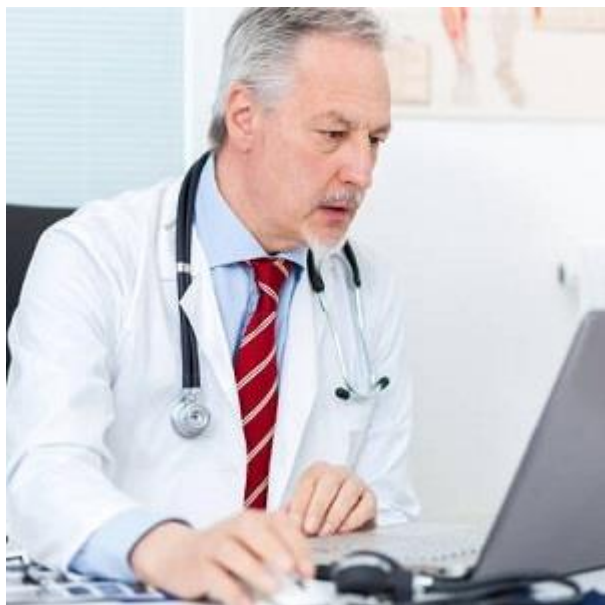


Publicato in Gazzetta il decreto privacy: tutte le novità e cosa fare



Tra i professionisti i più coinvolti sono i medici: i quesiti più comuni e le risposte a tutti i dubbi

Il Decreto Gdpr ([clicca qui per scaricare il codice privacy redatto da Altalex](#)) è stato pubblicato in Gazzetta Ufficiale ed entrerà ufficialmente in vigore dal prossimo 19 settembre. L'Italia adegua così la propria normativa alla [rivoluzione sulla privacy voluta dall'Europa](#), attivando una serie di regole stringenti che valgono per imprese e professionisti, medici in particolare vista la delicatezza dell'ambito lavorativo.

Chi non si adegua ([clicca qui per leggere le domande e risposte più comuni sull'argomento](#)) rischierà sanzioni amministrative che si applicheranno anche alle violazioni emesse prima che il decreto entrasse in vigore. Il decreto definisce cosa si intenda per comunicazione e diffusione dei dati personali, **individua nella figura del Garante della privacy l'autorità incaricata del controllo e della promozione delle regole deontologiche in materia**, stabilisce che il consenso al trattamento dei dati personali può essere espresso solo al compimento dei 14 anni di età, chi ha un'età inferiore necessita del consenso di chi ne **esercita la responsabilità genitoriale**, **le misure di garanzia che riguardano i dati genetici e il trattamento dei dati relativi alla salute** per finalità di prevenzione, diagnosi e cura sono adottate sentito il ministro della Salute che a sua volta deve acquisire il parere del Consiglio superiore di sanità. Viene introdotto il concetto di diritto

all'eredità del dato in caso di decesso e come forma di tutela viene introdotto il reclamo, alternativo al ricorso in tribunale.

Di questa importante novità se n'è parlato a maggio scorso nel corso di un convegno organizzato dall'Omceo veneziano del quale riportiamo i punti salienti degli avvocati **Silvia Boschello** e **Alexander Cassisa** e dell'informatico **Massimo Amoruso**.



pubblicità

GDPR: le novità

«Con il [regolamento europeo in materia di privacy](#) – ha spiegato l'avvocato **Silvia Boschello** – cambiano soprattutto le abitudini, **cambia totalmente l'approccio culturale**: per i dati personali serve un **livello di sicurezza più elevato**, non solo sotto il profilo informatico». Dopo aver illustrato le norme del percorso italiano ed europeo e quelle, sempre valide, legate alla salute e alla sicurezza delle cure, ha sottolineato anche come spesso **trasparenza e rispetto della privacy** siano principi che **possono cozzare** l'uno con l'altro e che vanno trattati con equilibrio.

