Di seguito si illustrano le novità normative applicabili al settore delle farmacie, alla luce di quanto emerso dall'incontro con gli uffici del Garante.

Il GDPR IN FARMACIA

Il Regolamento 2016/679 (GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali**,** sarà direttamente applicabile a tutti gli Stati membri **a decorrere dal 25 maggio 2018.**

Il GDPR si applica alla protezione dei dati personali[1] delle persone fisiche (art.1). Il regolamento, pertanto, si applica certamente alle farmacie perché possono trattare una molteplicità di dati personali.

1) INFORMATIVA e CONSENSO AL TRATTAMENTO DEI DATI

Il GDPR, a differenza di quanto prevede la normativa attuale, consente **il trattamento di dati sanitari** senza richiedere il consenso del cittadino, qualora il trattamento sia effettuato per finalità di assistenza sanitaria e di terapia da parte di professionisti della salute e se i dati sanitari sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale, come ad esempio è il caso della farmacia la cui conduzione professionale è sempre affidata ad un farmacista (art.9, paragrafo 2, lettera h e paragrafo 3).

Tale disposizione potrebbe comunque essere derogata dal legislatore italiano qualora decidesse di mantenere le restrizioni attuali oppure di introdurne di nuove. Infatti, l'art.9, paragrafo 4, del GDPR consente agli Stati membri di mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati relativi alla salute.

Non ci sono significativi cambiamenti per quanto riguarda l'acquisizione del consenso per finalità differenti rispetto a quelle sanitarie, rispetto alla precedente normativa (artt. 6, 7, 8).

Le **informative** esistenti, invece, dovranno essere aggiornate in base ai nuovi contenuti previsti dal GDPR. E' necessario indicare: la base giuridica del trattamento; se si trasferiscono i dati verso paesi terzi; il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di presentare un reclamo all'autorità di controllo (artt. 12,13,14).

In caso di **profilazione**, l'informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

2) PRINCIPIO DI RESPONSABILIZZAZIONE DEI TITOLARI. MISURE TECNICHE E ORGANIZZATIVE. OBBLIGO DI DIMOSTRAZIONE.

Al fine di rispettare il regolamento sulla privacy, non sussiste un elenco tassativo di misure completo ed esaustivo da porre in essere, ma il GDPR, introducendo il principio di responsabilizzazione, obbliga i titolari e i responsabili a mettere **in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento (art.24)**. Secondo il Garante "*Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i*

[1] Art.4. 1) «**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

limiti del trattamento dei dati personali – nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.”.

Il regolamento attribuisce la responsabilità al titolare che deve attuare le misure, sempre aggiornate *“tenendo conto dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche”* (Art.24). Pertanto, il titolare del trattamento nel decidere quali misure adottare dovrò effettuare una **valutazione dei rischi** dei dati trattati in farmacia Inoltre è stato introdotto **l’obbligo di dimostrazione** che il trattamento è effettuato nel rispetto del regolamento.

Il Regolamento impone e/o suggerisce alcune modalità, di seguito specificate, per tenere traccia di una policy privacy adeguata in modo che il titolare possa rispettare l’obbligo di dimostrazione che il trattamento di dati è conforme al regolamento.

3) INDIVIDUAZIONE DEI RUOLI: TITOLARE, RESPONSABILE, PERSONE AUTORIZZATE AL TRATTAMENTO (INCARICATI)

Di norma, il titolare di farmacia è **titolare del trattamento dei dati personali**. Nel caso di società, il titolare del trattamento è la società in quanto tale. Si ricorda che il titolare del trattamento ha una responsabilità generale sull’attuazione della normativa che non viene meno nel caso in cui si esternalizzino trattamenti o si incarichino persone specifiche (art.24).

In ogni caso quando la farmacia delega l’effettuazione di un trattamento o parte di esso ad un altro soggetto esterno (persona fisica o società) che effettua il trattamento per conto della farmacia, deve designarlo obbligatoriamente **responsabile del trattamento (art.28).** La farmacia ricorre, di norma, a soggetti esterni, ad esempio, in caso di trasmissione dei dati dei propri utenti (fatture) al commercialista o dei dati dei propri collaboratori al consulente del lavoro (buste paga), oppure nel caso di trasmissione dei dati per il monitoraggio della spesa sanitaria, o nel caso di società che effettuano la tariffazione. E’ possibile anche che la farmacia utilizzi un servizio di “cloud” da parte di fornitori terzi che gestiscono i dati per conto della farmacia,

In tutti questi casi, l’atto con cui il titolare designa un responsabile del trattamento deve trattarsi di un contratto (o altro atto giuridico conforme al diritto nazionale) e deve disciplinare tassativamente almeno le materie riportate al paragrafo 3 dell'art. 28.

Anche la farmacia può svolgere trattamenti in qualità di responsabile del trattamento, come ad esempio nel servizio di prenotazione CUP o in caso di assistenza integrativa. In tal caso sarà compito delle associazioni provinciali o delle unione reginali integrare negli accordi con la parte pubblica le clausole previste dal GDPR.

