Giuseppe Miceli
Monica Mandico
Elisabeta Cocolos

GUIDA ALLA NUOVA PRIVACY

A cura di Giuseppe Miceli e Rosalisa Lancia

Legislazione Tecnica

Finito di stampare nel mese di marzo 2019 da
STAMPAFLASH s.r.l.
Via Umbria 148/7 - 06059 Todi (PG)

Legislazione Tecnica S.r.L.
00144 Roma, Via dell'Architettura 16

Servizio Clienti
Tel. 06/5921743 - Fax 06/5921068
servizio.clienti@legislazionetecnica.it

Portale informativo: www.legislazionetecnica.it
Shop: ltshop.legislazionetecnica.it

Pagine non disponibili in anteprima

INDICE

Si riporta di seguito l'indice della modulistica e della ulteriore documentazione varia fornita a corredo del volume, nell'Area download collegata allo stesso, accessibile con le modalità indicate nella seconda pagina di copertina.
La sigla accanto a ciascun elemento identifica il nome del file fornito in download; gli elementi contrassegnati con "D" sono unicamente disponibili in formato elettronico per il download.

MODULISTICA

DOCUMENTAZIONE VARIA

D1	Linee guida per la valutazione di impatto (elaborazione Garante privacy)	D
D2	Linee guida sui responsabili della protezione dei dati (elaborazione WP 243)	D
D3	Analisi del rischio: strumento di valutazione dell'adeguamento al GDPR (elaborazione Michele Amadori)	D
D4	Testo coordinato del Codice della privacy (D. Leg.vo 30/06/2003, n. 196)	D

MODULISTICA E DOCUMENTAZIONE ESEMPLIFICATIVA IN LINGUA STRANIERA

MS1	Aviso de privacidad (esp)	D
MS2	Clauza de confidentialitate (rom)	D
MS3	Contract de confidentialitate (rom)	D
MS4	Informare privind prelucrarea datelor (rom)	D
MS5	Notificare privind protectia datelor cu caracter personal (rom)	D

INTRODUZIONE

di Giuseppe Miceli

In tutti gli Stati membri dell'Unione Europea, a partire dal 25 maggio 2018 [1], è già applicabile il nuovo Regolamento UE 2016/679 "*relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati*" (in inglese *General Data Protection Regulation*, in acronimo GDPR) [2] il quale ha abrogato la Direttiva 95/46/CE [3] e, per quanto attiene all'impianto normativo nazionale, per effetto del D. Leg.vo 101/2018 [4], ha modificato il D. Leg.vo 196/2003 [5], c.d. "*Codice della privacy*". L'attenta analisi del GDPR consente di rilevare come obiettivo principale del Legislatore comunitario sia stato quello di assicurare, in tutti gli Stati membri [6], un'applicazione omogenea della normativa in materia di protezione delle persone fisiche con attenzione al trattamento dei dati personali [7] e, quindi, al rispetto del diritto

---

[1] Il Regolamento UE 2016/679 (cosiddetto GDPR) 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 è stato pubblicato il 4 maggio 2016 sulla Gazzetta Ufficiale dell'Unione Europea e prevedeva un periodo di *vacatio* relativo alla sua efficacia e non alla vigenza. Tale termine lungo per la sua piena applicabilità (scaduto proprio il 25 maggio 2018) è stato ritenuto necessario per consentire l'adeguamento degli ordinamenti giuridici dei singoli paesi membri, nonché per agevolare l'allineamento alle nuove regole di trattamento dei dati personali da parte di imprese e Pubblica Amministrazione.

[2] Il GDPR si compone di 99 articoli e 173 "*considerando*" e, unitamente alla Direttiva UE 2016/680, definisce il nuovo quadro normativo unitario all'interno dell'Unione Europea abrogando la cosiddetta "*direttiva madre*", la n. 95/46/CE, e armonizzando la disciplina di settore.

[3] La Direttiva 95/46/CE, essendo stata concepita in un periodo precedente alla profonda evoluzione degli strumenti informatici e di internet, non poteva contenere una disciplina dei moderni ritrovati tecnologici che solo negli ultimi anni hanno riguardato: internet, le app, il cloud, i social network e il complesso scenario dell'internet of things.

[4] Decreto Legislativo 10 agosto 2018, n. 101 "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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)*", pubblicato in GU Serie Generale n. 205 del 04/09/2018, entrato in vigore il 19/09/2018.

[5] Decreto Legislativo 30 giugno 2003, n. 196, "*Codice in materia di protezione dei dati personali*".

[6] In effetti, come si avrà modo di approfondire nell'ambito di questo volume, l'applicazione del GDPR è obbligatoria non solo per i soggetti obbligati che hanno la propria sede in uno dei paesi membri UE bensì per tutti i soggetti che nell'ambito della propria attività d'impresa trattino dati personali su territorio UE o relativi a persone fisiche che appartengono all'area UE, quindi è corretto rilevare che – in presenza di tali circostanze – il GDPR si applichi anche a soggetti extra UE. Il diritto alla protezione dei dati personali è un diritto che dev'essere garantito a prescindere dalla nazionalità o dalla residenza delle persone fisiche (considerando 2), dovendo essere il trattamento dei dati personali al servizio dell'uomo (considerando 3).

[7] È di propedeutica importanza definire cosa si intende per "*dati personali*". Si tratta di informazioni in virtù delle quali si può identificare un individuo, anche indirettamente. Nell'ambito dei dati

della riservatezza [8] o della privacy [9], intesa quale diritto di ogni individuo alla intimità della vita privata e familiare, contro ingerenze altrui, a prescindere dalla tutela dell'onore, del decoro, della reputazione ed anche del diritto all'immagine, ciò in coerenza con una più generale armonizzazione normativa europea.
Il Regolamento segna una profonda innovazione dell'intera disciplina della protezione dei dati personali, ponendo fine alla involontaria frammentazione della disciplina, di fatto, attuata dai 28 paesi membri UE [10] e prevedendo una fitta serie di nuovi diritti e di adempimenti per la tutela di questi, in capo, rispettivamente, all'interessato e al soggetto passivo, *in primis* il titolare del trattamento dei dati.
Sul piano strettamente giuridico, il GDPR rappresenta lo strumento per la piena attuazione dei diritti fondamentali del cittadino europeo e, in particolare, il diritto alla protezione dei dati personali previsto nella Carta di Nizza [11] nonché dal Trattato sul funzionamento dell'Unione [12] che, oltre ad averne esteso l'applicazione

personali si distinguono categorie speciali di dati: dati sensibili e dati genetici; il GDPR aggiunge, inoltre, i dati genetici e biometrici.

[8] Il tema che attiene al diritto alla riservatezza è stato autorevolmente trattato e approfondito, tra gli altri, dal compianto prof. Stefano Rodotà in: S. Rodotà, *La privacy tra individuo e collettività*, in Pol. dir., 1974, p. 550; Id., *Repertorio di fine secolo*, Roma-Bari, 1992; Id., *Tecnologie e diritti*, Bologna, 1995; Id., *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in Riv. crit. dir. priv., 1997, p. 586; Id., *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, 1997.

[9] Con il termine "*privacy*" si intende il diritto alla riservatezza della propria vita privata e, quindi, alle informazioni riguardanti la stessa. Il lemma privacy non attiene solamente a informazioni atte al riconoscimento, bensì anche a dati legati a salute, preferenze sessuali, e così via. Ne deriva l'evidente importanza della tutela al diritto alla privacy ed alla protezione dei dati personali – diritti fondamentali – così come stabilito nella Costituzione italiana e nella Carta dei diritti fondamentali della Unione Europea.

[10] L'obiettivo principale che il Legislatore comunitario intendeva realizzare per effetto dell'emanazione della Direttiva 95/46/CE, ovvero la creazione di un mercato unico, è risultato – di fatto – quantomeno pregiudicato a causa dei differenti (se non, addirittura, incoerenti) approcci interpretativi con i quali ciascun Paese membro ha dovuto fare i conti. Approcci interpretativi che sono risultati essere inevitabilmente differenti in considerazione, oltre che di una opinabile chiarezza delle stesse norme comunitarie, anche per il legittimo potere di discrezione di cui è titolare ogni singolo Stato dell'UE.

[11] La Carta dei diritti fondamentali dell'Unione Europea del 7 dicembre 2000 (c.d. Carta di Nizza) alla quale è stato attribuito lo stesso valore giuridico dei Trattati europei, riconosce il diritto alla protezione dei dati personali e lo definisce come diritto fondamentale delle persone. La Carta di Nizza, infatti, riconosce a ogni persona il diritto al rispetto della vita privata e della vita familiare (art. 7) e il diritto alla protezione dei dati di carattere personale (art. 8), inoltre, viene specificato che il trattamento dei dati personali debba avvenire secondo il principio di lealtà, per finalità determinate e sulla base del consenso della persona interessata o un altro fondamento purché legittimo e previsto dalla legge (comma 2, art. 8) affidando il controllo sul rispetto di tali regole ad un'autorità indipendente.

[12] Il diritto alla tutela dei dati personali, unitamente alla tutela della privacy, rientrano a pieno titolo nell'ambito del diritto alla libertà personale e alla vita privata. Ogni individuo ha il diritto di escludere i terzi (*ius excludendi alios*) dalla propria sfera inviolabile (intesa, anche, come spazio fisico) nonché di impedire qualunque forma di ingerenza o intrusione. È riconosciuto a ciascuno il diritto di impedire la raccolta e il trattamento o la diffusione, senza il proprio consenso (o per

Pagine non disponibili in anteprima

- in caso di trasferimento di dati personali verso paesi terzi (art. 46 (2) GDPR); - nel caso in cui un'autorità di controllo sia chiamata a decidere in relazione a violazioni dei principi di sicurezza e responsabilizzazione del GDPR da parte del titolare del trattamento o del responsabile del trattamento. In tali circostanze i provvedimenti sanzionatori delle autorità potranno tenere conto di tali adesioni e valutare con maggior favore la violazione, con conseguente impatto anche sui valori della possibile sanzione amministrativa pecuniaria (art. 83 (2) (j) GDPR).
La progettazione e adozione di programmi di formazione specifici in materia di privacy per il personale autorizzato al trattamento dei dati (ex art. 29 GDPR). Sia il titolare del trattamento che il responsabile del trattamento devono adottare delle misure idonee a garantire che il personale abbia un approccio consapevole dei rischi della privacy e che vi sia una sensibilità per i temi privacy a livello aziendale.

1.5 Il principio del *risk based approach*

Strettamente connesso al principio di *accountability* è quello del *risk based approach*. A differenza del Codice della privacy e in particolare dell'abrogato Allegato B [(37)], ovvero il "*Disciplinare tecnico in materia di misure minime di sicurezza*", il nuovo Regolamento europeo per la protezione dei dati personali non contiene un elenco di misure minime, bensì fa espresso riferimento alle misure di sicurezza adeguate, ovvero a quelle misure di sicurezza progettate dal titolare o responsabile del trattamento come risultato dell'analisi dei rischi che incombono sui dati personali e propedeutiche al trattamento dei dati stessi. In effetti, con l'adozione da parte del Legislatore di quello che è stato definito un *risk based approach*, il Legislatore comunitario ha inteso spostare in capo al titolare e al responsabile del trattamento la responsabilità di progettare e definire, dopo un'attenta analisi dei rischi, le misure di sicurezza adeguate a garantire la protezione dei dati personali trattati [(38)]. Tanto è vero che gli obblighi imposti in materia di protezio-

[(37)] L'Allegato B del Codice della privacy è stato definitivamente abrogato per effetto dell'entrata in vigore del D. Leg.vo 101/2018, art. 27. L'abrogato Allegato B è comunque consultabile al seguente link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1557184

[(38)] L'analisi del principio generale dell'approccio basato sul rischio consente di evidenziare che il GDPR conferisce a tale principio una importanza maggiore di quanto non facesse la Direttiva 95/46/CE. Il GDPR, a differenza della Direttiva 95/46/CE, qualifica l'obbligo di adozione di misure di sicurezza "*appropriate*" non come un mero dovere a sé stante – che, peraltro, gravava sul titolare già per effetto dell'art. 17 della direttiva – bensì come un vero e proprio principio generale del trattamento. Sul punto, il D. Leg.vo 101/2018 ha ulteriormente esaltato la rilevanza di tale principio, passando dalla previsione obbligatoria dell'adozione, almeno, di misure minime di sicurezza, oltre a quelle adeguate secondo lo stato dell'arte, alla previsione dell'obbligo di adozione di misure "*adeguate*" ovvero da modulare in base alle caratteristiche del caso concreto, dando così effettiva attuazione a quel più generale obiettivo della responsabilizzazione del titolare. In buona sostanza, il titolare del trattamento – come pure il responsabile – non potrà più interpretare tale obbligo in chiave "*formalistica*" quanto, piuttosto, in maniera proattiva, dimostrando di aver

ne dei dati personali non opereranno in maniera indiscriminata, ma tengono in considerazione i rischi che possano configurarsi in un determinato trattamento dei dati personali. Ecco quindi che i titolari del trattamento sono chiamati a una valutazione preliminare dei possibili rischi connessi alle proprie attività, adottando, ove necessario, adeguate misure di protezione [(39)]. Per effetto del GDPR, il Legislatore comunitario ha realizzato il suo intento di *valorizzare l'approccio basato sul rischio*, fornendo i parametri essenziali (natura, ambito applicativo, contesto e finalità del trattamento, nonché rischi possibili) in virtù dei quali poter valutare l'adeguatezza delle misure adottate e garantire, così, la conformità del trattamento alla disciplina rilevante.

A tal fine, il Regolamento europeo 2016/679 contiene la definizione di rischio nei considerando 75 e 76 [(40)] mentre all'art. 24 il GDPR sancisce a carico del titolare e del responsabile del trattamento la propedeuticità, rispetto al trattamento dei dati personali, dell'analisi dei rischi connessi al trattamento stesso, al fine di implementare le appropriate misure di sicurezza.

Anche il considerando 83 del Regolamento prevede che, nel valutare l'adeguato livello di sicurezza, si debba tener conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o

---

adottato una strategia aziendale che, nel suo complesso, sia idonea a esonerare il titolare da responsabilità e a riconoscerlo *compliant*, ovvero osservante, della disciplina di protezione dei dati.

[(39)] Rispetto al concetto di adeguatezza, deve evidenziarsi che questo si configura come la "*capacità di soddisfare una qualità o un risultato posto come obiettivo*". Il che si traduce nel fatto che le soluzioni adottate a garanzia dei sistemi e dei servizi informatici raggiungano un livello di accettabilità, sia in termini tecnici che qualitativi.

[(40)] Considerando 75: "*I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione 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, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati*".

Considerando 76: "*La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato*".

Pagine non disponibili in anteprima

- la durata, ovvero la persistenza, dell'attività di trattamento;
- la portata geografica dell'attività di trattamento [29].

2.4.3 Il concetto di "*monitoraggio regolare e sistematico*"

Sempre ai fini della nomina del RPD-DPO si fa riferimento al concetto di "*monitoraggio regolare e sistematico*" degli interessati, concetto che non trova definizione all'interno del GDPR; tuttavia, il considerando 24 menziona il "*monitoraggio del comportamento di detti interessati*" [30] ricomprendendovi senza dubbio tutte le forme di tracciamento e profilazione su internet anche per finalità di pubblicità comportamentale.
Occorre rilevare, però, che la nozione di monitoraggio non trova applicazione solo con riguardo agli utenti di internet, in quanto il tracciamento online va considerato solo uno dei possibili esempi di monitoraggio del comportamento degli interessati.
L'aggettivo "*regolare*" ha almeno uno dei seguenti significati a giudizio del Gruppo di lavoro Articolo 29:

- che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito;
- ricorrente o ripetuto a intervalli costanti;
- che avviene in modo costante o a intervalli periodici.

L'aggettivo "*sistematico*" ha almeno uno dei seguenti significati a giudizio del Gruppo Articolo 29:

- che avviene per sistema;
- predeterminato, organizzato o metodico;
- che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
- svolto nell'ambito di una strategia [31].

---

[29] Alcuni esempi di trattamento su larga scala sono i seguenti: trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività; trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il loro tracciamento attraverso titoli di viaggio); trattamento di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche da un responsabile del trattamento specializzato nella prestazione di servizi di questo tipo rispetto ai clienti di una catena internazionale di fast food.

[30] "*Per stabilire se un'attività di trattamento sia assimilabile al controllo del comportamento dell'interessato, è opportuno verificare se le persone fisiche sono tracciate su internet, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, in particolare per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali*". Si osservi che il considerando 24 riguarda l'applicazione extraterritoriale del GDPR; inoltre, vi è una differenza fra l'espressione "*monitoraggio del loro comportamento*" (articolo 3, paragrafo 2, lettera b) e "*monitoraggio regolare e sistematico degli interessati*" (articolo 37, paragrafo 1, lettera b), per cui le due espressioni potrebbero ben riferirsi a concetti distinti.

[31] Ecco alcune esemplificazioni di attività che possono configurare un monitoraggio regolare e sistematico di interessati: curare il funzionamento di una rete di telecomunicazioni; la prestazio-

Inoltre le disposizioni dell'articolo 37, paragrafo 1, lettera c), riguardano il trattamento di categorie particolari di dati ai sensi dell'articolo 9 e di dati personali relativi a condanne penali e a reati di cui all'articolo 10.

2.4.4 Chi nomina il RPD-DPO

A nominare il RPD-DPO, secondo l'articolo 37, possono essere il titolare del trattamento [32] e il responsabile [33] del trattamento. A seconda di chi soddisfi i criteri relativi all'obbligatorietà della nomina, potrà essere il solo titolare del trattamento ovvero il solo responsabile del trattamento, oppure sia l'uno sia l'altro a dover nominare un RPD; questi soggetti saranno poi tenuti alla reciproca collaborazione.
Vale la pena di evidenziare che anche qualora il titolare del trattamento sia tenuto, in base ai criteri suddetti, a nominare un RPD, il suo eventuale responsabile del trattamento non è detto sia egualmente tenuto a procedere a tale nomina – che però può costituire una buona prassi.

2.4.5 Designazione di un unico RPD-DPO

È possibile la nomina di un unico RPD per più organismi (art. 37), così che un gruppo imprenditoriale può nominare un unico RPD a condizione che quest'ultimo sia "*facilmente raggiungibile da ciascuno stabilimento*". Il concetto di raggiungibilità si riferisce ai compiti del RPD in quanto punto di contatto per gli interessati [34], l'autorità di controllo [35] e i soggetti interni all'organismo o all'ente, visto che uno dei compiti del RPD consiste nell'"*informare e fornire*

ne di servizi di telecomunicazioni; il reindirizzamento di messaggi di posta elettronica; attività di marketing basate sull'analisi dei dati raccolti; profilazione e *scoring* per finalità di valutazione del rischio (per esempio, a fini di valutazione del rischio creditizio, definizione dei premi assicurativi, prevenzione delle frodi, accertamento di forme di riciclaggio); tracciamento dell'ubicazione (per esempio da parte di app su dispositivi mobili); programmi di fidelizzazione; pubblicità comportamentale; monitoraggio di dati relativi allo stato di benessere psicofisico, alla forma fisica e alla salute attraverso dispositivi indossabili; utilizzo di telecamere a circuito chiuso; dispositivi connessi quali contatori intelligenti, automobili intelligenti, dispositivi per la domotica, ecc.

[32] Ai sensi della definizione contenuta all'articolo 4, punto 7, il titolare del trattamento è la persona o l'organismo che determina le finalità e i mezzi del trattamento.

[33] Ai sensi della definizione contenuta all'articolo 4, punto 8, il responsabile del trattamento è la persona o l'organismo che tratta dati personali per conto del titolare del trattamento.

[34] Cfr. articolo 38, paragrafo 4: "*Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento*".

[35] Cfr. articolo 39, paragrafo 1, lettera e): "*fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione*". Anche articolo 39, paragrafo 1, lettera a).

Pagine non disponibili in anteprima

25) «**servizio della società dell'informazione**»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio (1);

26) «**organizzazione internazionale**»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

Accountability Si tratta del principio di "*responsabilizzazione*" dei titolari del trattamento e dei responsabili del trattamento nell'adottare proattivamente comportamenti tali da dimostrare l'adozione di misure concrete per assicurare l'applicazione al GDPR.

Anonimizzazione Processo che rende i dati personali anonimi, in modo che la persona a cui i dati si riferiscono non possa più essere identificata.

Article 29 Working Party (abbreviato in **WP29** o **G29**; in italiano **Gruppo Articolo 29**) Gruppo di lavoro europeo indipendente su dati e tutela della privacy, organo consultivo indipendente istituito in conformità all'articolo 29 della Direttiva 95/46/CE sulla protezione dei dati personali. Il WP29, che riuniva i rappresentanti di ciascuna Autorità nazionale di protezione dei dati con la missione di contribuire a sviluppare standard europei adottando raccomandazioni e pareri, già a partire dal 25 maggio 2018 è stato sostituito dall'European Data Protection Board (EDPB) o Comitato europeo per la protezione dei dati. Tale nuovo organismo garantisce l'applicazione del Regolamento europeo. Per un opportuno approfondimento: www.edpb.europa.eu

Attività di monitoraggio Sistemi di videosorveglianza o di controllo degli strumenti messi a disposizione dei dipendenti per lo svolgimento della prestazione lavorativa (si pensi a: computer, telefoni, tablet ecc.), nonché gli strumenti di rilevazione degli accessi e delle presenze (c.d. lettori *badge*).

Attività principali Attività primarie svolte dal titolare del trattamento ovvero quelle che non fanno parte delle mere attività accessorie rispetto al trattamento dei dati svolto. In particolare, le attività principali sono le operazioni essenziali necessarie al raggiungimento degli obiettivi perseguiti dal titolare del trattamento o dal responsabile del trattamento o per le quali il trattamento di dati costituisca una componente inscindibile dalle attività svolte dal titolare del trattamento o dal responsabile del trattamento.

Audit Processo sistematico, indipendente e documentato teso a ottenere le evidenze dell'attività di monitoraggio e a valutarle secondo obiettività, al fine di stabilire in quale misura i criteri che regolano l'attività di audit siano stati effettivamente soddisfatti.

Autenticazione informatica L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità di un soggetto.

Autorità di controllo Una o più autorità pubbliche indipendenti che hanno il compito di assicurare il rispetto delle norme sulla privacy in ogni paese membro UE.

Autorità di controllo capofila Nel caso di trattamento transfrontaliero, è l'autorità di controllo dove ha sede il titolare o il responsabile del trattamento, alla quale viene trasferita la competenza sul trattamento stesso rispetto ad altre autorità di controllo (definite "*autorità interessate*"). Seguendo un "*principio di sportello unico*", quindi, per ogni trattamento

transfrontaliero il controllo viene svolto sotto la direzione di una sola autorità capofila. In queste ipotesi, l'attribuzione della competenza va quindi valutata con attenzione perché ci possono essere diversi casi, come ad esempio quello in cui una multinazionale ha la sede dell'amministrazione centrale in un paese, e in un altro paese ha uno stabilimento che assume decisioni autonome su finalità e mezzi di uno specifico trattamento.

Autorità o organismo pubblico o ente assimilato Si tratta delle autorità che hanno il mandato legale per governare, amministrare una parte o un aspetto della vita pubblica, come ad esempio tutti i rami del potere esecutivo di uno Stato, Provincia, Comune ecc. Alla luce delle Linee guida di interpretazione del Regolamento UE 2016/679, si considerano rientranti in questa definizione anche organismi privati incaricati di funzioni pubbliche o che esercitano pubblici poteri in ambiti quali, per esempio: trasporti pubblici, forniture idriche ed elettriche, infrastrutture stradali, emittenti radiotelevisive pubbliche, istituti per l'edilizia pubblica o organismi di disciplina professionale.

Azione di mitigazione o riduzione del rischio Azione volta a rendere più efficiente un processo riducendo l'impatto dei rischi associati al processo stesso. In pratica si tratta – ad esempio – di eseguire in modo automatico i *backup* degli archivi contenenti i dati personali, e non invece e soltanto manualmente.

Banca dati Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

Base giuridica del trattamento È il "*fondamento di liceità del trattamento*" o giustificazione per un'operazione di trattamento. Può consistere, per esempio, nel consenso dell'interessato, nell'adempimento di obblighi contrattuali o precontrattuali (è una forma speciale del consenso dell'interessato), in interessi vitali dell'interessato (per situazioni di vita o di morte, quali per esempio servizi di emergenza che ricevono un elenco di nomi ed età dei residenti al momento di rispondere a una chiamata di emergenza), in obblighi di legge cui è soggetto il titolare (si pensi ai registri di impiego, all'attività giornalistica, ai rapporti sugli incidenti nei registri relativi alla salute e sicurezza ecc.), nell'interesse pubblico/legittimo o esercizio di pubblici poteri (si pensi, per esempio, al caso di partiti politici autorizzati a gestire una copia del registro elettorale o anche ai casi di procedure adottate per prevenire le frodi, per la sicurezza, o ai casi di trasferimento di dati tra parti diverse della stessa azienda), ecc.

Blocco Conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.

Codici deontologici e di buona condotta Documenti di autoregolamentazioni di settore promosse ed approvate dall'Autorità Garante italiana, elaborate col concorso delle associazioni di un determinato settore. Sono introdotte già dal Codice della privacy (art. 12) la cui importanza è ribadita dal GDPR (art. 40).

Comitato Il Comitato europeo per la protezione dei dati (EDPB - European Data Protection Board) è un organismo dell'UE incaricato dell'applicazione del Regolamento generale sulla protezione dei dati a partire dal 25 maggio 2018. È composto dal responsabile di ciascuna autorità per la protezione dei dati e dal Garante europeo della protezione dei dati o dai loro rappresentanti. Può fare da consulente alla Commissione Europea in merito a qualsiasi questione relativa alla protezione dei dati personali nell'Unione.

Pagine non disponibili in anteprima

PRINCIPALI ADEMPIMENTI A CARICO DEL TITOLARE DEL TRATTAMENTO

Il rinnovato impianto normativo – sin qui descritto – in materia di "*protezione delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati*" sancisce una serie di adempimenti a carico del titolare del trattamento. Tali obblighi sono incentrati al principio di "*responsabilizzazione*", ovvero *accountability*, dato che il Legislatore affida agli stessi soggetti obbligati il compito di decidere le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle normative e dei criteri specifici indicati nel GDPR. Con un approccio operativo, il complesso dei nuovi obblighi che gravano a carico del titolare del trattamento può essere schematizzato come nella seguente tabella riepilogativa.
Nell'ultima colonna si riporta la sigla di identificazione dei moduli e dei documenti forniti in download e nelle pagine seguenti (si veda in Appendice il paragrafo "*Modulistica e documentazione varia*").

Obbligo/ Adempimento	Articoli di riferimento del GDPR	Definizione	Modulistica o documentazione di riferimento
Valutazione del rischio *(risk based approach*)	35, parr. 1, 3 e 4; 36, par. 1	Effettuare una valutazione dell'impatto sulla privacy (*Privacy Impact Assessment*) ossia l'analisi della valutazione dei rischi per i trattamenti previsti.	D1
Privacy by design* e *privacy by default	25	Il GDPR sancisce l'obbligo di assicurare che le misure adottate attuino efficacemente i principi di *privacy by design*, cioè la protezione dei dati fin dalla progettazione del sistema di protezione, e la *privacy by default*, cioè la privacy come impostazione predefinita che preveda il trattamento dei soli dati necessari al perseguimento delle finalità dichiarate. Il corretto adempimento di tale complesso obbligo comporta un'analisi preventiva da parte dei titolari del trattamento che tenga conto del contesto complessivo dove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.	M1A M1B M1C

segue

Obbligo/ Adempimento	Articoli di riferimento del GDPR	Definizione	Modulistica o documentazione di riferimento
Privacy assessment	35, par. 7	Si tratta della fase di mappatura dei dati da trattare; l'analisi dei soggetti addetti al trattamento e l'attività volta a individuare il sistema di *governance* della privacy descrittiva delle finalità dei trattamenti. L'attività prosegue con l'implementazione delle misure di sicurezza adottate per mitigare i rischi che dovrà tenere conto dell'analisi dei rischi e dei costi di attuazione. Nel caso in cui dovessero sussistere rischi residuali, il titolare ha la possibilità di consultare l'autorità di controllo competente per ottenere indicazioni per la gestione di tali rischi.	M20A M20B D3
Registro delle attività dei trattamenti dei dati personali	30	Il registro delle attività di trattamento deve essere tenuto da tutti i titolari e i responsabili, è indispensabile per ogni valutazione e analisi del rischio e deve essere esibito su richiesta del Garante. Il registro deve contenere le categorie dei soggetti interessati al trattamento; i dati trattati; i soggetti destinatari di comunicazione dei dati; i termini per la cancellazione da parte dei soggetti richiedenti; i comunicati aventi come destinatari i paesi terzi ovvero le specifiche organizzazioni internazionali; i ruoli e le responsabilità per i trattamenti; le misure di sicurezza tecniche/organizzative adottate per la protezione dei dati. Tali informazioni dovranno essere riportate nel registro in maniera aggiornata rispetto a tutti i trattamenti effettuati dal titolare e dal responsabile del trattamento.	M2

segue

Pagine non disponibili in anteprima

M1A

PRIVACY POLICY GENERALE PER SERVIZI VARI E SITO INTERNET

La nostra Società [inserire denominazione/ragione sociale e sede legale] ritiene che la protezione dei dati personali e la privacy dei nostri utenti siano assolutamente importanti. Il presente documento di informativa sulla privacy indica tutte le informazioni utili a consentire all'utente di comprendere quali dati raccogliamo, perché li raccogliamo e come li utilizziamo, nel rispetto della normativa applicabile. In caso di ulteriori ed eventuali domande ci potrà contattare al seguente indirizzo email: ..... . Sarà nostra cura risponderle nel più breve tempo possibile.

1. TITOLARE

Titolare del trattamento dei dati personali raccolti attraverso l'utilizzo del servizio di [inserire riferimento al servizio offerto agli utenti dall'Azienda, ad es. consulenza, organizzazione di eventi, servizi alla persona, ecc.] (di seguito, "*Servizio*") ed attraverso il sito web [inserire l'URL del sito] (di seguito, "*Sito*") per utenti italiani è: [nome dell'azienda] Sede legale ..... Telefono ..... e-mail: ..... (di seguito, "*Azienda*" o "*Società*").

2. DATI TRATTATI

2.1. Dati raccolti tramite il Servizio

L'Azienda raccoglie esclusivamente i dati personali che l'utente fornisce volontariamente registrandosi al o utilizzando il Servizio. Tra i dati forniti volontariamente dall'utente tramite l'utilizzo del Servizio potranno essere acquisiti dati personali quali:

- nome;
- cognome;
- codice fiscale;
- indirizzo di residenza;
- data di nascita;
- indirizzo email;
- [inserire gli altri tipi di dati personali raccolti dall'Azienda tramite il Servizio]

2.2 Dati raccolti tramite il Sito

[Specificare se si tratti di settori del Sito ad accesso "*libero*" o ad accesso "*riservato*"]
Per la consultazione della parte *"pubblica"* del Sito (ossia quella liberamente accessibile da ogni utente), non è previsto alcun conferimento di dati personali dell'utente.
A seguito della mera navigazione nelle pagine pubblicamente accessibili del Sito, alcuni dati di navigazione potranno essere in ogni caso raccolti automaticamente, tra cui:

- indirizzi IP;
- indirizzi URI (Uniform Resource Identifier) delle risorse richieste;

- orario e metodo utilizzato per formulare le richieste al server;
- codice numerico circa lo stato della risposta resa dal server (buon fine, errore, ecc.);
- [inserire gli altri tipi di dati di navigazione raccolti dall'Azienda tramite il Sito].

I dati di navigazione sono relativi al sistema operativo e all'ambiente informatico dell'utente la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di Internet.

[Attenzione: se si usa Google Analytics o altri strumenti simili, è il caso di inserire un messaggio come quello seguente]

L'Azienda utilizza a questo scopo uno strumento di terze parti (Google Analytics) per scopi esclusivamente statistici e di marketing. I dati sono tuttavia gestiti in forma completamente anonimizzata. Sebbene queste informazioni non siano raccolte per essere associate a interessati identificati, per loro natura potrebbero, attraverso elaborazioni ed associazioni con dati detenuti da terzi, consentire di identificare gli utenti. Questi dati vengono utilizzati al solo fine di ricavare informazioni statistiche anonime sull'uso del Sito e per controllarne il corretto funzionamento, e vengono cancellati immediatamente dopo l'elaborazione.

[Qualora siano in uso ulteriori strumenti di terze parti quali, per esempio Facebook, Twitter, altri social network, ecc., se ne deve dare atto, oltre a dover adempiere agli obblighi informativi da inserire nella cookie policy, se prevista]

Per l'accesso alla parte a contenuti riservati del Sito, oppure per ogni eventuale presa di contatto con l'Azienda da parte dell'utente attraverso, per esempio, l'invio di messaggi di posta elettronica ai recapiti dell'Azienda indicati nel Sito, i dati dell'utente dovranno considerarsi acquisiti e, quindi, trattati nel pieno rispetto della normativa vigente. Tali dati possono includere quelli forniti in fase di registrazione al Sito e di utilizzo delle aree riservate, quali ad esempio (oltre ai dati personali già indicati), nome utente, password, domande di sicurezza e relative risposte, eventuali documenti di identità caricati, ecc.

3. FINALITÀ DEL TRATTAMENTO

La Società tratta i dati personali che l'utente ha fornito tramite il Servizio o il Sito esclusivamente in connessione con l'utilizzo del Servizio o del Sito stesso. In particolare, i dati personali dell'utente possono essere utilizzati per le seguenti finalità:

a) erogazione del Servizio [indicare le attività di cui si compone il Servizio] e delle funzionalità del Sito, come registrazione, accesso alle aree riservate, comunicazione con l'Azienda, comunicazione con gli altri utenti, ecc. [se necessario aggiungere altre funzionalità offerte dal Sito];
b) elaborazione dei dati di pagamento e fatturazione: l'Azienda tratterà i dati personali dell'utente solo per facilitare gli acquisti relativi al Servizio e per elaborare i pagamenti effettuati, anche attraverso il Sito; in nessun modo la Società acquisirà i dati bancari dell'utente poiché ogni pagamento verrà eseguito tramite Paypal o altre piattaforme di pagamento di terze parti;
c) invio di informazioni sul Servizio, come, ad esempio, stato dei pagamenti, eventi, ecc. [specificare i servizi offerti] e di aggiornamenti sulle funzionalità del Sito, per esempio, via e-mail o posta [se l'utente ha prestato il suo consenso esplicito];
d) [indicare espressamente tutte le ulteriori diverse finalità per le quali potranno – anche solo opzionalmente e con il consenso esplicito dell'utente – essere utilizzati i