«L'approccio – ha aggiunto – è basato sulla **prevenzione del rischio**». Vanno esattamente in questa direzione, allora, le due maggiori novità del GDPR: la **responsabilizzazione** del titolare del trattamento dei dati e la possibilità di **rendicontare** quanto fatto in materia di sicurezza. «Il titolare – ha spiegato il legale – può decidere autonomamente le modalità, le garanzie e il limite del trattamento dei dati. In sostanza **siete liberi di decidere come e cosa fare**. Vi viene chiesto, però, che queste decisioni vengano approntate e rendicontate: dovete, cioè, essere **in grado di dimostrare** il percorso fatto. Questa normativa non deve spaventarvi: può essere **l'occasione di riorganizzare** le vostre strutture».

Il processo di riorganizzazione prevede, allora, la valutazione del rischio di violazione dei dati e la progettazione delle attività da fare per arrivare alla sicurezza: servono **un'organizzazione articolata**, supportata anche dall'esterno se necessario, e **competenze in materia**, soprattutto sotto il profilo giuridico e informatico.

La mancata organizzazione potrebbe, infatti, portare a un rischio di business, cioè di **contenziosi** legati non solo alla responsabilità professionale, al rischio di **sanzioni pesantissime** – che possono arrivare per singola violazione nei casi base fino **a 10 milioni di euro** e al 2% del fatturato totale annuo lordo, nei casi gravi fino **a 20 milioni di euro** e al 4% del fatturato – e a una **vulnerabilità** rispetto all'immagine, alla reputazione della struttura sanitaria. Le misure di sicurezza – ha aggiunto l'avvocato civilista **Alexander Cassisa** – sono tutti gli **accorgimenti tecnici e organizzativi** che il titolare del trattamento decide di assumere per tutelare i dati personali dei propri pazienti.

Si tratta, dunque, sia di misure **informatiche** (firewall, proxy, sistemi operativi aggiornati, antivirus, procedure di backup...), sia di **misure fisiche** – i raccoglitori con la chiave, le cartelle, lo stanzino del server – sia di misure **organizzative**: come e dove custodisco le password, come raccolgo i dati, dove li conservo, le procedure per rispondere alle richieste d'accesso, ecc».

E dato che è sempre e solo il titolare che decide cosa fare e come farlo, quali siano gli strumenti più idonei in base alla propria valutazione del rischio, **non esiste un elenco tassativo** di provvedimenti da adottare, come invece avveniva per il codice privacy: nel GDPR si parla solo **di misure di sicurezza adeguate**. Tra i parametri, dunque, che devono essere considerati ci sono: lo stato dell'arte della propria attività, i costi, la natura, l'oggetto e le finalità del trattamento dei dati.

Il consenso privacy

Proprio legata alle novità contenute nel GDPR circola la voce che in sanità **non sia più necessario** raccogliere il consenso al trattamento dei dati personali. «È uno degli slogan – ha aggiunto l'avvocato Boschello – che sta passando in questi giorni, ma **deve essere preso con le pinze** e guardato alla luce dell'intero testo normativo». In sostanza il consenso **non deve più essere necessariamente documentato per iscritto**, ma questa resta comunque la forma più idonea per raccogliarlo, insieme alla spunta sul formato digitale, considerato anche che il titolare **deve essere in grado di dimostrare di averlo**. «Deve essere specifico e libero – ha proseguito – e alla base deve avere un linguaggio comprensibile, accessibile e chiaro».

L'articolo 9 del GDPR dice chiaramente che il trattamento dei dati sensibili, quelli cioè che identificano l'origine razziale, etnica, politica, sindacale e lo stato di salute della persona, **è vietato**. «Un divieto che si supera – ha spiegato Silvia Boschello – se si ha un consenso esplicito al trattamento, se è necessario per tutelare un interesse vitale della persona, se riguarda un dato reso pubblico dallo stesso paziente, per finalità di medicina preventiva o del lavoro o per un interesse pubblico nel settore sanitario».

