NUOVA PRIVACY DAL 25 MAGGIO 2018

2018

SCHEDA PRATICA

Regolamento Ue privacy

Il 25 maggio entrerà in vigore il nuovo Regolamento Ue sulla privacy

NOVITÀ

DIVERSI GLI OBBLIGHI E LE RESPONSABILITÀ in materia di tutela dei dati personali nonché i nuovi adempimenti in capo alle imprese da mettere in atto durante tutto il processo di adeguamento del nuovo Regolamento Ue 679/2016, dalla messa in sicurezza dei dati, attraverso l'utilizzo di nuovi strumenti informatici o attraverso la definizione di misure organizzative interne adeguate, onde evitare che i dati siano violati, persi, alterati, distrutti o comunque trattati illecitamente, all'obbligo di riservatezza, fino alla tenuta in alcuni casi del Registro del trattamento, alla designazione nei casi previsti del Responsabile del trattamento dati e più in generale gli obblighi del segreto professionale.

PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE

PROTEZIONE PER IMPOSTAZIONE PREDEFINITA

REGOLAMENTO UE 679/2016

REGOLE DI ADEGUAMENTO

CONSENSO

Art. 7 del Regolamento

Il titolare del trattamento deve essere in grado di dimostrare che l'interessato abbia prestato il proprio consenso al trattamento dei dati personali.

DOVRÀ ESSERE

SPECIFICO – INFORMATO – INEQUIVOCABILE – ESPLICITO – LIBERO – VERIFICABILE - REVOCABILE

Deve essere sempre distinguibile da altre richieste o dichiarazioni rivolte all'interessato

INFORMATIVA DA RIAGGIORNARE

1. l'informativa dovrà essere rielaborata inoltre secondo le nuove modalità individuate dal Regolamento.

NELL'INFORMATIVA DOVRANNO ESSERE INDICATI:

1. i **dati del titolare o del suo rappresentante**, e nei casi previsti anche il Responsabile del Protezione dei Dati (c.d. DPO);
2. i dati di **contatto del RPD-DPO** (Responsabile della protezione dei dati - Data Protection Officer) da parte del titolare;
3. le **finalità del trattamento** (per ogni finalità dovrà essere richiesto un consenso specifico);
4. il **periodo di conservazione dei dati** o, se non è possibile, i criteri utilizzati per determinare tale periodo ecc.).

1. Il principio della trasparenza impone che le informazioni destinate al pubblico o all'interessato siano **concise, facilmente accessibili e di facile comprensione** e che sia usato un **linguaggio semplice e chiaro**
2. **Può essere fornita per iscritto e preferibilmente in formato elettronico**

DPO

CASI DI OBBLIGATORIETÀ DESIGNAZIONE – Art. 37

- il **trattamento sia effettuato da un'autorità pubblica o da un organismo pubblico** (eccetto le autorità giurisdizionali quando esercitano le loro funzioni);
- le **attività principali** del titolare del trattamento o del responsabile del trattamento consistano in trattamenti che, per loro natura, ambito di applicazione e/o finalità, **richiedono il monitoraggio regolare e sistematico degli interessati su larga scala**;
- le attività principali del titolare del **trattamento** o del responsabile del trattamento consistano nel trattamento, su larga scala, di **categorie particolari** di dati personali di cui all'articolo 9 (**dati sensibili**) o di dati relativi a condanne penali e a reati di cui all'articolo 10.

REGISTRO TRATTAMENTI

ESCLUSIONE OBBLIGO	tutti gli organismi con meno di 250 dipendenti
OBBLIGO	→ trattamenti che possano presentare un rischio per i diritti e le libertà degli interessati → trattamento occasionale → trattamento di categorie particolari – dsti sensibili → dati personali relativi a condanne penali e a reati
UTILIZZO CONSIGLIATO	Se ne consiglia l'utilizzo: → per avere un quadro completo e aggiornato dei trattamenti all'interno di un'azienda o di un soggetto pubblico → per dimostrare e documentare dinanzi all'Autorità di controllo la conformità dell'organizzazione alle norme del Regolamento Europeo.

