblica o l'organismo pubblico sono soggetti, al fine di conciliare l'accesso del pubblico ai documenti ufficiali e il diritto alla protezione dei dati personali*". Il GDPR, quindi, rimette al diritto degli Stati membri il bilanciamento tra accesso e protezione dei dati personali. In attesa delle modifiche normative, dobbiamo fare riferimento al quadro attuale, e dunque a quanto previsto dal Codice della Privacy e dal Decreto Trasparenza.

Analizziamo, quindi, la disciplina nazionale, in merito, attualmente prevista[34].

La diffusione di dati personali attraverso i siti istituzionali è lecita, secondo quanto disposto dell'art. 19 D.Lgs. 196/2003 e 7-*bis* D.Lgs. 33/2013, qualora sia prevista da una norma di legge o di regolamento.

E, anche qualora una norma di legge o di regolamento ne preveda la pubblicazione, è comunque imprescindibile rispettare, con riguardo ai dati "comuni", i principi di necessità, pertinenza e non eccedenza (principi del Codice della Privacy, a cui corrispondono i principi di minimizzazione dei dati, limitazione della conservazione e protezione dei dati per impostazione predefinita - privacy by default). I (vecchi) dati sensibili, ora "categorie particolari di dati" possono essere pubblicati solo quando sia indispensabile per le finalità di trasparenza, mentre i dati inerenti lo stato di salute non possono mai essere diffusi.

Per fare degli esempi pratici, non è, in generale, pertinente la diffusione delle generalità complete (luogo e data di nascita, indirizzo o altri recapiti privati) dell'interessato, così come può non essere pertinente la diffusione del codice fiscale, della e-mail privata, o di altri dati che appunto appaiano eccedenti rispetto alle finalità di pubblicazione.

Il corretto percorso di pubblicazione può evincersi dalle Linee guida del Garante Privacy in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per

[34] 22 aprile 2018.

finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati[35], che contengono anche un utilissimo schema[36] da utilizzarsi tutte le volte che sia obbligatorio diffondere dati o documenti contenenti dati personali. Queste Linee guida, come abbiamo visto, sono destinate a rimanere in vigore fino a quando non vengano modificate, sostituite o abrogate.

Ogni qual volta risulti necessario pubblicare dati personali (anche se comuni), pertanto, si dovrebbe imprescindibilmente:

A. Accertare il fondamento normativo (legge o regolamento); e,
B. Rispettare i principi di minimizzazione dei dati, limitazione della conservazione e protezione dei dati per impostazione predefinita - privacy by default.

### *3.5.2. Il rapporto tra trattamento di dati personali e accesso generalizzato*

Il D.Lgs. 97/2016, modificando il Decreto Trasparenza, ha innovato la definizione di trasparenza, ora intesa come "*accessibilità totale dei dati e documenti detenuti dalle pubbliche amministrazioni, allo scopo di tutelare i diritti dei cittadini, promuovere la partecipazione degli interessati all'attività amministrativa e favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche*". In ossequio a tale principio, è stato introdotto l'istituto dell'accesso generalizzato, che consiste nel diritto di chiunque ad accedere a dati o documenti detenuti dalla Pubblica Amministrazione. Questo diritto non è però incondizionato, e incontra dei limiti anche per quanto riguarda il contemperamento con la disciplina del trattamento di dati personali.

Difatti, l'art. 5-*bis* del D.Lgs. 33/2013 prevede che l'istituto dell'accesso generalizzato (i cui limiti si è tentato di esplicitare con la determina 1309/2016 dell'ANAC[37] e con la delibera 2/2017 del DFP[38]) incontri dei limiti, e in particolare l'accesso può essere negato quando il diniego sia necessario per evitare un pregiudizio concreto (tra l'altro) alla protezione dei dati personali, in conformità con la disciplina legislativa in materia.

Quando sussista questo "pregiudizio concreto" è un giudizio non facile, ma sul sito del Garante Privacy vi sono molti pareri in tema di diniego di accesso generalizzato, che possono fornire (unitamente alle Linee guida e alla Circolare) delle utili indicazioni.