Il regolamento consente la nomina di **sub-responsabili del trattamento** da parte di un responsabile (si veda art. 28, paragrafo 4), per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario.

Infine, come in passato, ogni titolare del trattamento designerà **incaricati al trattamento** i dipendenti e i collaboratori autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile. Il Garante[2] ha affermato che *“alla luce del principio di "responsabilizzazione" di titolari e responsabili del trattamento* si ritiene opportuno che titolari e responsabili del trattamento mantengano in essere la struttura organizzativa e le modalità di designazione degli incaricati di trattamento così come delineatesi negli anni anche attraverso gli interventi del Garante” .

[2] Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personal

4) TUTTE LE FARMACIE DEVONO REGIRE E DETENERE UN AGGIORNATO REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO DEI DATI PERSONAI

Per agevolare l'identificazione e l'analisi dei dati trattati, la valutazione dei rischi, l'adozione di misure adeguate a proteggere i dati e aumentare la consapevolezza e la responsabilità dei soggetti coinvolti**, tutte le farmacie, come del resto tutte le imprese o i professionisti che trattano dati sanitari, devono obbligatoriamente detenere, in forma scritta, anche in formato elettronico, un registro delle attività di trattamento dei dati personali svolte sotto la propria responsabilità (art 30, paragrafo 5).**

Il Garante ha affermato che si tratta di *"uno **strumento fondamentale** non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda* (in questo caso della farmacia n.d.r)*"*.

Su richiesta, la farmacia deve mettere a disposizione il registro a disposizione dell'autorità di controllo. Il contenuto minimo obbligatorio del registro è indicato nel regolamento.

Federfarma, in collaborazione con Promofarma, metterà a disposizione un modello di registro elettronico delle attività di trattamento e una procedura informatica per redigerlo in modo consapevole e adeguato.

5) LA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI (DPIA) NON E' RICHIESTA PER MOLTI TRATTAMENTI EFFETTUATI IN FARMACIA

Qualora nell'ambito della valutazione del rischio il titolare del trattamento verifichi che il trattamento possa comportare un rischio elevato per i diritti e le libertà delle persone fisiche il titolare è obbligato ad effettuare e formalizzare in un documento la valutazione di impatto sulla protezione dei dati personali (DPIA) (art. 35, paragrafo 1).

La DPIA, pertanto, non è obbligatoria per ogni singolo trattamento ma deve essere valutata in base alle Linee-guida del Gruppo di lavoro art. 29 n. 248 concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679.

Seguendo un approccio condiviso con gli uffici del Garante della privacy, Federfarma ha elaborato un documento (allegato n.1) nel quale sono elencati i **trattamenti per i quali non la singola farmacia, non deve effettuare una valutazione di impatto sulla protezione dei dati,** in quanto tali trattamenti sono stabiliti e disciplinati a monte da un legge, da un atto amministrativo, o da un accordo, utilizzando sistemi informativi pubblici o comunque istituiti da un accordo con la parte pubblica. In tali casi, anche se sussistessero trattamenti ad alto rischio per i diritti e le libertà, ogni valutazione e le conseguenti decisioni in ordine alle modalità di funzionamento dei sistemi che trattano dati non può essere effettuata dalla singola farmacia, in quanto non po' incidere sulle modalità del trattamento dei dati a garanzia dei cittadini. La valutazione di impatto e le conseguenti garanzie a tutela dei cittadini deve essere effettuata a monte, nel rispetto del principio privacy by design e by default, da parte degli enti e delle organizzazione che hanno istituito e deciso il trattamento.

Inoltre, in tale documento, si esemplificano **trattamenti standardizzati che possono essere effettuati dalle farmacie in regime privatistico, in qualità di responsabili del trattamento** utilizzando piattaforme o software messi a disposizioni dal titolare, fornitore del servizio, per i quali

la valutazione di impatto sulla protezione dei dati personali dovrebbe essere effettuata appunto dal titolare del trattamento e non dalla farmacia.

Infine, le farmacie possono effettuare trattamenti di dati personali in regime privatistico in modo standardizzato, utilizzando piattaforme informatiche messe a disposizione da associazioni dei titolari di farmacia, rete di farmacie, cooperative ecc. In quel caso, qualora sussista un trattamento di dati ad alto rischio per i diritti e le libertà degli interessati, la farmacia, obbligata ad effettuare una DPIA potrà utilizzare la valutazione di impatto sulla protezione dei dati eventualmente redatta dalla Rete di farmacie, dall'Associazione di categoria, dalla cooperativa ecc, valevole per tutte le farmacie che aderiscono al progetto.

L'ufficio legale della Federazione è a disposizione per valutare ulteriori casistiche non ricomprese nel documento che eventualmente le associazioni territoriali dovessero raccogliere in ordine all'obbligo di valutazione di impatto sulla protezione dei dati.

6. MISURE DI SICUREZZA (ART. 32)

Non esiste più un elenco tassativo di misure minime di sicurezza elencate dal legislatore ma ogni titolare del trattamento dovrà scegliere e adottare misure organizzative e tecniche adeguate per garantire un livello di sicurezza adeguate al rischio.