CYBER SECURITY

ADOZIONE DI TUTTE LE MISURE NECESSARIE PER LA SICUREZZA INFORMATICA

CRITTOGRAFIA	**PSEUDONIMIZZAZIONE DATI**	**BACKUP DATI**	**SICUREZZA PASSWORD**

ESEMPIO 1 – Obblighi settore sanitario e farmaceutico

Ho una farmacia, sono obbligata all'adeguamento al nuovo Regolamento? E in riferimento a quali aspetti?

Il nuovo Regolamento Ue 2016/79 che come ormai è ben noto farà ufficialmente la sua grande entrata il **25 maggio 2018** andrà a colpire "chiunque" abbia a che fare con il trattamento di dati personali Pmi, PA, Organizzazioni no profit, banche, ecc. di conseguenza anche le farmacie, studi medici ecc. Anzi poiché di indiscusso rilievo in termini di protezione dei dati maggior attenzione merita **il settore sanitario e farmaceutico**.

Un settore con diversi aspetti riservati alla privacy sanitaria da non sottovalutare, considerato che in una farmacia ad esempio, come spesso accade, transitano dati sensibili di gran lunga superiori a quelle di altre piccole organizzazioni, dalla prenotazione di esami diagnostici, alla registrazione di intolleranze alimentari o patologie ecc., e da qui, quindi, la necessita di proteggere anche i sistemi informatici.

Un settore con diversi aspetti riservati alla privacy sanitaria da non sottovalutare, considerato che in una farmacia ad esempio, come spesso accade, transitano dati sensibili di gran lunga superiori a quelle di altre piccole organizzazioni, dalla prenotazione di esami diagnostici, alla registrazione di intolleranze alimentari o patologie ecc., e da qui, quindi, la necessita di proteggere anche i sistemi informatici.

In area sanitaria le informazioni attinenti ogni paziente, come anzidetto, sono particolarmente sensibili e quindi richiedono un livello di gestione e sicurezza molto alto, occorrerà quindi adottare misure atte a garantirne l'integrità, la correttezza e l'aggiornamento da cui non solo dipende il rispetto della riservatezza del paziente, ma soprattutto della sua salute.

In area farmaceutica e medical device il grande impatto sarà:

- sulla gestione dei Clinical Trials;
- sull'uso di tutte le apparecchiature software;
- sull'informazione medico scientifica tradizionale e digitale;
- sulle dichiarazioni annuali che le Aziende obbligatoriamente devono fare all'Agenzia del Farmaco.

DOMANDA 1 – NUOVO SISTEMA

Con l'avvento del GDPR cosa cambia per la mia aziende?

Il nuovo Regolamento (Ue) 2016/679 relativo alla libera circolazione e alla protezione del trattamento dei dati personali delle persone fisiche (che abroga la direttiva 95/46/CE - regolamento generale sulla protezione dei dati). Pubblicato nella Gazzetta Ufficiale europea il 4 maggio 2016 è entrato in vigore il 24 maggio 2016, ma la sua piena attuazione è stata prevista per il **25 maggio 2018**.

Con l'avvento delle nuove norme gli studi professionali, le aziende ecc., non dovranno più attenersi al vecchio Codice della privacy **(il D.Lgs. 196 del 2003) bensì al nuovo Regolamento e al Decreto Legislativo che verrà approvato da qui a breve (l'iter legislativo** verrà concluso entro il 19 maggio proprio a pochi giorni dall'entrata in vigore del nuovo Regolamento)**.**

Le imprese dovranno metter mano al tema privacy con uno sguardo non solo al quadro giuridico nazionale ma in un'ottica comunitaria, il fine ultimo infatti è quello di applicare le medesime norme in tutto il continente, per garantire la certezza giuridica per le imprese e lo stesso livello di protezione dei dati in tutta l'UE.

I **vantaggi** vanno infatti dall'avere un'unica autorità per la protezione dei dati (anche per attività svolte all'estero) e norme univoche in tutto il territorio dell'Unione europee (si pensi ai vantaggi per le imprese che si spingono sempre più verso l'internalizzazione).

Precedentemente l'obiettivo principale da parte delle aziende era quello di svolgere una serie di adempimenti a cui le stesse dovevano provvedere, ora si pone l'attenzione sul **principio di sensibilizzazione delle imprese.** L'approccio sarà basato infatti sul rischio e sulle misure di **accountability** (responsabilizzazione) di titolari e responsabili, ossia, sull'**adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento**.

DOMANDA 2 – NOMINA DPO

Devo nominare un Responsabile della protezione dei dati?

L'obbligo di designazione è stabilito dall'art. 37 del Regolamento ovvero qualora:

- il trattamento sia effettuato da un'autorità pubblica o da un organismo pubblico (eccetto le autorità giurisdizionali quando esercitano le loro funzioni);
- le attività principali del titolare del trattamento o del responsabile del trattamento consistano in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
- le attività principali del titolare del trattamento o del responsabile del trattamento consistano nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 (dati sensibili) o di dati relativi a condanne penali e a reati di cui all'articolo 10.

Al di fuori di tali ipotesi, invece, la designazione del DPO rimane facoltativa.

Non è obbligatoria ad esempio:

- in relazione a trattamenti effettuati da **liberi professionisti operanti in forma individuale**;
- agenti, rappresentanti e mediatori operanti non su larga scala;
- imprese individuali o familiari;
- piccole e medie imprese, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti.

Nonostante la non obbligatorietà, il Garante ne consiglia e ne raccomanda anche a tali soggetti la designazione, anche alla luce del principio di "accountability" (secondo il principio di responsabilizzazione).

E' obbligatoria ad esempio nei casi di istituti di credito; imprese assicurative; sistemi di informazione creditizia; società finanziarie; società di informazioni commerciali; società di revisione contabile; società di recupero crediti; istituti di vigilanza; partiti e movimenti politici; sindacati; CAF e patronati; società operanti nel settore delle "utilities" (telecomunicazioni, distribuzione di energia elettrica o gas); imprese di somministrazione di lavoro e ricerca del personale; società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione; società di call center; società che forniscono servizi informatici; società che erogano servizi televisivi a pagamento.

DOMANDA 3 – ADEGUAMENTO ATTIVITÀ

Cosa devo fare per adeguare la mia attività al nuovo Regolamento?

In sintesi secondo il nuovo regolamento europeo ogni azienda dovrà:

- effettuare un controllo interno;
- verificare il proprio livello di esposizione ai rischi;
- svolgere una serie di interventi per mitigare i rischi;
- innalzare il livello di tutela;
- documentare le scelte prese secondo un processo di accountability che caratterizza l'intero regolamento.

Ovvero:

- designare, nei casi previsti e in tempi stretti il Responsabile della protezione dei dati (o **DPO** – **Data Protection Officer**);
- istituire, nei casi previsti, il **Registro delle attività del trattamento**, in cui sono descritti i trattamenti effettuati e le procedure di sicurezza adottate;
- definire tutti gli adempimenti da adottare per ogni evento che potrebbe accadere in azienda dalla notifica delle violazioni dei dati personali, i cosiddetti **Data Breach**, alla valutazione di impatto, fino all'eventuale consultazione preventiva con il Garante ecc;
- formare adeguatamente le persone "attive" del processo;
- **definizione delle politiche di sicurezza** e valutazione dei rischi;
- **adeguare il proprio sito web alle richieste del nuovo Regolamento;**
- **modificare e riaggiornare tutte le informative da fornire all'interessato;**
- **adottare tutte le misure adeguate per la cyber security.**

DOMANDA 4 – ADEGUAMENTO SITO WEB

Come devo mettere in regola il mio sito web?