Un esempio pratico può essere tratto da un recente parere del Garante Privacy[39], richiesto da un USR, con riguardo all'estrazione in formato elettronico di tutta la documentazione in merito ai registri attestanti le presenze e assenze di tutti gli alunni, per tre anni. Il Garante ha ritenuto legittimo il diniego opposto dall'Istituto comprensivo a cui i dati erano stati richiesti, in quanto si trattava di dati personali di minorenni, e per di più non ci si limitava ai meri nominativi ma venivano richiesti anche gli specifici giorni di presenza o assenza di ciascun alunno.

---

[35] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3134436.

[36] http://www.garanteprivacy.it/image/image_gallery?uuid=6d3a64fb-ebf4-4e22-b7dd-8b5db4c18816&groupId=10160&t=1401208198794.

[37] http://www.anticorruzione.it/portal/public/classic/AttivitaAutorita/AttiDellAutorita/_Atto?ca=6666.

[38] http://www.funzionepubblica.gov.it/articolo/dipartimento/01-06-2017/circolare-n-2-2017-attuazione-delle-norme-sull%E2%80%99accesso-civico.

[39] http://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/7273244.

In questo contesto, il ruolo del Data Protection Officer assume una rilevante importanza, sia per quanto riguarda l'accesso generalizzato, sia anche per il tema delle pubblicazioni online. Si pensi ad esempio a una richiesta, come quella dell'esempio appena illustrato, di accesso generalizzato alle presenze degli studenti (o dei docenti), o ad altri documenti contenenti dati personali. Per le (certamente frequenti) ipotesi di non semplice soluzione, il DPO, grazie alla sua competenza specialistica, può (e anzi deve) fornire consulenza non solo al titolare del trattamento, ma anche ai dipendenti che trattino dati personali. Il dipendente quindi, in caso di dubbio, si dovrà rivolgere al DPO, per ricevere le opportune delucidazioni.

# 4. ABBREVIAZIONI E ACRONIMI

Nella presente tabella è riportato un elenco degli acronimi, che ricorrono all'interno del presente documento, con il relativo significato.

| ACRONIMO | SIGNIFICATO |
|---|---|
| AgID | Agenzia per l'Italia Digitale |
| ANS | Anagrafe Nazionale Studenti |
| CdE | Consiglio d'Europa |
| CERT-PA | Computer Emergency Response Team - Pubblica Amministrazione |
| DPIA | Data Protection Impact Assessment (valutazione d'impatto sulla protezione dei dati) |
| DPO | Data Protection Officer (in italiano RPD) |
| GDPR | General Data Protection Regulation (Regolamento UE 2016/679) |
| ICT | Information and Communication Technology (Tecnologie dell'informazione e della comunicazione) |
| IoT | Internet of Things (in italiano Internet delle Cose) |
| MM-PA | Misure Minime di sicurezza per la Pubblica Amministrazione descritte dalla circolare n. 2/2017 dell'AgID |
| NIS | Direttiva 2016/1148, detta anche Direttiva NIS (Network and Information Security) |
| RGPD | Regolamento Generale sulla Protezione dei Dati (in inglese GDPR) (Regolamento UE 2016/679) |
| RPD | Responsabile della Protezione dei Dati (in inglese DPO) |
| VPN | Virtual Private Network |

# 5. LINKOGRAFIA


→ http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32016R0679&from=EN (Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati).

→ http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048 (Guidelines on Data Protection Officers ('DPOs')).

→ http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052 (Personal data breach notification under Regulation 2016/679 (wp250rev.01)).

→ http://194.242.234.211/documents/10160/0/WP+248+-+Linee-guida+concernenti+valutazione+impatto+sulla+protezione+dati (Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679).

→ http://garanteprivacy.it/regolamentoue/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali (Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali - Garante Privacy).

→ http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7322110 (Nuove Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico (in aggiunta a quelle adottate dal Gruppo Art. 29)).

→ http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-06-30;196!vig= (Codice in materia di protezione dei dati personali - DECRETO LEGISLATIVO 30 giugno 2003, n. 196).

→ http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3134436 Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati.