Implementazione del modello privacy in azienda

Framework normativo

- GDPR
- CODICE DELLA PRIVACY (Dlgs 196/2003) COME COORDINATO E AGGIORNATO DA:
- L. 27 dicembre 2019, n. 160,
- D.L. 14 giugno 2019, n. 53
- D.M. 15 marzo 2019
- Decreto di adeguamento al GDPR (Decreto Legislativo 10 agosto 2018, n. 101).

Definizione della politica interna sui Dati Personali, individuazione delle figure chiave e del team privacy

- adottare un modello organizzativo che permetta di analizzare, impostare e strutturare le fasi di adeguamento al Regolamento Europeo del titolare con riguardo alle proprie specifiche attività di trattamento; documentare e comprovare tutte le misure, le procedure e gli adempimenti posti in essere dal Titolare nel rispetto del GDPR e la loro efficacia
- art. 5 par. 2 GDPR "Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»), disposizione alla quale fa da eco il considerando 74, ripreso dall'art. 24 GDPR, per il quale: "… dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure…"
- responsabilizzare management e team supporto (IT, legal, referente BU; HR; marketing)
- Assenza modello riferimento diversamente dall'approccio del precedente codice privacy del 2003 dove veniva fornito invece un modello di adeguamento standard, ovvero attraverso l'allegato B

Inventario delle attività di trattamento, dei dati ed interviste

- Prassi adottata nascente da modello 231 e applicata modello privacy
- individuare attività trattamento più a rischio di violazioni e procedere a una valutazione di impatto sul trattamento dei dati quando un trattamento presenta rischi elevati per i diritti e le libertà delle persone fisiche (art. 35 GDPR – cfr. art. 6, comma 2, lett. A, D.Lgs. 231/2001);
- prevedere e programmare misure di formazione affinchè il trattamento sia effettuato conformemente al GDPR e garantisca la tutela dei diritti degli interessati (art. 29 GDPR – cfr. art. 6, comma 2, lett. B e D, D.Lgs. 231/2001);
- mettere in atto misure tecniche e organizzative adeguate sia per realizzare efficacemente i principi di protezione dei dati "by design" e "by default", tenendo conto anche dei costi di attuazione, e sia per garantire un livello di sicurezza adeguato al rischio (artt. 25 e 32 GDPR – cfr. art. 6, comma 2, lett. C, D.Lgs. 231/2001);
- In caso di eventuale violazione di dati personali degli interessati, adottare misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati anche successivamente al verificarsi di un Data Breach, rivedendo e implementando le misure adottate (art. 34 GDPR – cfr. art. 7, comma 4, D.Lgs. 231/2001);
- procedere a riesame della valutazione d'impatto sulla protezione dei dati quando insorgono variazioni del rischio nelle attività di trattamento (art. 35 GDPR – cfr. art. 7, comma 4, D.Lgs. 231/2001);
- procedere a un riesame e aggiornamento delle adottate misure tecniche e organizzative quando necessario, e ad un'integrazione delle garanzie necessarie per soddisfare i requisiti del regolamento anche nel corso del trattamento (art. 35 GDPR – art. 7, comma 4, D.Lgs. 231/2001.

DIFFERENZA DA 231: l'adozione di un modello organizzativo in materia di dati personali non consente di per sé di escludere automaticamente la responsabilità dell'organizzazione in caso di data breach e/o di inadempimento ai principi e alle norme del GDPR

Standard di riferimento possibili

- Nella costruzione del modello organizzativo privacy è utile inoltre tenere in considerazione anche i recenti standard forniti dalle normative ISO, in particolare la ISO/IEC 27701, di recente pubblicazione (agosto 2019), per la gestione delle informazioni personali e della privacy (che va ad aggiornare le normative precedenti quali la ISO/ IEC 27001:2017 e la ISO/IEC 27002), volta a fornire uno strumento pratico alle organizzazioni per implementare il sistema di gestione e **sicurezza dei dati personali**, per documentare le scelte di natura tecnica e organizzativa adottate, per migliorare i controlli e le verifiche interne e da ultimo per coordinarsi con le autorità di controllo per le verifiche del caso.
- In alternativa a tale norma rimane una validissima opzione orientarsi verso la ISO 29100, finalizzata a definire un manuale operativo in ambito privacy, pubblicata nel 2011 e aggiornata nel 2015.

Implementazione della Valutazione d'Impatto sulla Protezione dei Dati e della Privacy Policy (documenti "high level") 1di2

- Nella pratica, il modello **potrà essere strutturato** al fine di dare conto e raccogliere in ordine sistematico:
- le disposizioni normative che regolano il settore di appartenenza dell'organizzazione in ambito privacy;
- la definizione dei principi e dei termini fondamentali in ambito Privacy in relazione alla natura dei trattamenti effettuati;
- la descrizione dell'organizzazione e la tipologia dei trattamenti di dati personali;
- la **mappatura dei flussi informativi** e la tipologia di dati trattati;
- l'organigramma del Titolare;
- le privacy policy (ad es. informative privacy per clienti, personale, fornitori, utenti esterni, ecc.; modelli di consenso al trattamento);
- i ruoli, le funzioni e le responsabilità del Titolare del Trattamento nonché dei soggetti delegati al trattamento dati personali;
- i **rapporti contrattuali tra Titolare, Contitolari, Responsabili del Trattamento e, se nominato, del DPO** e le relative responsabilità;
- gli atti di nomina degli autorizzati interni al trattamento, con le relative competenze, doveri, ruoli e responsabilità (ex art. 2 quaterdecies D.lGS. 101/2018 e art. 29 GDPR);

2di2

- le attività di formazione del personale, predisponendo un sistema che documenti la formazione svolta per ciascun soggetto (art. 39 GDPR);
- le procedure di comportamento del personale interno e le policy di utilizzo dei sistemi e **dispositivi elettronici**, e-mail, internet, e sistemi di archiviazione elettronica;
- le procedure di audit per verificare la compliance al GDPR;
- la valutazione delle misure tecniche e organizzative per garantire livelli di sicurezza adeguati al rischio (art. 32, par. 2, GDPR);
- la documentazione inerente al riesame, agli aggiornamenti e all'implementazione delle **misure tecniche e organizzative** adottate;
- la procedura di valutazione dei rischi (Risk Assessment) ex art. 32, paragrafo 2, GDPR, e la procedura di valutazione di impatto (DPIA) dei trattamenti previsti sulla protezione dei dati in presenza di rischi elevati per i diritti e le libertà degli interessati;
- le **prassi operative** in caso di violazioni di dati ("Data Breach") e di incidenti della sicurezza sia per la propria organizzazione che per gli eventuali responsabili del trattamento e/o contitolari;
- le procedure per l'esercizio dei diritti degli interessati;
- i modelli di notifica al Garante ex art. 33 in caso di data breach e di comunicazione agli interessati ex art. 34 GDPR, il modello di richiesta di esercizio dei diritti degli interessati e di riscontro da parte dell'organizzazione;
- l'adozione di **codici di condotta** e/o modelli organizzativi L. 231/2001;
- le certificazioni aziendali.

In caso di Gruppo societario

- Se poi si tratta di un gruppo di imprese occorrerà anche chiarire e definire **il ruolo delle singole società all'interno del gruppo, i rapporti interni e quelli con la capogruppo**, come avviene la circolazione dei dati tra le singole entità, le rispettive responsabilità, le finalità dei trattamenti effettuati da ciascuna entità e via dicendo.

Privacy by design e by default (art. 25 GDPR)

Protezione dei dati fin dalla progettazione

Configurare il Trattamento identificando e formalizzando, fin dalla fase di progettazione, le misure tecniche e organizzative più adeguate in relazione ai rischi, volte ad attuare in maniera efficace i principi di protezione dei Dati Personali e a integrare nel Trattamento le necessarie garanzie al fine di soddisfare i requisiti del GDPR e tutelare i diritti degli Interessati

Protezione dei dati per impostazione predefinita

Adottare, per impostazione predefinita, misure tecniche e organizzative che garantiscano il Trattamento dei soli Dati Personali necessari per ogni specifica finalità e per il periodo strettamente necessario, assicurando il livello di protezione dei Dati Personali identificato in fase di progettazione

Approccio basato sul rischio

Prima di avviare una nuova attività che comporti un Trattamento di Dati Personali, **occorre valutare il rischio** che può derivare agli Interessati in caso di violazione dei Dati Personali e adottare misure atte a mitigarlo (art. 32 GDPR). **Ove il livello di impatto sia elevato,** occorre condurre una **Valutazione di impatto dei Trattamenti sulla protezione dei Dati Personal**i (artt. 35 - 36 GDPR).

PRIVACY ASSESSMENT

- **Documental assessment** (analisi di tutti i documenti e le procedure privacy aziendali)
- **Mappatura dei Dati Personali**
- **Interviste** ai soggetti coinvolti nel trattamento
- **System assessment** (analisi di tutti i sistemi e di tutte le misure adottate)
- **Valutazione dei rischi** sulla sicurezza de Dati Personali e delle libertà individuali
- **Valutazione di impatto dei Trattamenti sulla protezione dei Dati Personali** (artt. 35-36 GDPR)
- Individuazione delle **misure tecniche e organizzative adeguate** per minimizzare i rischi
- **Report di Assessment** (gap analysis tra le risultanze dell'Assessment e la norma applicabile)

REMEDIATION E IMPLEMENTATION

- **Aggiornamento e revisione documentale** di tutte le Informative privacy, i consensi, le nomine, il Registro dei trattamenti, il Registro delle violazioni, le procedure e i sistemi
- **Aggiornamento e implementazione delle misure tecniche e organizzative**
- **Aggiornamento e implementazione del Modello Organizzativo Privacy**
- **Formazione del personale**

MAINTENANCE E CONTROL

- **Mantenimento e aggiornamento periodico** della documentazione privacy, delle procedure e delle misure tecniche e organizzative adottate
- **Monitoraggio periodico tramite audit interni ed esterni** (utilizzo di checklist)

Registro dei trattamenti del Titolare

ART. 30, PARAGRAFO 1 E CONSIDERANDO 82 GDPR
FAQ DELL'AUTORITÀ GARANTE DELL'8 OTTOBRE 2018

Ogni **Titolare del trattamento** deve tenere un Registro delle attività di trattamento svolte sotto la propria responsabilità che **deve** contenere:

- **il nome e i dati di contatto del Titolare del trattamento** e, ove applicabile, del Contitolare del trattamento, del Rappresentante del titolare del trattamento e del Responsabile della protezione dei dati;
- le **finalità** del Trattamento;
- una descrizione delle **categorie di Interessati** e delle **categorie di Dati Personali**;
- le **categorie di Destinatari** a cui i Dati Personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi o di organizzazioni internazionali;
- ove applicabile, i **trasferimenti di Dati Personali verso un paese terzo** o **un'organizzazione internazionale**, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo paragrafo dell'articolo 49, la documentazione delle garanzie adeguate;
- ove possibile, i **termini ultimi previsti per la cancellazione** delle diverse categorie di Dati Personali;
- ove possibile, una **descrizione generale delle misure di sicurezza tecniche e organizzative** di cui all'articolo 32, paragrafo 1 GDPR.

Registro dei trattamenti del Responsabile

ART. 30, PARAGRAFO 2 E CONSIDERANDO 82 GDPR
FAQ DELL'AUTORITÀ GARANTE DELL'8 OTTOBRE 2018

Ogni **Responsabile del trattamento** deve tenere un Registro delle attività di trattamento svolte per conto di un Titolare che **deve** contenere:

- il **nome e i dati di contatto del Responsabile** o dei Responsabili del trattamento**, di ogni Titolare del trattamento** per conto del quale agisce il Responsabile del trattamento, del Rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del Responsabile della protezione dei dati;
- le **categorie dei Trattamenti effettuati per conto di ogni Titolare** del trattamento;
- ove applicabile, i **trasferimenti di Dati Personali verso un paese terzo o un'organizzazione internazionale**, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo paragrafo dell'articolo 49, la documentazione delle garanzie adeguate;
- ove possibile, una **descrizione generale delle misure di sicurezza tecniche e organizzative** di cui all'articolo 32, paragrafo 1.

Registro dei trattamenti (1 di 2)

L'Autorità Garante sulla Protezione dei Dati Personali afferma che **può** essere riportata nel Registro delle attività di trattamento **qualsiasi altra informazione che il Titolare o il Responsabile ritengano utile indicare** (ad es. le **modalità di raccolta del consenso,** l'indicazione di eventuali **Designati al Trattamento** individuati dal Titolare in merito ad alcune tipologie di trattamento, etc.). In particolare, si suggerisce di indicare:

- la **base giuridica** del Trattamento;
- l'elenco dei **Destinatari** cui sono comunicati i Dati Personali, distinti fra Titolari autonomi e Responsabili del trattamento;
- la **valutazione del rischio** e le **azioni di mitigazione dello stesso**;
- la Valutazione di **impatto sulla protezione dei Dati Personali**.

Il Registro dei trattamenti è un **documento di censimento e analisi dei Trattamenti effettuati** e, in quanto tale, **deve essere mantenuto costantemente aggiornato** poiché il suo contenuto deve sempre corrispondere all'effettività dei Trattamenti posti in essere.

Qualsiasi **cambiamento**, in particolare in ordine alle modalità, finalità, categorie di Dati, categorie di Interessati, deve essere immediatamente inserito nel Registro, dando conto delle modifiche sopravvenute.

Il Registro può essere compilato **sia in informato cartaceo che elettronico,** ma deve in ogni caso recare, in maniera verificabile:

- **la data della sua prima istituzione** (o la data della prima creazione di ogni singola scheda per tipologia di Trattamento);
- **la data dell'ultimo aggiornamento.**

Registro dei trattamenti (2 di 2)

Ai sensi dell'art. 30, par. 5 GDPR, in ambito privato **i soggetti obbligati alla tenuta del Registro dei trattamenti** sono così individuabili:

- **imprese o organizzazioni con almeno 250 dipendenti**;
- qualunque Titolare o Responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui **Trattamenti che possano presentare un rischio – anche non elevato – per i diritti e le libertà dell'Interessato**;
- qualunque Titolare o Responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui **Trattamenti non occasionali**;
- qualunque Titolare o Responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui **trattamenti delle categorie particolari di Dati di cui all'articolo 9, paragrafo 1 GDPR, o di Dati Personali relativi a condanne penali e a reati di cui all'articolo 10 GDPR**.

Al di fuori dei casi di tenuta obbligatoria del Registro, anche alla luce del Considerando 82 GDPR, **il Garante ne raccomanda la redazione a tutti i Titolari e Responsabili del trattamento,** in quanto strumento che, fornendo piena contezza del tipo di Trattamenti svolti, contribuisce a meglio attuare, con modalità semplici e accessibili a tutti, il principio di **accountability** e, al contempo, ad agevolare in maniera dialogante e collaborativa l'attività di controllo del Garante stesso.

Per le PMI il Garante ha fornito sul proprio sito internet due modelli di «**Registro semplificato**» delle attività di trattamento, del Titolare e del Responsabile.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

SCHEDA REGISTRO DEI TRATTAMENTI *[per i contenuti vedi Faq sul registro delle attività di trattamento: https://www.garanteprivacy.it/regolamentoue/registro]*							
TITOLARE/CONTITOLARE/RAPPRESENTANTE DEL TITOLARE *[inserire la denominazione e i dati di contatto]*							
RESPONSABILE DELLA PROTEZIONE DEI DATI *[inserire la denominazione e i dati di contatto]*							
TIPOLOGIA DI TRATTAMENTO	**FINALITA' E BASI LEGALI DEL TRATTAMENTO**	**CATEGORIE DI INTERSSATI**	**CATEGORIE DI DATI PERSONALI**	**CATEGORIE DI DESTINATARI** *[Indicare eventuali responsabili del trattamento o altri titolari cui i dati siano comunicati]*	**TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI** *[Indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del RGPD]*	**TERMINI ULTIMI DI CANCELLAZIONE PREVISTI**	**MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE**

Informativa privacy (1 di 2)

ARTT. 13 – 14 E CONSIDERANDO 39, 58, 59, 60 61 E 62 GDPR

L'**Informativa sul trattamento dei dati personali**, che il Titolare del trattamento fornisce all'Interessato, deve **tassativamente contenere le seguenti informazioni**:

- **l'identità e i dati di contatto del Titolare** del trattamento e, ove applicabile, del suo Rappresentante e del Responsabile per la protezione dei dati;
- i **Dati Personali trattati**;
- le **finalità** del Trattamento cui sono destinati i Dati Personali nonché **la base giuridica** del Trattamento;
- qualora il Trattamento si basi sull'art. 6, par. 1, lett. f) GDPR, i **legittimi interessi perseguiti** dal Titolare o da terzi;
- se la comunicazione dei Dati Personali è un **obbligo legale o contrattuale o un requisito necessario** per la conclusione del contratto, se l'Interessato ha **l'obbligo di fornire i Dati Personali e le possibili conseguenze del mancato conferimento**;
- gli eventuali **Destinatari o categorie di Destinatari** dei Dati Personali e l'ambito di diffusione dei Dati;
- il **periodo di conservazione** dei Dati Personali oppure, se non possibile, i criteri utilizzati per determinare tale periodo;
- ove applicabile, **l'intenzione del Titolare di trasferire i Dati Personali a un paese terzo o a un'organizzazione internazionale** e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere copia di tali Dati o il luogo dove sono stati resi disponibili;
- i **diritti dell'Interessato** previsti agli artt. 15-22 GDPR;
- il diritto dell'Interessato di proporre **reclamo all'Autorità di controllo**;
- l'esistenza di **un processo decisionale automatizzato**, compresa la profilazione, e la logica utilizzata nonché le conseguenze per l'Interessato.

Informativa privacy (2 di 2)

L'Informativa sul Trattamento dei Dati Personali raccolti presso l'Interessato deve essere fornita dal Titolare all'Interessato **prima dell'inizio del Trattamento dei Dati e dell'acquisizione del consenso** (art. 13 GDPR).

Ove i Dati Personali non sia direttamente raccolti presso l'Interessato, il Titolare deve fornire l'Informativa **entro un termine ragionevole, che non può superare un mese dalla raccolta, oppure al momento della comunicazione dei Dati** a Terzi o all'Interessato (art. 14 GDPR).

L'Informativa sul Trattamento dei Dati Personali deve avere **forma concisa, trasparente, intellegibile e facilmente accessibile per l'Interessato** (Considerando 58 GDPR)**.** Il Garante chiarisce che l'Informativa, da redigere in un **linguaggio chiaro e semplice**, deve essere data **in linea di principio per iscritto e preferibilmente in formato elettronico**, anche se sono ammessi «altri mezzi» (e quindi anche la forma orale). In ottica di accountability, è opportuno prediligere comunque una forma che consenta al Titolare di provare, in caso di ispezione del Garante, di aver fornito l'Informativa all'Interessato.

Il GDPR consente l'utilizzo di **icone** (che saranno adottate dalla Commissione Europea e dovranno essere identiche in tutta l'UE) per presentare i contenuti dell'Informativa in forma sintetica, ma solo in combinazione con l'informativa estesa (cd. **Informativa stratificata**).

Qualora il Titolare intenda trattare ulteriormente i Dati Personali per una **finalità diversa** da quella per cui sono stati raccolti, il GDPR impone al Titolare di **informarne l'Interessato prima di procedere al Trattamento ulteriore** (art 13, par. 3 GDPR).

In relazione all'Informativa da rendere in occasione del **reclutamento del personale** (cd. recruiting), il nuovo art. 111-bis del D.lgs. 196/2003 («Informazioni in caso di ricezione di curriculum») stabilisce che l'Informativa non è dovuta in caso di ricezione di curriculum spontaneamente trasmessi dagli Interessati ai fini dell'eventuale instaurazione di un rapporto di lavoro. Rimane l'obbligo per il Titolare di rendere **l'Informativa** all'Interessato **«al momento del primo contatto utile, successivo all'invio del curriculum»**. Il Titolare **non è tenuto ad acquisire il consenso dell'Interessato** purché il Trattamento sia effettuato sulla base e nei limiti dell'art. 6, par. 1, lett. B GDPR (Trattamento necessario per l'esecuzione di misure precontrattuali adottate su richiesta dell'Interessato).

Esempi di Interessati cui rendere l'Informativa:

- Lavoratori subordinati (compresi gli apprendisti, i lavoratori a termine od occasionali) o prestatori di lavoro nell'ambito di un contratto di somministrazione o di tirocinio
- Candidati all'instaurazione di un rapporto di lavoro
- Persone fisiche che ricoprono cariche sociali o altri incarichi nelle persone giuridiche
- Clienti e fornitori
- Liberi professionisti, consulenti, agenti, rappresentati e mandatari
- Lavoratori autonomi e collaboratori
- Visitatori sito web

Data Protection Agreement (1 di 2)

ART. 28 E CONSIDERANDO 81 GDPR

Qualora un **Trattamento debba essere effettuato per conto del Titolare del trattamento**, quest'ultimo ricorre unicamente a **Responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate** in modo tale che il Trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'Interessato.

I Trattamenti da parte di un Responsabile del trattamento sono disciplinati da un **contratto o da altro atto giuridico** a norma del diritto dell'Unione o degli Stati membri, che vincoli il Responsabile del trattamento al Titolare del trattamento e che **stipuli la materia disciplinata e la durata del Trattamento, la natura e la finalità del Trattamento, il tipo di Dati Personali e le categorie di Interessati, gli obblighi e i diritti del Titolare del trattamento**.

Il contratto o atto di nomina a Responsabile del trattamento («Data Protection Agreement»), stipulato in **forma scritta, anche in formato elettronico**, deve tassativamente prevedere:

- le **istruzioni documentate** fornite dal Titolare al Responsabile cui quest'ultimo deve attenersi, anche in caso di trasferimento di Dati Personali a un paese terzo o un'organizzazione internazionale;
- le **operazioni di Trattamento assegnate** al Responsabile;
- la garanzia del Responsabile che le **Persone Autorizzate** al trattamento dei Dati Personali siano **vincolate alla riservatezza**;
- **l'indicazione di misure di sicurezza** tecniche e organizzative **adeguate** adottate dal Responsabile;
- **l'autorizzazione generale o specifica alla nomina si Sub-responsabili**;
- l'impegno del Responsabile ad **assistere il Titolare** per garantire il **rispetto degli obblighi di misure di sicurezza, di notifica dei Data breach e di Valutazione d'impatto sulla protezione dei Dati Personali**;
- la **cancellazione o restituzione di tutti i Dati Personali** al termine della prestazione dei servizi relativi al Trattamento;
- l'impegno del Responsabile a mettere a disposizione del Titolare tutte le **informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 GDPR** e a contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare o da altro soggetto da questi incaricato.

Data Protection Agreement (2 di 2)

Quando un Responsabile del trattamento ricorre a un altro Responsabile del trattamento (Sub-responsabile) per l'esecuzione di specifiche attività di Trattamento per conto del Titolare del trattamento, **il Responsabile deve imporre su tale Sub-responsabile del trattamento, mediante un contratto o un altro atto giuridico, gli stessi obblighi in materia di protezione dei Dati contenuti nel contratto o in altro atto giuridico tra il Titolare e il Responsabile del trattamento**, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR.

Qualora il Sub-responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei Dati Personali, **il Responsabile iniziale conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del Sub-responsabile**.

È risarcibile qualsiasi danno causato da una violazione del GDPR e il **Titolare e il Responsabile sono responsabili in solido per il risarcimento del danno**.

Il Responsabile del trattamento ne risponde solo se non ha adempiuto agli obblighi previsti dal GDPR (tenuta del Registro dei trattamenti, nomina del DPO ove necessaria e adozione di adeguate misure di sicurezza) o ha agito in modo contrario alle istruzioni impartitegli dal Titolare.

Pertanto, il Titolare è tenuto al risarcimento, fatto salvo il diritto di regresso nei confronti del Responsabile, dei danni patrimoniali e non, cagionati a chiunque a seguito di una violazione della normativa vigente in materia di protezione dei Dati Personali.

In data 2 settembre 2020, l'European Data Protection Board (EDPB), che dal 25 maggio 2018 ha sostituito il Working Party art. 29, ha emanato le «**Guidelines 07/2020 on the concepts of controller and processor in the GDPR**" contenenti le linee guida in tema di Titolare e Responsible del trattamento.

Trattamento di Dati Personali nell'ambito del rapporto di lavoro

ARTT. 88 GDPR «TRATTAMENTO DEI DATI NELL'AMBITO DEI RAPPORTI DI LAVORO»

1. Gli **Stati membri** possono prevedere**, con legge o tramite contratti collettivi, norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro**, in particolare per finalità di assunzione, esecuzione del contratto di lavoro, compreso l'adempimento degli obblighi stabiliti dalla legge o da contratti collettivi, di gestione, pianificazione e organizzazione del lavoro, parità e diversità sul posto di lavoro, salute e sicurezza sul lavoro, protezione della proprietà del datore di lavoro o del cliente e ai fini dell'esercizio e del godimento, individuale o collettivo, dei diritti e dei vantaggi connessi al lavoro, nonché per finalità di cessazione del rapporto di lavoro.

2. Tali norme includono misure appropriate e specifiche a salvaguardia della dignità umana, degli interessi legittimi e dei diritti fondamentali degli interessati, in particolare per quanto riguarda la trasparenza del trattamento, il trasferimento di dati personali nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune e i sistemi di monitoraggio sul posto di lavoro.

D.LGS. 196/2003 – TITOLO VIII «TRATTAMENTI NELL'AMBITO DEL RAPPORTO DI LAVORO»

ART. 111 «REGOLE DEONTOLOGICHE PER TRATTAMENTI NELL'AMBITO DEL RAPPORTO DI LAVORO»

1. Il Garante promuove, ai sensi dell'articolo 2·quater, l'adozione di **regole deontologiche** per i soggetti pubblici e privati interessati al trattamento dei dati personali effettuato nell'ambito del rapporto di lavoro per le finalità di cui all'articolo 88 del Regolamento, prevedendo anche specifiche modalità per le informazioni da rendere all'interessato.

ART. 113 «RACCOLTA DI DATI E PERINENZA»

1. Resta fermo quanto disposto dall´articolo 8 della legge 20 maggio 1970, n. 300, nonché dall'articolo 10 del decreto legislativo 10 settembre 2003, n. 276..

ART. 114 «CONTROLLO A DISTANZA»

1. Resta fermo quanto disposto dall´articolo 4 della legge 20 maggio 1970, n. 300.

ART. 115 «TELELAVORO, LAVORO AGILE E LAVORO DOMESTICO»

1. Nell´ambito del rapporto di lavoro domestico, del telelavoro e del lavoro agile il datore di lavoro è tenuto a garantire al lavoratore il rispetto della sua personalità e della sua libertà morale.

2. Il lavoratore domestico è tenuto a mantenere la necessaria riservatezza per tutto quanto si riferisce alla vita familiare.

PARERE 2/2017 SUL TRATTAMENTO DEI DATI PERSONALI SUL POSTO DI LAVORO ADOTTATO L'8 GIUGNO 2017 DAL WORKING PARTY ART. 29

Dati Personali, finalità e basi giuridiche del Trattamento nell'ambito del rapporto di lavoro

TIPOLOGIA DI DATI PERSONALI

- Dati anagrafici e di contatto (nome, cognome, codice fiscale, numero di telefono, indirizzo e-mail, residenza, domicilio, etc.)
- Dati relativi a istruzione, formazione e lavoro (diploma, laurea, specializzazioni, job title, inquadramento, precedenti esperienze lavorative, etc.)
- Dati contenuti nel curriculum vitae
- Dati relativi a documenti identificativi e di riconoscimento
- Dati riferiti alla retribuzione (stipendio, benefit, indennità, assegno per il nucleo familiare e carichi di famiglia)
- Dati di pagamento e informazioni fiscali (IBAN, CU, etc.)
- Dati attinenti l'utilizzo di strumenti di lavoro, sistemi informatici aziendali, device e autovetture aziendali
- Dati connessi all'accesso ai locali aziendali e alla videosorveglianza
- Dati relativi all'idoneità o inabilità al lavoro
- Dati relativi allo stato di salute (invalidità, assenze per malattia, maternità o infortunio, permessi L. 104/1992)
- Dati riguardanti l'appartenenza a sindacati o partiti politici
- Dari relativi alla fede religiosa e alle convinzioni filosofiche
- Dati relativi alla donazione del sangue o all'appartenenza ad associazioni di volontariato

BASI GIURIDICHE DEL TRATTAMENTO

- Art. 6, paragrafo 1, lett. b), c) e f) GDPR
- Art. 9, paragrafo 2, lett. b), f) e h) GDPR

Nel Parere 2/2017, il WP 29 esclude dalle basi giuridiche del Trattamento dei Dati Personali dei lavoratori il loro mero consenso.

FINALITA' DEL TRATTAMENTO

- instaurazione, gestione ed esecuzione del rapporto di lavoro;
- adempimenti di obblighi previsti da leggi, regolamenti, contratti collettivi nazionali e aziendali e procedure interne, anche in materia di diritto del lavoro, fiscale, della sicurezza e della protezione sociale, salute e sicurezza del lavoro, medicina preventiva o medicina del lavoro;
- servizio di controllo interno per la sicurezza del lavoro e la tutela del patrimonio aziendale in relazione agli strumenti di lavoro e sistemi informatici aziendali in dotazione (rif. Linee Guida Garante 1° marzo 2007), agli accessi sia fisici che informatici, nonché al sistema di videosorveglianza nelle forme richieste dalla normativa di settore (rif. Provvedimento Garante 8 aprile 2010);
- pianificazione e organizzazione del lavoro, produzione e assicurazione della qualità, programmazione e controllo dei costi, nonché eventuale esercizio o difesa di diritti in sede amministrativa o giudiziaria.

Trattamento di Dati Particolari e Dati Giudiziari nell'ambito del rapporto di lavoro

L'**art. 21, comma 1 del D.lgs. 101/2018**, in attuazione delle disposizioni del GDPR, ha demandato al Garante il compito di individuare, con proprio provvedimento di carattere generale, le prescrizioni contenute nelle Autorizzazioni Generali già adottate ante GDPR, relative alle situazioni di trattamento di cui agli artt. 6, par. 1, lett. c) ed e), 9, par. 2, lett. b) e 4, nonché al Capo IX, del GPRR, che risultino compatibili con le disposizioni comunitarie e il decreto medesimo che ha novellato il Codice, provvedendo altresì al loro aggiornamento ove occorrente.

L'«Autorizzazione generale al trattamento dei dati giudiziari da parte di privati, di enti pubblici economici e di soggetti pubblici n. 7/2016» non rientra tra quelle richiamate dall'art. 21, comma 1, D.lgs. 101/2018 ed ha, pertanto, cessato di produrre effetti giuridici alla data del 19 settembre 2018, ai sensi del comma 3 dell'art. 21.

Dati Particolari

Ai sensi dell'art. 21 del D.lgs. 101/2018, il Garante, in data 13 dicembre 2018, ha emanato il «**Provvedimento che individua le prescrizioni contenute nelle Autorizzazioni generali nn. 1/2016, 3/2016, 6/2016, 8/2016 e 9/2016 che risultano compatibili con il Regolamento e con il d.lgs. n. 101/2018 di adeguamento del Codice - 13 dicembre 2018**».

Conseguentemente, in relazione ai Trattamenti dei Dati Personali appartenenti alle cd. categorie particolari nel contesto lavorativo, si deve far riferimento alle «**Prescrizioni relative al trattamento di categorie particolari di dati nei rapporti di lavoro (aut. gen. n. 1/2016)**» che definiscono l'ambito di applicazione del provvedimento, gli Interessati, le finalità del Trattamento e le prescrizioni specifiche relative alle categorie di Dati e alle modalità di Trattamento.

Dati Giudiziari

L'art. 2-octies del D.lgs. 196/2003 prevede che «***il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, del Regolamento,*** *che non avviene sotto il controllo dell'autorità pubblica, è consentito, ai sensi dell'articolo 10 del medesimo Regolamento,* ***solo se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, che prevedano garanzie appropriate per i diritti e le libertà degli interessati***.» e che «*In mancanza delle predette disposizioni di legge o di regolamento, i trattamenti dei dati di cui al comma 1 nonché le garanzie di cui al medesimo comma sono individuate con* ***decreto del Ministro della giustizia***».

Il Legislatore italiano ha dunque voluto dare rilevanza soltanto a quelle autorizzazioni al Trattamento di Dati Giudiziari derivanti da **fonti normative primarie e secondarie**, escludendo codici di condotta o forme di autoregolamentazione.

Il Garante, con i provvedimenti n. 314 e 315 del 22 maggio 2018, ha poi chiarito che il **contratto collettivo non può costituire una valida base giuridica per il Trattamento di Dati Giudiziari** in ragione della genericità con cui in tale documento si fa riferimento al Trattamento dei dati contenuti nel certificato penale e della circostanza per cui lo stesso risulta sprovvisto dei riferimenti alle specifiche esigenze di onorabilità legate allo svolgimento di determinati incarichi.

Pertanto, soltanto i Datori di Lavoro che possono vantare una specifica previsione di legge o di regolamento che consenta loro di trattare Dati Giudiziari (e.g. TUF, TUB, Codice Assicurazioni Private), potranno legittimamente trattare tali Dati, sempre che tali provvedimenti di rango normativo prevedano garanzie appropriate per i diritti e le libertà degli interessati.

Persone Designate e Autorizzate Trattamento dei Dati Personali

ART. 29 GDPR «TRATTAMENTO SOTTO L'AUTORITÀ DEL TITOLARE DEL TRATTAMENTO O DEL RESPONSABILE DEL TRATTAMENTO»

Il Responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del Titolare del trattamento, che abbia accesso a Dati Personali non può trattare tali dati se non è **istruito** in tal senso dal Titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

ART. 2-QUATERDECIES D.LGS. 196/2003 «ATTRIBUZIONE DI FUNZIONI E COMPITI A SOGGETTI DESIGNATI»

1. Il Titolare o il Responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che **specifici compiti e funzioni connessi al Trattamento di Dati Personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità**.

2. Il Titolare o il Responsabile del trattamento individuano le modalità più opportune per **autorizzare al trattamento dei Dati Personali le persone che operano sotto la propria autorità diretta**.

In una struttura organizzativa, pur non essendo obbligatoria, la nomina di uno o più **Designati al trattamento per specifici compiti o funzioni**, ai sensi dell'art. 2-quaterdecies del D.lgs. 196/2003, è tanto più opportuna quanto più la realtà sia articolata.

Il Designato viene identificato sulla base di uno specifico **atto di attribuzione**, che deve essere analitico, e non può a sua volta designare altri designati.

Tra i possibili compiti e funzioni tipici del Designato al trattamento si distinguono i seguenti:

- catalogare analiticamente, con aggiornamento periodico, i Trattamenti di Dati Personali e le banche dati gestite;
- individuare gli Autorizzati al trattamento e, successivamente, diramare le istruzioni necessarie per un corretto, lecito e sicuro Trattamento;
- attuare obblighi di informazione e di acquisizione del consenso, se dovuto, nei confronti degli Interessati;
- predisporre e gestire, se dovuta, la notificazione di un Data breach;
- garantire all'Interessato l'effettivo esercizio dei diritti;
- collaborare per l'attuazione delle prescrizioni del Garante;
- predisporre e aggiornare un sistema di sicurezza idoneo.

L'**Autorizzato al trattamento compie le operazioni di Trattamento** sotto la diretta autorità del Titolare o del Responsabile, **attenendosi alle istruzioni impartite**. Ha un ruolo prettamente esecutivo.

La **designazione degli Autorizzati al trattamento** è necessaria in quanto permette di considerare legittimo il flusso e il Trattamento dei Dati Personali nell'ambito dell'organizzazione del Titolare o del Responsabile.

L'Autorizzato al trattamento deve essere istruito dal Titolare o dal Responsabile del trattamento **tramite specifiche istruzioni operative** e deve ricevere un'**adeguata formazione.**

Data breach

L'art 4, paragrafo 1, n. 12 GDPR definisce la «**Violazione dei Dati Personali**» (Data breach) 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.

Le "**Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679**", adottate dal Working Party art. 29 il 3 ottobre 2017, hanno chiarito che le violazioni possono essere classificate in base ai seguenti tre principi ben noti della sicurezza delle informazioni:

- "**violazione della riservatezza**", in caso di divulgazione dei Dati Personali o accesso agli stessi non autorizzati o accidentali;
- "**violazione dell'integrità**", in caso di modifica non autorizzata o accidentale dei Dati Personali;
- "**violazione della disponibilità**", in caso di perdita, accesso o distruzione accidentali o non autorizzati di Dati Personali.

In caso di violazione dei Dati Personali, il Titolare del trattamento, **senza giustificato ritardo e, ove possibile, entro 72 dal momento in cui ne è venuto a conoscenza, deve notificare la violazione al Garante** a meno che sia improbabile che la violazione dei Dati Personali comporti un **rischio per i diritti e le libertà delle persone fisiche** (art. 33 GDPR)**.**

Il Responsabile del trattamento che viene a conoscenza di un'eventuale violazione è tenuto a informare tempestivamente il Titolare affinché quest'ultimo possa attivarsi.

Le notifiche al Garante effettuate **oltre il termine di 72 ore** devono essere accompagnate dai **motivi del ritardo.**

Debbono essere notificate unicamente le violazioni di Dati Personali che possano avere **effetti avversi significativi sugli individui**, causando danni fisici, materiali o immateriali (e.g perdita del controllo dei propri Dati Personali, limitazione di alcuni diritti, furto d'identità o rischio di frode, perdita finanziaria, danno alla reputazione).

La notifica deve contenere le **informazioni previste all'art. 33, par. 3 GDPR** e indicate nell'Allegato al «Provvedimento del Garante del 30 luglio 2019 sulla notifica delle violazioni dei dati personali». Il Garante ha messo a disposizione sul proprio sito un «**Modello di notifica al Garante**».

Quando la violazione dei Dati Personali possa presentare un **rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento comunica la violazione all'Interessato senza ingiustificato ritardo** (art. 34 GDPR), salvo non ricorra una delle condizioni previste all'art. 34, par. 3 GDPR.

Il Titolare del trattamento, a prescindere dalla notifica al Garante, **documenta tutte le violazioni** dei Dati Personali, predisponendo ad esempio un apposito **Registro delle violazioni**. Tale documentazione consente al Garante di effettuare eventuali verifiche sul rispetto della normativa.