Tutti i siti web che posseggono un modulo di contatto, di raccolta dati, che utilizza la tecnologia dei cookies o magari che posseggono anche un'area dedicata all'e-commerce dovranno mettersi in regola con le disposizioni del nuovo Regolamento, ovvero dovranno:

- adeguare le misure idonee che permettano all'utente di confermare il **proprio consenso** all'attività di trattamento e tracciamento dei dati personali;
- fornire una chiara e dettagliata **Privacy Policy**;
- Informare l'utente in riguardo a chi sia il **Responsabile del trattamento dei dati;**
- Informare l'utente in riguardo ai **tempi di conservazione dei dati, le modalità di cancellazione, la modifica degli stessi;**
- Informare l'utente se il sito web prevede procedure **tecniche volte a profilarne la navigazione e le preferenze** (cookies ecc.);
- predisporre il sito di un software che permetta, nel caso in cui l'utente scelga di poter navigare con i cookies non attivi, di bloccare preventivamente qualsiasi **attività di tracciamento** che non sia espressamente confermata da parte del navigatore. L'utente dovrà avere la facoltà di poter navigare sul sito decidendo quali cookies potranno rimanere attivi e quali no;
- fornire espressamente all'utente **le finalità per cui i dati vengono raccolti** (n.b. per ogni finalità dovrà essere fornita una specifica informativa – per più finalità quindi, più informative).

DOMANDA 5 - INFORMATIVA

Dovrò reinviare la modulistica aggiornata a tutti i miei clienti? Dovrò reinviarla solo ai nuovi, a partire dal 25 maggio, o anche a quelli acquisiti prima di tale data? Dovrò riaggiornare tutta la modulistica riguardo al consenso per l'utilizzo dei dati? Quali caratteristiche dovrà contenere la nuova modulistica? Dovrò chiedere il consenso per ogni finalità?

Anzitutto c'è da precisare che il rinnovo dell'informativa per il consenso è uno dei primi adempimenti da porre in essere all'interno del processo di adeguamento al nuovo Regolamento.

A partire da 25 maggio tutta la modulistica presente in azienda dovrà riportare i riferimenti alla nuova normativa e non più al codice della privacy quindi, facendo un esempio pratico, per ogni finalità di trattamento non dovrà più riportare sommariamente ai riferimenti all'art. 7 del Codice della privacy (diritto dell'interessato alla cancellazione, opposizione, rettifica ecc. dei dati) bensì specificatamente e dettagliatamente ai singoli artt. del nuovo Reg. UE 2016/679: art. 15 (diritto di accesso); art. 16 (diritto di rettifica); art. 17 - diritto alla cancellazione («diritto all'oblio»); art. 18 (diritto di limitazione di trattamento); art.20 (diritto alla portabilità dei dati) ecc.

Altra precisazione doverosa è quella di capire se il consenso prestato prima del 25 maggio, rimane valido o meno; in proposito vanno effettuate due valutazioni: la vecchia modulistica rispecchia i nuovi standard europei? Il consenso è stato espresso in maniera specifica?

Una volta valutata la vecchia modulistica e se risponde in maniera positiva alle caratteristiche sopra esposte non occorre reinviarla, così come anche il consenso raccolto precedentemente al 25 maggio 2018 che resta valido e non dovrà essere raccolto nuovamente. In caso contrario, dovrà essere reinviata secondo le nuove forme anche ai "vecchi clienti" e sarà opportuno adoperarsi prima di tale data per raccogliere nuovamente il consenso degli interessati secondo quanto prescrive il regolamento per non incorrere in pesanti conseguenze in caso di controlli da parte dell'Autorità competenti.

Lo conferma anche il considerando 171: "qualora il trattamento si basi sul consenso a norma della direttiva 95/46/CE, **non occorre che l'interessato presti nuovamente il suo consenso**, se questo è stato espresso secondo modalità conformi alle condizioni del presente regolamento, affinché il titolare del trattamento possa proseguire il trattamento in questione dopo la data di applicazione del presente regolamento".