Collana **MultiCompact**
Professional aided software

Andrea Omar Bianco

GDPR
per i professionisti

GUIDA ALLE PROCEDURE PER L'ADEGUAMENTO

SOFTWARE INCLUSO
Gestionale dei servizi necessari all'adeguamento privacy alla normativa vigente in materia di GDPR (General Data Protection Regulation)

GRAFILL

Andrea Omar Bianco

GDPR PER I PROFESSIONISTI

Ed. I (12-2019)

ISBN 13 978-88-277-0102-7
EAN 9 788827 701027

Collana **Manuali** (252)

Bianco, Andrea Omar <1989->
GDPR per i professionisti / Andrea Omar Bianco.
– Palermo : Grafill, 2019.
(Manuali ; 252)
ISBN 978-88-277-0102-7
1. Diritto alla riservatezza – Tutela – Legislazione.
342.450858 CDD-23 SBN Pal0323282
CIP – Biblioteca centrale della Regione siciliana "Alberto Bombace"

Finito di stampare nel mese di dicembre 2019
presso **Tipografia Luxograph S.r.l.** Piazza Bartolomeo Da Messina, 2 – 90142 Palermo

SOMMARIO

INTRODUZIONE

Svolgere la propria professione diventa sempre più difficile! Un'ennesima incombenza normativa colpisce i Professionisti.

È il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, noto con il diminutivo di GDPR o RGPD.

Dal 25 di maggio 2018, tutte le attività che raccolgono o trattano dati personali saranno costrette a conformarsi.

La speranza di proroghe è vana. L'obiettivo è quello di scoraggiare gli abusi, i trafficanti di dati, l'approccio menefreghista nonché superficiale che fino alla riforma è stato perpetrato.

La normativa introdotta, mira alla difesa di un bene a cui pochi prestano attenzione, la privacy. Questo testo, vi consentirà di avere un valido supporto per gestire tutte le incombenze richieste quotidianamente sub materia.

1. *Svolgo la mia professione da solo!*

La normativa non prevede esenzioni e non tiene conto della strutturazione interna del professionista. Se possedete un titolo professionale senza esercitare allora potete chiudere questo libro.

2. *La precedente normativa?*

Il decreto legislativo 30 giugno 2003, n. 196[1], è stato integrato dall'entrata in vigore della nuova normativa europea. Grazie al decreto legislativo 10 agosto 2018, n. 101[2], il Governo ha conciliato la decaduta legislazione con la nuova normativa.

3. *E se facessi orecchie da mercante?*

Far finta di nulla sarebbe molto semplice. Chi penserebbe mai di denunciarmi? Il cliente fornisce la propria autorizzazione e non ha gli strumenti adatti per comprendere a fondo ciò che sottopongo alla sua attenzione. Pende completamente dalle mie labbra. Figurarsi poi se qualcuno verrà mai a casa mia per controllare i dati raccolti!

---

1 Decreto legislativo 30 giugno 2003, n. 196, recante «D*isposizioni 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, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*». Pubblicato sulla *Gazzetta Ufficiale* 29 luglio 2003, n. 174 – Suppl. Ord. n. 123.

2 Decreto legislativo 10 agosto 2018, n. 101, recante «*Codice in materia di protezione dei dati personali*». Pubblicato sulla *Gazzetta Ufficiale* 4 settembre 2018, n. 205.

Niente di più errato.

Sebbene sia difficile che il cliente possa essere parte attiva nella segnalazione di una eventuale violazione (in quanto ciò presupporrebbe la conoscenza di quest'ultimo dei propri diritti, nonché, la consapevolezza dei doveri del professionista e della normativa in quanto tale) questa possibilità non può dirsi remota.

A tal proposito, è opportuno considerare che il cliente potrebbe essere un professionista avente un buon livello di conoscenza della materia in oggetto. Ciò, senza mai dimenticare la macchina dello Stato che, in situazioni di difficoltà potrebbe strumentalizzare la normativa per fare cassa.

Infine, lo stesso Garante potrebbe rivolgere degli avvertimenti al Titolare del Trattamento o al Responsabile del trattamento sulla circostanza che l'attività svolta possa aver violato il GDPR, così da conformare i trattamenti alle disposizioni normative, specificandone tempi e modi.

Dunque, cosa accadrebbe se mancasse l'adeguamento?

L'articolo 83 e seguenti del GDPR disciplinano le ipotesi nelle quali è prevista l'applicazione di sanzioni amministrative, pecuniarie e/o penali.

Le prime, possono raggiungere i 10 milioni di euro o, se superiore, il 2% del fatturato mondiale. Ad esempio, nei casi di:

- violazione delle condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione;
- trattamento illecito di dati personali che non richiede l'identificazione dell'interessato;
- mancata o errata notificazione e/o comunicazione di un data *breach* all'Autorità nazionale competente;
- violazione dell'obbligo di nomina del DPO;
- mancata applicazione di misure di sicurezza.

L'importo delle **sanzioni amministrative pecuniarie** può salire fino a 20 milioni di euro, o alternativamente, sino al 4% del fatturato mondiale dell'impresa nelle ipotesi di:

- inosservanza di un ordine, di una limitazione provvisoria o definitiva concernente un trattamento, imposti da un'Autorità nazionale competente;
- trasferimento illecito *cross-border* di dati personali ad un destinatario in un Paese terzo.

4. *Fornitori*

Un altro aspetto importante riguarda il rapporto con le organizzazioni che vengono pagate per svolgere attività connesse al trattamento dei dati.

La normativa UE pone le stesse responsabilità del titolare in capo a tutti coloro i quali, su vostro incarico, collaborano al trattamento dei dati: consulente finanziario, web master, medico del lavoro, RSPP, dipendenti, collaboratori di studio, fornitori di servizi, domiciliatari, ecc..

La circostanza che le categorie appena citate vengano retribuite, non esime il titolare del trattamento (il professionista) dall'ipotesi di co-responsabilità obbligandolo, nel contempo, a regolarizzare il rapporto con i fornitori in ordine al trattamento dei dati.