Nel valutare l'adeguato livello di sicurezza, si tiene 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 illegale, a dati personali trasmessi, conservati o comunque trattati.

Il rischio zero è impossibile, ma è importante che la farmacia con una idonea valutazione dei rischi, sappia motivare le scelte effettuate per diminuire il rischio di violazione del dato e renderlo accettabile.

Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati **se non è istruito** in tal senso dal titolare del trattamento.

Federfarma, in collaborazione con Promofarma metterà a disposizione sul proprio sito alcuni strumenti operativi che aiutino le farmacie ad effettuare una valutazione dei rischi e ad adottare misure di sicurezza adeguate.

7. NOTIFICA IN CASO DI VIOLAZIONE DI DATI PERSONALI – DATA BREACH (ART.33)

Il Regolamento introduce un nuovo obbligo consistente nella notifica all'autorità di controllo (Garante privacy), di casi di violazione dei dati personali, che presentano un rischio per i diritti e le libertà degli interessati. Sicuramente presentano tale rischio i dati sanitari o i dati raccolti per effettuare una profilazione, per finalità di marketing.

Per violazione di dati personali si intende la distruzione, perdita, modifica, divulgazione non autorizzata l'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati (art.33 comma 2).

La notifica **non** deve essere fatta qualora il titolare del trattamento ritenga sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

La notifica deve effettuata essere entro 72 ore dal momento in cui il titolare del trattamento è venuto a conoscenza della violazione. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

Il regolamento stabilisce il contenuto obbligatorio della notifica. Federfarma, in collaborazione con Promofarma, metterà a disposizione un modello di notifica.

8. LE FARMACIE NON DEVONO DESIGNARE IL RESPONSABILE DELLA PROTEZIONE DEI DATI (Data protection officer - DPO)

In base all'art.37 del GDPR, tutti i soggetti pubblici e alcuni soggetti privati**,** in presenza di determinati trattamenti, dovranno obbligatoriamente nominare un responsabile della protezione dei dati (Data protection officer - DPO) che abbia una conoscenza specialistica della normativa in materia di protezione dei dati personali e che possa assistere il titolare del trattamento o il responsabile del trattamento nell'attuazione della normativa..

Saranno obbligati a nominare il DPO tutti i soggetti pubblici, e

- i soggetti privati la cui attività principale consiste nel trattamento di particolari categorie di dati su larga scala tra cui i dati sanitari;

- oppure i soggetti privati che effettuato trattamenti su larga scala che richiedono un monitoraggio regolare e sistematico dei dati.

Come chiarito in occasione dell'incontro con gli uffici del Garante, le farmacie non effettuano trattamenti di dati personali su larga scala e pertanto non sono obbligate e designare il DPO. Ovviamente tali considerazioni non sono estensibili tout court alle grandi catene di farmacie qualora avessero, per determinati trattamenti, un bacino d'utenza molto più vasto.

9. DIRITTO DI ACCESSO, RETTIFICA, CANCELLAZIONE, LIMITAZIONE E PORTABILITÀ DEI DATI

Diritto alla portabilità del dato (art.20)

Il diritto può essere esercitato, solo per i dati trattati in modo automatizzato e su consenso esplicito. Riguarda in modo marginale il settore delle farmacie.

Inoltre, l'art. 20, paragrafo 2, obbliga il titolare a trasmettere i dati portabili direttamente a un diverso titolare "se tecnicamente fattibile".

Diritto di accesso dell'interessato (art.15)

L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali.

Diritto di rettifica (art.16)

L’interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l’interessato ha il diritto di ottenere l’integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Diritto alla cancellazione («diritto all’oblio») (art.17)

L’interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l’obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti altrimenti trattati;

b) l’interessato revoca il consenso su cui si basa il trattamento e se non sussiste altro fondamento giuridico per il trattamento;

c) l’interessato si oppone al trattamento e non sussiste (diritto di opposizione al trattamento) alcun motivo legittimo prevalente per procedere al trattamento,

d) i dati personali sono stati trattati illecitamente;

e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell’Unione o dello Stato membro cui è soggetto il titolare del trattamento;

f) i dati personali sono stati raccolti relativamente all’offerta di servizi della società dell’informazione.

Dritto di limitazione del trattamento

Tale diritto è esercitabile **in caso di violazione** dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), **se l'interessato chiede la rettifica dei dati (in attesa di tale rettifica da parte del titolare**) o **si oppone al loro trattamento** ai sensi dell'art. 21 del regolamento (in attesa della valutazione da parte del titolare).

Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la limitazione è vietato a meno che ricorrano determinate circostanze (consenso dell'interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante).

10. SANZIONI

Il GDPR (art.83) prevede un sistema sanzionatorio severo ma graduato, attribuendo notevole discrezionalità dall’Autorità Garante. Le sanzioni previste sono il Richiamo, l’Ammonizione, la Sospensione dal trattamento dei dati, sanzioni pecuniarie fino a 20 milioni di euro oppure il 4% del fatturato totale annuale.