5. *Tipologia di dati*

Durante lo svolgimento dell'attività professionale, vi troverete a dover acquisire informazioni collegate alla vita privata, professionale, pubblica del cliente. Ciò che farete, dunque, non sarà

altro che trattare «*dati personali*» ossia: nome, cognome, data di nascita, dati bancari, indirizzo postale, e-mail, fotografie, video, indirizzi IP, localizzazioni, ecc..

Inoltre, a seconda della prestazione professionale esercitata, potranno essere acquisiti «*dati particolari*», utili ad identificare un tratto caratteristico dell'identità del soggetto: fisica, genetica, psichica, fisiologica, economica, culturale, giuridica, ecc..

CAPITOLO 1

COSA SAPERE

1.1. Brevi cenni sulle novità introdotte dal GDPR

Il GDPR rivoluziona il modo in cui la privacy viene affrontata dalle singole realtà di tutta Europa, disciplinandola come mai prima d'ora ed istituendo un quadro formativo incentrato sui doveri e sulla responsabilizzazione del Titolare del trattamento.

Ad essere stato introdotto è il **principio di accountability** che comprende la definizione delle responsabilità all'interno delle singole organizzazioni.

Il **Titolare del trattamento**, ovvero il massimo **responsabile della tutela della privacy**, è tenuto al rispetto dei **principi previsti dal GDPR**, comprovandoli attraverso una serie di strumenti indicati dalla nuova normativa.

Ciò, è possibile attraverso una valutazione dei rischi e degli impatti antecedente all'avvio del trattamento di dati personali, nonché ad una progettazione strutturata della tutela della privacy stessa.

La riforma, richiede lo sviluppo di ulteriori **misure e tecniche organizzative** per comprovare l'adeguatezza dei propri sistemi come pure delle proprie pratiche, al fine di escludere, in caso di una violazione dei dati, una eventuale responsabilità.

Il GDPR introduce quindi due concetti chiave:

1) *Privacy by design*;
2) *Privacy by default*.

Il primo si riferisce alla necessità di progettare misure di sicurezza e privacy adeguate alle nuove esigenze e normative.

Il secondo invece alla capacità di disegnare misure di sicurezza e privacy per default, considerandole come un prerequisito fondamentale per il normale funzionamento dei sistemi informativi aziendali.

Ad essere ulteriormente evidenziati sono infine i **principi di liceità del trattamento**, trattamento possibile previa autorizzazione dell'interessato all'utilizzo dei propri dati personali, ma anche di **adeguatezza**, **pertinenza** e **non eccedenza dei dati** rispetto alle finalità per cui vengono raccolti e trattati.

La trasparenza in tal senso diventa fondamentale, come anche l'assoluto **rispetto della privacy** di ogni singolo individuo coinvolto.

Sicché, i sistemi, si fanno più trasparenti, maggiormente strutturati e specifici ma, soprattutto, a norma.

La presenza di una figura responsabile, che garantisca la tutela della privacy, non esclude che debba essere dimostrata la conoscenza e il rispetto della normativa. Tale adeguamento dovrà, dunque, essere provato attraverso una adeguata documentazione interna nonché attraverso una regolarizzazione conforme dei rapporti professionali e il possesso di qualifiche e certificazioni ufficiali (per chi intenda intraprendere la professione di Consulente Privacy).

Queste ultime, possono essere conseguite attraverso un corso dedicato all'aggiornamento riguardo la GDPR in aggiunta ad una sana esperienza sul campo.

1.2. Organigramma

Le figure chiavi indicate e disciplinate dal GDPR sono da ricondursi al Titolare(contitolare) e quindi il professionista/i, il Responsabile del trattamento che nella maggior parte dei casi è esterno con tutti gli eventuali Sub-Responsabili nominati da quest'ultimo, il **DPO/RPD** (difficilmente nominato perché sulla scorta della struttura dei professionisti non è obbligatoria la designazione) e gli autorizzati/incaricati dal trattamento dei dati.

La presenza di tutte queste figure dipende dalle dimensioni dello studio.

1.2.1. *Il Titolare del trattamento*

Il professionista è sempre il Titolare del Trattamento cioè colui il quale singolarmente o insieme ad altri professionisti, chiamati e nominati eventualmente Contitolari, scelgono le finalità e modalità di trattamento dei dati personali.

Nell'espletamento di questo potere il professionista deve avere piena e libera autonomia, in particolare per:

- valutare «*ab origine*» quali dati sia necessario acquisire;
- determinare le finalità del trattamento;
- adottare tutte le misure tecniche e organizzative adeguate per garantire il trattamento dei soli dati necessari ad ogni specifica finalità di trattamento;
- predisporre politiche interne (protocolli) conformi alla sua organizzazione e al Regolamento;
- dimostrare, in caso di controllo, che il trattamento è conforme al Regolamento (principio di *Accountability*) e di aver adottato misure tecniche e organizzative efficaci ed adeguate per proteggere i dati acquisiti.

1.2.2. *Contitolare del Trattamento*

«*La figura del contitolare del trattamento è prevista all'art. 26 "Contitolari del trattamento" GDPR, il quale precisa che i contitolari possono anche essere più di due. Gli stessi, inoltre, devono determinare congiuntamente le finalità e mezzi del trattamento (si veda Gruppo di lavoro articolo 29, Parere 1/2010 – WP 169).*

Si ravvisa dunque la necessità di una codecisione in merito alle finalità (perché) ed a i mezzi (come) di un determinato trattamento.

Tramite un accordo fra le parti, i contitolari hanno l'obbligo di determinare, in modo trasparente, le proprie responsabilità e i propri compiti sull'osservanza degli obblighi derivanti dal GDPR con particolare attenzione ai diritti dell'interessato e gli obblighi di fornire le informazioni previste al momento della raccolta (Art. 13 e art. 14).

Da un punto di vista prettamente pratico, per l'individuazione del contitolare del trattamento non vi sono diciamo differenze con i parametri di identificazione ex art. 4.7.

"L'insieme ad altri" si riferisce, così come riportato nell'articolo, alla figura del contitolare prevista all'art. 26 "…due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi…".

CAPITOLO 2

COSA FARE

2.1. Introduzione

In questo capitolo si cercherà di dare delle linee guida al fine di garantire una conformità valida dello studio del professionista ai dettati normativi.

Prima di iniziare il professionista deve porsi delle domande, ossia:

«1) *Ho verificato se i dati dei miei clienti in mio possesso acquisiti prima dell'entrata in vigore della normativa europea sono stati acquisiti nel rispetto del vecchio Codice privacy e se sono stati superati i termini di conservazione?*

2) *Ho predisposto tutta la modulistica per procedere, durante il primo incontro con il Cliente, alla raccolta dei dati fornendo allo stesso una informativa completa, semplice e chiara?*

3) *Ho organizzato le mie attività in modo da raccogliere e trattare solo ed esclusivamente dati necessari o utili in vista dell'espletamento del mandato professionale ricevuto?*

4) *Ho organizzato la conservazione dei documenti relativi alle varie pratiche in modo da averne sempre, al momento giusto, la disponibilità ed in modo che i dati siano accessibili al solo personale autorizzato?*

5) *Ho nominato e adeguatamente istruito i miei collaboratori e dipendenti?*

6) *Ho formalizzato mediante apposita nomina i rapporti con i professionisti ai quali mi rivolgo per la gestione e lo sviluppo delle attività dello studio?*

7) *Detengo e aggiorno regolarmente i miei Registri da Titolare, da Responsabile Esterno o in caso da Domiciliatario?*

8) *I miei PC sono protetti dalle minacce esterne?*

9) *Dispongo, in caso di bisogno, di un tecnico-informatico di fiducia al quale rivolgermi per la soluzione di specifici problemi?*

10) *Provvedo ad eseguire un salvataggio integrale (backup) di tutti i dati su i PC perlomeno 1 volta alla settimana?*

11) *Ho definito un tempo di conservazione dei dati personali in linea con le finalità dei trattamenti.*

12) *Mi sono preoccupato della sicurezza fisica dello studio, ossia adottare misure o cautele atte ragionevolmente a prevenire accessi indesiderati e azioni concretantesi nella lesione della riservatezza, disponibilità, integrità delle banche dati?*

13) *Quando devo rottamare PC, Notebook e altri strumenti elettronici utilizzati per le attività dello studio, mi assicuro che la dismissione avvenga nel rispetto della esigenza di protezione dei dati?*

14) *Portatili e altri strumenti informatici rimovibili sono utilizzati al di fuori dello studio in modo da minimizzare i rischi di perdita accidentale, sottrazione fraudolenta e similari?*»[1].

Se la risposta ad ogni domanda è positiva allora possiamo affermare che lo studio è effettivamente adeguato al Regolamento. Nel caso in cui manchi anche una delle risposte in oggetto si può affermare, a seconda della domanda o che non si è adeguati o che vi sia un alto rischio di violazione del dato per il quale è necessario intervenire.

2.2. Verifica del consenso e dei dati acquisiti antecedentemente alla riforma

Il professionista come prima incombenza deve verificare di essere in possesso di un consenso e che quest'ultimo sia stato acquisito in modo valido.

Considerando l'art. 43, n. 9, altre disposizioni del Codice: artt. 18, 20, possiamo dire che il garante attribuisce essenzialmente la valida base giuridica del trattamento del consenso ottenuto prima della data di entrata in vigore del Regolamento europeo purché sia stato raccolto con modalità tali per cui risulti «*esplicito*» (se riferito a dati sensibili e a decisioni basate su trattamenti automatizzati), «*libero, specifico, informato*» e «*manifestato attraverso dichiarazione o azione positiva inequivocabile*» (se riferito a dati ordinari).

In sintesi il professionista deve verificare di aver fornito e ottenuto dal suo cliente o tramite un informativa ad hoc o tramite un consenso all'interno di un altro documento (ad es. il mandato, un contratto di servizio, ecc.) un documento che rispetti i dettami del D.Lgs. n. 196/2003. In questo caso dovrà fornire un **supplemento** di informativa con le nuove informazioni richieste in base alle norme e alla piena trasparenza (vedi l'articolo 5, comma 1, lettera *a)*), offrendo contestualmente agli interessati la possibilità di **revocare** il consenso originariamente fornito e naturalmente specificando le eventuali conseguenze di tale revoca.

Ipotizzandone la mancanza o l'inadeguatezza delle modalità il Professionista obbligatoriamente dovrà richiedere ai suoi clienti, seguendo le nuove indicazioni e presentando un formato informativo tale da ottenere dai vecchi clienti un legittimo consenso, l'autorizzazione al trattamento dei loro dati. In tal guisa, non sorgono problemi se il cliente è reperibile ed ancora seguito dallo studio perché l'acquisizione del Consenso sarà indubbiamente facile.

Nel caso in cui l'assistito non fosse più cliente occorrerà richiedere il consenso per i dati per i quali il professionista è tenuto per legge alla conservazione. In caso di irreperibilità lasciare sempre traccia del tentativo di regolarizzazione del rapporto sotto il profilo privacy, mediante ricevuta della raccomandata AR, una email, pec, un fax, ecc., così da poter detenere e conservare, per il tempo previsto dalla legge, i dati che allo scadere andranno distrutti o resi anonimi.

Nel caso di persona fisica defunta oppure in caso di società ormai estinta, occorrerà:

– in caso di persona fisica, non si potrà richiedere il consenso ma bisognerà attendere lo scadere dei termini di legge per procedere alla distruzione o anonimizzazione;

[1] Decalogo a cura dell'Avv. Paolo Marini, Altalex 2018.

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)*.

(Testo rilevante ai fini del SEE)

[G.U.U.E. 4/05/2016, L 119]

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

Visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 16, vista la proposta della Commissione europea, previa trasmissione del progetto di atto legislativo ai parlamenti nazionali, visto il parere del Comitato economico e sociale europeo ([1]),

Visto il parere del Comitato delle regioni ([2]), deliberando secondo la procedura legislativa ordinaria ([3]), considerando quanto segue:

1. La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («*Carta*») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («*TFUE*») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

2. I principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali dovrebbero rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza. Il presente regolamento è inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche.

3. La direttiva 95/46/CE del Parlamento europeo e del Consiglio ([4]) ha come obiettivo di armonizzare la tutela dei diritti e delle libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati e assicurare la libera circolazione dei dati personali tra Stati membri.

4. Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la

---

1 GU C 229 del 31.7.2012, pag. 90.

2 GU C 391 del 18.12.2012, pag. 127.

3 Posizione del Parlamento europeo del 12 marzo 2014 (non ancora pubblicata nella *Gazzetta ufficiale*) e posizione del Consiglio in prima lettura dell'8 aprile 2016 (non ancora pubblicata nella *Gazzetta ufficiale*). Posizione del Parlamento europeo del 14 aprile 2016.

4 Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281 del 23.11.1995, pag. 31).

libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica.

5. L'integrazione economica e sociale conseguente al funzionamento del mercato interno ha condotto a un considerevole aumento dei flussi transfrontalieri di dati personali e quindi anche dei dati personali scambiati, in tutta l'Unione, tra attori pubblici e privati, comprese persone fisiche, associazioni e imprese. Il diritto dell'Unione impone alle autorità nazionali degli Stati membri di cooperare e scambiarsi dati personali per essere in grado di svolgere le rispettive funzioni o eseguire compiti per conto di un'autorità di un altro Stato membro.

6. La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. 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. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali.

7. Tale evoluzione richiede un quadro più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno. È opportuno che le persone fisiche abbiano il controllo dei dati personali che li riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche.

8. Ove il presente regolamento preveda specificazioni o limitazioni delle sue norme ad opera del diritto degli Stati membri, gli Stati membri possono, nella misura necessaria per la coerenza e per rendere le disposizioni nazionali comprensibili alle persone cui si applicano, integrare elementi del presente regolamento nel proprio diritto nazionale.

9. Sebbene i suoi obiettivi e principi rimangano tuttora validi, la direttiva 95/46/CE non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche. La compresenza di diversi livelli di protezione dei diritti e delle libertà delle persone fisiche, in particolare del diritto alla protezione dei dati personali, con riguardo al trattamento di tali dati negli Stati membri può ostacolare la libera circolazione dei dati personali all'interno dell'Unione. Tali differenze possono pertanto costituire un freno all'esercizio delle attività economiche su scala dell'Unione, falsare la concorrenza e impedire alle autorità nazionali di adempiere agli obblighi loro derivanti dal diritto dell'Unione. Tale divario creatosi nei livelli di protezione è dovuto alle divergenze nell'attuare e applicare la direttiva 95/46/CE.

10. 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, il livello di protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di tali dati dovrebbe essere equivalente in tutti gli Stati membri. È opportuno assicurare un'applicazione coerente e omogenea delle norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali in tutta l'Unione. Per quanto riguarda il trattamento dei

dati personali per l'adempimento di un obbligo legale, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, gli Stati membri dovrebbero rimanere liberi di mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione delle norme del presente regolamento. In combinato disposto con la legislazione generale e orizzontale in materia di protezione dei dati che attua la direttiva 95/46/CE gli Stati membri dispongono di varie leggi settoriali in settori che richiedono disposizioni più specifiche. Il presente regolamento prevede anche un margine di manovra degli Stati membri per precisarne le norme, anche con riguardo al trattamento di categorie particolari di dati personali («*dati sensibili*»). In tal senso, il presente regolamento non esclude che il diritto degli Stati membri stabilisca le condizioni per specifiche situazioni di trattamento, anche determinando con maggiore precisione le condizioni alle quali il trattamento di dati personali è lecito.

11. Un'efficace protezione dei dati personali in tutta l'Unione presuppone il rafforzamento e la disciplina dettagliata dei diritti degli interessati e degli obblighi di coloro che effettuano e determinano il trattamento dei dati personali, nonché poteri equivalenti per controllare e assicurare il rispetto delle norme di protezione dei dati personali e sanzioni equivalenti per le violazioni negli Stati membri.

12. L'articolo 16, paragrafo 2, TFUE conferisce al Parlamento europeo e al Consiglio il mandato di stabilire le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale e le norme relative alla libera circolazione di tali dati.

13. Per assicurare un livello coerente di protezione delle persone fisiche in tutta l'Unione e prevenire disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno, è necessario un regolamento che garantisca certezza del diritto e trasparenza agli operatori economici, comprese le micro, piccole e medie imprese, offra alle persone fisiche in tutti gli Stati membri il medesimo livello di diritti azionabili e di obblighi e responsabilità dei titolari del trattamento e dei responsabili del trattamento e assicuri un monitoraggio coerente del trattamento dei dati personali, sanzioni equivalenti in tutti gli Stati membri e una cooperazione efficace tra le autorità di controllo dei diversi Stati membri. Per il buon funzionamento del mercato interno è necessario che la libera circolazione dei dati personali all'interno dell'Unione non sia limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali. Per tener conto della specifica situazione delle micro, piccole e medie imprese, il presente regolamento prevede una deroga per le organizzazioni che hanno meno di 250 dipendenti per quanto riguarda la conservazione delle registrazioni. Inoltre, le istituzioni e gli organi dell'Unione e gli Stati membri e le loro autorità di controllo sono invitati a considerare le esigenze specifiche delle micro, piccole e medie imprese nell'applicare il presente regolamento. La nozione di micro, piccola e media impresa dovrebbe ispirarsi all'articolo 2 dell'allegato della raccomandazione 2003/361/CE della Commissione ([5]).

14. È opportuno che la protezione prevista dal presente regolamento si applichi alle persone fisiche, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al trattamento dei loro dati personali. Il presente regolamento non disciplina il trattamento dei dati personali relativi a persone giuridiche, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto.

---

[5] Raccomandazione della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese (C(2003) 1422) (GU L 124 del 20.5.2003, pag. 36).

15. Al fine di evitare l'insorgere di gravi rischi di elusione, la protezione delle persone fisiche dovrebbe essere neutrale sotto il profilo tecnologico e non dovrebbe dipendere dalle tecniche impiegate. La protezione delle persone fisiche dovrebbe applicarsi 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. Non dovrebbero rientrare nell'ambito di applicazione del presente regolamento i fascicoli o le serie di fascicoli non strutturati secondo criteri specifici, così come le rispettive copertine.

16. Il presente regolamento non si applica a questioni di tutela dei diritti e delle libertà fondamentali o di libera circolazione dei dati personali riferite ad attività che non rientrano nell'ambito di applicazione del diritto dell'Unione, quali le attività riguardanti la sicurezza nazionale. Il presente regolamento non si applica al trattamento dei dati personali effettuato dagli Stati membri nell'esercizio di attività relative alla politica estera e di sicurezza comune dell'Unione.

17. Il regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio ([6]) si applica al trattamento di dati personali effettuato da istituzioni, organi, uffici e agenzie dell'Unione. Il regolamento (CE) n. 45/2001 e gli altri atti giuridici dell'Unione applicabili a tale trattamento di dati personali dovrebbero essere adeguati ai principi e alle norme stabiliti dal presente regolamento e applicati alla luce dello stesso. Per offrire un quadro di protezione dei dati solido e coerente nell'Unione, si dovrebbe procedere, successivamente all'adozione del presente regolamento, ai necessari adeguamenti del regolamento (CE) n. 45/2001, al fine di consentirne l'applicazione contemporaneamente al presente regolamento.

18. Il presente regolamento non si applica al trattamento di dati personali effettuato da una persona fisica nell'ambito di attività a carattere esclusivamente personale o domestico e quindi senza una connessione con un'attività commerciale o professionale. Le attività a carattere personale o domestico potrebbero comprendere la corrispondenza e gli indirizzari, o l'uso dei social network e attività online intraprese nel quadro di tali attività. Tuttavia, il presente regolamento si applica ai titolari del trattamento o ai responsabili del trattamento che forniscono i mezzi per trattare dati personali nell'ambito di tali attività a carattere personale o domestico.

19. La protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro, e la prevenzione di, minacce alla sicurezza pubblica, e la libera circolazione di tali dati sono oggetto di uno specifico atto dell'Unione. Il presente regolamento non dovrebbe pertanto applicarsi ai trattamenti effettuati per tali finalità. I dati personali trattati dalle autorità pubbliche in forza del presente regolamento, quando utilizzati per tali finalità, dovrebbero invece essere disciplinati da un più specifico atto dell'Unione, segnatamente la direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio ([7]). Gli Stati membri possono conferire alle autorità competenti ai sensi della direttiva (UE) 2016/680 altri compiti che non siano necessariamente svolti a fini di prevenzione, indagine, accertamento

---

6 Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati (GU L 8 del 12.1.2001, pag. 1).

7 Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (Cfr. pagina 89 della presente *Gazzetta ufficiale*).

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).

[G.U.R.I. 4/09/2018, N. 205]

IL PRESIDENTE DELLA REPUBBLICA

Visti gli articoli 76 e 87 della Costituzione;

Vista la legge 25 ottobre 2017, n. 163, recante delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea – Legge di delegazione europea 2016-2017, e in particolare l'articolo 13, che delega il Governo all'emanazione di uno o più decreti legislativi di adeguamento del quadro normativo nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016;

Vista la legge 24 dicembre 2012, n. 234, recante norme generali sulla partecipazione dell'Italia alla formazione e all'attuazione della normativa e delle politiche dell'Unione europea;

Visto il Codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196;

Visto il 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);

Vista la direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio;

Vista la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;

Vista la direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche;

Visto il decreto legislativo 18 maggio 2018, n. 51, recante attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio;

Vista la preliminare deliberazione del Consiglio dei ministri, adottata nella riunione del 21 marzo 2018;

Acquisito il parere del Garante per la protezione dei dati personali, adottato nell'adunanza del 22 maggio 2018;

Acquisiti i pareri delle competenti Commissioni parlamentari della Camera dei deputati e del Senato della Repubblica;

Vista la deliberazione del Consiglio dei ministri, adottata nella riunione dell'8 agosto 2018;

Sulla proposta del Presidente del Consiglio dei ministri e dei Ministri per gli affari europei e della giustizia, di concerto con i Ministri per la pubblica amministrazione, degli affari esteri e della cooperazione internazionale, dell'economia e delle finanze e dello sviluppo economico;

EMANA

il seguente decreto legislativo:

Capo I

Modifiche al titolo e alle premesse del codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196

Art. 1

Modifiche al titolo e alle premesse del decreto legislativo 30 giugno 2003, n. 196

1. Al titolo del decreto legislativo 30 giugno 2003, 196, dopo le parole «dati personali» sono aggiunte le seguenti: «, recante disposizioni per l'adeguamento dell'ordinamento nazionale al 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».

2. Alle premesse del decreto legislativo 30 giugno 2003, n. 196, dopo il terzo Visto sono inseriti i seguenti:

«Vista la legge 25 ottobre 2017, n. 163, recante delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea – Legge di delegazione europea 2016-2017» e, in particolare, l'articolo 13, che delega il Governo all'emanazione di uno o più decreti legislativi di adeguamento del quadro normativo nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016;

Vista la legge 24 dicembre 2012, n. 234, recante norme generali sulla partecipazione dell'Italia alla formazione e all'attuazione della normativa e delle politiche dell'Unione europea;

Visto il 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);».

Capo II

Modifiche alla parte i del codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196

Art. 2

Modifiche alla parte I, titolo I, del decreto legislativo 30 giugno 2003, n. 196

1. Alla parte I, titolo I, del decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:

a) la rubrica del titolo I è sostituita dalla seguente: «Principi e disposizioni generali»;

b) prima dell'articolo 1 è inserito il seguente Capo:

«Capo I (*Oggetto, finalità e Autorità di controllo*)»;

c) l'articolo 1 è sostituito dal seguente:

«Art. 1 (*Oggetto*). – 1. Il trattamento dei dati personali avviene secondo le norme del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, di seguito «Regolamento», e del presente codice, nel rispetto della dignità umana, dei diritti e delle libertà fondamentali della persona.»;

d) l'articolo 2 è sostituito dal seguente:

«Art. 2 (*Finalità*). – 1. Il presente codice reca disposizioni per l'adeguamento dell'ordinamento nazionale alle disposizioni del regolamento.»;

e) dopo l'articolo 2 è inserito il seguente:

«Art. 2-*bis* (*Autorità di controllo*). – 1. L'Autorità di controllo di cui all'articolo 51 del regolamento è individuata nel Garante per la protezione dei dati personali, di seguito «Garante», di cui all'articolo 153.»;

f) dopo l'articolo 2-*bis* sono inseriti i seguenti Capi:

«Capo II (*Principi*) – Art. 2-*ter* (*Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*). – 1. La base giuridica prevista dall'articolo 6, paragrafo 3, lettera *b)*, del regolamento è costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento.

2. La comunicazione fra titolari che effettuano trattamenti di dati personali, diversi da quelli ricompresi nelle particolari categorie di cui all'articolo 9 del Regolamento e di quelli relativi a condanne penali e reati di cui all'articolo 10 del Regolamento, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri è ammessa se prevista ai sensi del comma 1. In mancanza di tale norma, la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di compiti di interesse pubblico e lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di quarantacinque giorni dalla relativa comunicazione al Garante, senza che lo stesso abbia adottato una diversa determinazione delle misure da adottarsi a garanzia degli interessati.

3. La diffusione e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalità sono ammesse unicamente se previste ai sensi del comma 1.

4. Si intende per:

a) "*comunicazione*", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-*quaterdecies*, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;

b) "*diffusione*", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Art. 2-*quater* (*Regole deontologiche*). – 1. Il Garante promuove, nell'osservanza

del principio di rappresentatività e tenendo conto delle raccomandazioni del Consiglio d'Europa sul trattamento dei dati personali, l'adozione di regole deontologiche per i trattamenti previsti dalle disposizioni di cui agli articoli 6, paragrafo 1, lettere *c)* ed *e)*, 9, paragrafo 4, e al capo IX del Regolamento, ne verifica la conformità alle disposizioni vigenti, anche attraverso l'esame di osservazioni di soggetti interessati e contribuisce a garantirne la diffusione e il rispetto.

2. Lo schema di regole deontologiche è sottoposto a consultazione pubblica per almeno sessanta giorni.

3. Conclusa la fase delle consultazioni, le regole deontologiche sono approvate dal Garante ai sensi dell'articolo 154-*bis*, comma 1, lettera *b)*, pubblicate nella *Gazzetta Ufficiale* della Repubblica italiana e, con decreto del Ministro della giustizia, sono riportate nell'allegato A del presente codice.

4. Il rispetto delle disposizioni contenute nelle regole deontologiche di cui al comma 1 costituisce condizione essenziale per la liceità e la correttezza del trattamento dei dati personali.

Art. 2-*quinquies* (*Consenso del minore in relazione ai servizi della società dell'informazione*). – 1. In attuazione dell'articolo 8, paragrafo 1, del Regolamento, il minore che ha compiuto i quattordici anni può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione. Con riguardo a tali servizi, il trattamento dei dati personali del minore di età inferiore a quattordici anni, fondato sull'articolo 6, paragrafo 1, lettera *a)*, del Regolamento, è lecito a condizione che sia prestato da chi esercita la responsabilità genitoriale.

2. In relazione all'offerta diretta ai minori dei servizi di cui al comma 1, il titolare del trattamento redige con linguaggio particolarmente chiaro e semplice, conciso ed esaustivo, facilmente accessibile e comprensibile dal minore, al fine di rendere significativo il consenso prestato da quest'ultimo, le informazioni e le comunicazioni relative al trattamento che lo riguardi.

Art. 2-*sexies* (*Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante*). – 1. I trattamenti delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento, necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera *g)*, del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

2. Fermo quanto previsto dal comma 1, si considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle seguenti materie:

a) accesso a documenti amministrativi e accesso civico;

b) tenuta degli atti e dei registri dello stato civile, delle anagrafi della popolazione residente in Italia e dei cittadini italiani residenti all'estero, e delle liste elettorali, nonché rilascio di documenti di riconoscimento o di viaggio o cambiamento delle generalità;

IL SOFTWARE GESTIONALE GDPR ALLEVOLUTION PRIVACY

L'acquisto della presente pubblicazione include un abbonamento al software gestionale GDPR **Allevolution Privacy** (*versione completa*) di *Allevolution s.r.l.s.*. Il software fornisce servizi necessari all'adeguamento privacy e al suo mantenimento e, per chi non ha mai avuto un sistema informatico di gestione della propria attività rappresenta, altresì, un valido supporto per registrare clienti, fornitori, dipendenti, collaboratori e consulenti.

L'utente di **Allevolution Privacy** avrà a disposizione tutto ciò che serve per l'adeguamento alla normativa vigente in materia di GDPR. Il software gestionale funziona in Cloud e, con una semplice connessione internet, è accessibile da qualsiasi luogo e con qualunque dispositivo.

Ogni area del software riporta tutti i documenti di riferimento, predisposti per singola categoria e per ogni esigenza professionale; in questo modo l'utente potrà scegliere, in base alle proprie esigenze, se utilizzare i documenti base oppure modificarli o integrarli. Inoltre, grazie alla funzione anagrafiche, i dati verranno inseriti automaticamente all'interno dei documenti.

Registri e documenti sono costantemente aggiornati alle modifiche normative e alle pronunce del garante e, grazie ad un editor di testo integrato, per la creazione dei documenti non è necessario utilizzare software di terze parti.

Allevolution Privacy (*versione completa*) è concesso in abbonamento gratuito per 12 mesi e dovrà essere attivato entro sei mesi dalla ricezione del voucher Grafill (vedi punto 5 del paragrafo seguente). La mancata attivazione entro il suddetto periodo farà decadere il diritto all'abbonamento gratuito. Trascorsi 12 mesi dall'attivazione dell'abbonamento, in mancanza di disdetto dall'utente, secondo i termini e le condizioni contrattuali previste, l'abbonamento si rinnoverà per altri 12 mesi al prezzo di listino consultabile sul sito **www.allevolution.it.**

Attivazione del software gestionale GDPR Allevolution Privacy

1) Collegarsi al seguente indirizzo internet:

https://www.grafill.it/pass/0102_7.php

2) Inserire i codici "**A**" e "**B**" (vedi ultima pagina del volume) e cliccare **[Continua]**;
3) **Utenti già registrati su www.grafill.it**: inserire i dati di accesso e cliccare **[Accedi]**, accettare la licenza d'uso e cliccare **[Continua]**;
4) **Utenti non ancora registrati su www.grafill.it**: cliccare **[Iscriviti]**, compilare il form di registrazione e cliccare **[Iscriviti]**, accettare la licenza d'uso e cliccare **[Continua]**;
5) Un voucher per l'attivazione del software gestionale GDPR **Allevolution Privacy** sarà inviato all'indirizzo e-mail inserito nel form di registrazione.

Il software gestionale GDPR **Allevolution Privacy** contiene le seguenti funzioni.

Anonimizzazione

Allevolution Privacy è un supporto per l'anonimizzazione della documentazione del cliente. Compilando l'anagrafica clienti è possibile collegare la relativa documentazione e, grazie all'assegnazione di un codice, sarà possibile trovarla facilmente. Ciò permette di garantire l'anonimato ed è una funzione molto utile, soprattutto per i professionisti e nella loro gestione dei fascicoli.

Anagrafiche

Con il software è possibile creare e gestire le anagrafiche di clienti, fornitori, dipendenti, Dpo, collaboratori e di tutte le figure coinvolte. Inoltre, è possibile conservare (funzione riservata a professionisti) Nomine/Contratti del Cliente e la Dichiarazione Antiriciclaggio.

Archiviazione e backup

Il software consente l'archiviazione illimitata dei documenti inseriti nel gestionale ed è previsto un sistema di backup giornaliero dei dati.

Definizione dei ruoli

È possibile nominare gli autorizzati al trattamento, i responsabili del trattamento e i responsabili della protezione dei dati (*Data Protection Officer*) utilizzando la modulistica disponibile.

Trattamenti: analisi e registri delle attività

Il software consente di definire trattamenti illimitati, le finalità di ognuno e di generare in automatico il registro delle attività del titolare (che è già compilato); inoltre, è possibile:

- definire i registri dei responsabili esterni per ogni cliente;
- definire il registro della violazione dei dati (*Data Breach*) e, per i professionisti, il registro del trattamento per le domiciliazioni; per ogni singola categoria di appartenenza è possibile inserire tutti i possibili e prevedibili trattamenti;
- compilare le voci richieste in base alle necessità ed eliminare le parti già indicate se non corrispondono alle tue esigenze;
- eseguire una modifica del registro, grazie ad lista con una serie di possibili voci per ogni singola richiesta che permette di completare i campi mancanti.

Gestione delle lettere di incarico e di revoca

È possibile generare facilmente le lettere di incarico o di revoca per tutte le figure coinvolte nel processo di tutela della privacy aziendale.

Gestione dell'accordo tra i contitolari del trattamento

Attraverso un apposito documento già predisposto, è possibile predisporre l'accordo del trattamento sulla distribuzione dei ruoli per i contitolari, in modo da definire le responsabilità.

Richieste di consenso e la loro archiviazione

In linea con la normativa europea, è possibile creare automaticamente le richieste di consenso e archiviare i consensi ottenuti.

Data Breach

Il software consente di redigere la comunicazione di violazione dei dati personali da destinare al garante e agli interessati. È possibile inviarla tramite il software e conservarne la copia.

Personalizzazione dei documenti

Il software consente di personalizzare tutti i documenti inseriti.

Audit

Il software consente svolgere *audit privacy* e archiviare le risultanze. L'*audit privacy* è uno strumento di verifica della conformità dell'azienda relativamente alla conservazione del trattamento dei dati. Durante l'*audit* vengono svolte verifiche formali ed evidenziate situazioni critiche o prassi errate. L'*audit privacy* rappresenta per ogni azienda la prova di una costante attenzione verso i trattamenti effettuati in conformità alla normativa privacy.

Tipica attività *pre-audit* è l'analisi accurata della documentazione privacy utilizzata in azienda che prende in esame: le procedure, il flusso, la conservazione dei dati e la loro custodia, il tipo di accesso ai dati consentito al personale, nonché le modalità di esecuzione del trattamento. Specifica attenzione viene dedicata al sistema informatico, ciò al fine di assicurarci che esso sia a norma e che i dati siano presidiati da sufficienti misure di sicurezza.

Al termine dell'*audit* vengono evidenziate situazioni critiche o prassi errate nel trattamento dei dati personali. Vengono, inoltre, ipotizzate delle soluzioni quantificabili e misurabili da parte del management.

L'*audit privacy* rappresenta un momento fondamentale, poiché esso fornisce una prova costante di conformità e consente all'Organismo di Vigilanza di ottenere evidenze circa quello che è il sistema di protezione dei dati informatici.

Valutazione dei rischi e PIA

Il cliente sarà in grado di analizzare tutti i rischi del trattamento e ottenere una valutazione pre-misure di mitigazione e post-misure di mitigazione adottate. Inoltre, grazie alle sue istruzioni, supporti e guide, il cliente potrà munirsi di valide soluzioni per contenere e/o eliminare i rischi fisici e informatici dei trattamenti.

Il software consente di gestire la PIA, cioè la valutazione di impatto della protezione dei dati. Infatti, è possibile scaricare un gestionale ufficiale della CNIL dedicato alla redazione della Pia, con il quale si potrà eseguire la valutazione di impatto.

Violazione dei dati ed Esercizio dei Diritti dell'Interessato

Il software gestisce la comunicazione al garante privacy di perdite e furti dei dati aziendali, e quindi l'esercizio dei diritti dell'interessato. Il software redige, invia per email e archivia la segnalazione del *Data Breach* al garante e agli interessati. Inoltre, usando il registro *Data Breach* si potrà documentare la violazione.

Protocolli

Il software presenta un complesso di regole e procedure cui ci si deve attenere in determinate attività, utili per l'adozione di istruzioni e misure fondamentali per garantire il rispetto della normativa. Queste procedure possono essere ampliate ed è possibile predisporne di nuove.

Nel caso in cui abbiate necessità di ulteriori protocolli ossia Protocollo per la Cancellazione e Smaltimento dei supporti elettronici, Protocollo per la gestione delle utenze abilitate al trattamento dei dati e delle informazioni personali, Protocollo per il corretto utilizzo delle risorse informative aziendali, Protocollo per la gestione dei diritti dell'Interessato, Protocollo Data Breach, Protocollo per gli Amministratori di Sistema, ecc.. Consultare il listino Consulenza Protocolli del fornitore del servizio.

Formazione

Attraverso slide e documenti hai una visione completa sui principali adempimenti previsti per il GDPR, puoi consultare il regolamento e il D.Lgs. n. 101/2018 e avere delle guide sempre aggiornate sugli adempimenti. Tramite nostri consulenti si potranno effettuare sia formazioni in *e-learning* sia frontali. In questo caso visionare il pacchetto Formazione.

Multi-accesso

Il software consente l'accesso a più utenti, al fine di ottemperare alle varie incombenze, facilitando così le procedure di adeguamento.

Servizio di consulenza

È possibile usufruire di un servizio di formazione, nonché implementare la documentazione in proprio possesso. È possibile richiedere il Mog 679 e una consulenza per le fasi di adeguamento e mantenimento dello stesso; in tal caso richiedere una consulenza alla *Allevolution s.r.l.s.*.

Personalizzazioni

È possibile usufruire di un servizio di personalizzazione delle funzioni del gestionale. Oltre all'adeguamento l'utente potrà chiedere di inserire altri servizi che possono essere oggetto di digitalizzazione; in tal caso richiedere una consulenza alla *Allevolution s.r.l.s.*.

Collana **MultiCompact**
Professional aided software

Le modifiche introdotte attraverso il Regolamento (UE) 2016/679 e la normativa nazionale in materia privacy (D.Lgs. n. 101/2018) hanno assunto importanza rilevante per tutti, professionisti compresi e da qui l'esigenza di produrre un testo a taglio tecnico-scientifico che consenta la corretta comprensione dell'apparato normativo e delle prassi da seguire. La presente pubblicazione si configura come un manuale teorico-pratico per professionisti che vogliono adeguarsi alla riforma. Una parte è dedicata alla normativa sulla gestione del trattamento dei dati per la professione. Sono riportati esempi, checklist, modulistiche (informative, registri, audit), procedure, linee guida e prassi per la propria realtà professionale. Nel testo sono riportate informazioni utili sulla formazione dei collaboratori, al fine di evitare errori nell'applicazione della norma, e per creare un valido sistema interno ed esterno di misure tecniche e organizzative, sia fisiche che informatiche, volto al rispetto del art. 32 del Regolamento, e ad evitare la violazioni dei dati (data breach).

SOFTWARE INCLUSO

L'acquisto della presente pubblicazione include, in abbonamento gratuito per 12 mesi, il gestionale GDPR **Allevolution Privacy** (versione completa) di Allevolution s.r.l.s.. Il software fornisce servizi necessari all'adeguamento privacy e al suo mantenimento e, per chi non ha mai avuto un sistema informatico di gestione della propria attività rappresenta, altresì, un valido supporto per registrare clienti, fornitori, dipendenti, collaboratori e consulenti. L'utente di **Allevolution Privacy** avrà a disposizione tutto ciò che serve per l'adeguamento alla normativa vigente in materia di GDPR. Il software gestionale funziona in Cloud e, con una semplice connessione internet, è accessibile da qualsiasi luogo e con qualunque dispositivo. Ogni area del software riporta tutti i documenti di riferimento, predisposti per singola categoria e per ogni esigenza professionale; in questo modo l'utente potrà scegliere, in base alle proprie esigenze, se utilizzare i documenti base oppure modificarli o integrarli. Inoltre, grazie alla funzione anagrafiche, i dati verranno inseriti automaticamente all'interno dei documenti. Registri e documenti sono costantemente aggiornati alle modifiche normative e alle pronunce del garante e, grazie ad un editor di testo integrato, per la creazione dei documenti non è necessario utilizzare software di terze parti.

Andrea Omar Bianco, avvocato penalista, specializzato in penale dell'economia, D.Lgs. 231/2001 e GDPR. È relatore in convegni sub materia, esercita la professione in ambito giudiziale ed è consulente, con il ruolo di OdV e DPO, di enti pubblici e società private.

ISBN 13 978-88-277-0103-4
9 788827 701034 >
Euro 35,00