L'informativa GDPR

Tra i consigli pratici arrivati dagli esperti, quello di **esporre subito negli studi l'informativa** al trattamento dei dati personali aderente alle nuove regole europee, affrontando poi uno alla volta gli altri adempimenti necessari.

Tra le caratteristiche indispensabili: deve avere **un linguaggio chiaro**, semplice e comprensibile, deve contenere **i dati del titolare** e quelli di contatto dell'eventuale DTO, il data protection officer, devono essere esplicitate **le finalità**, la base giuridica del trattamento, il **periodo di conservazione** dei dati e i **diritti dell'interessato**. «La struttura del testo – ha aggiunto – non cambia, bisogna solo aggiungere delle cose». E proprio sul fronte delle nuove informative, anche l'Ordine, nella figura del suo segretario Luca Barbacane, si è detto disponibile a dare una mano agli iscritti, magari predisponendo qualche modulo ad hoc.

Il registro del trattamento

In nome della trasparenza e della capacità di rendicontazione col GDPR entra in gioco un altro strumento fondamentale: il **registro del trattamento**. Deve essere compilato da **tutte le strutture**, può avere formato elettronico o cartaceo ed è la base su cui, poi, saranno **condotti eventuali controlli**.

«Se fate bene l'informativa – ha consigliato il legale – il registro è fatto». Vanno, infatti, conservati i dati di contatto, le finalità del trattamento, le categorie degli interessati, cioè dei pazienti, e dei dati personali (dati sensibili, identificativi e fiscali), **le categorie delle attività di trattamento svolte per conto del titolare, le categorie dei destinatari, cioè a chi si comunicano i dati dei pazienti (pubblica amministrazione, strutture sanitarie pubbliche o private, ecc.)**, i trasferimenti dei dati in paesi extra UE, i termini per la cancellazione e le misure di sicurezza adottate, unica voce non presente nell'informativa. Nell'informativa va anche indicato il periodo di conservazione dei dati «che nel vostro caso – consiglia l'avvocato Boschello – significa **almeno per un decennio**».

Il documento sulla valutazione di impatto (DPIA)

«Questo – ha spiegato ancora il legale – è un documento particolare che deve essere fatto solo quando **implementate un'attività del tutto nuova** nel vostro studio: organizzate, ad esempio una videosorveglianza, o iniziate a profilare la vostra clientela per fare una promozione mirata della vostra attività o ancora scegliete un nuovo software o un nuovo gestionale». In questi casi si deve stilare questo documento che parte da una valutazione del rischio per questo singolo progetto e ripercorre le misure di sicurezza che si ritiene idoneo adottare. In alcuni casi di rischio elevato si può chiedere anche una consultazione al Garante.

I contitolari dei dati e il data processor

Altra novità contenuta nel GDPR sono i contitolari dei dati. «Si tratta ad esempio – ha sottolineato **Alexander Cassisa** – di più medici o di più studi professionali che hanno un fine comune, la salute del paziente, ma specializzati in ambiti diversi. Il rapporto tra i contitolari deve essere **normato da un contratto** che individui le specifiche responsabilità».

In sostanza il contitolare è qualcuno che decide con il titolare sul trattamento dei dati: entrando nei casi specifici potrebbero essere, ad esempio, **i medici di una medicina di gruppo integrata** o anche quei camici bianchi che occupano gli stessi spazi, lo studio o gli ambulatori con altri colleghi, magari con segreteria e servizi condivisi e un unico gestionale. Questo rapporto tra contitolari deve essere contrattualizzato per **individuare esattamente** tutte le responsabilità.

C'è poi un'altra figura significativa: il **data processor**, cioè il responsabile del trattamento. «È una figura – ha aggiunto – già nota dal codice della privacy: è colui che elabora e tratta i dati per conto del titolare, un soggetto che per ricoprire questo ruolo deve avere **un atto di nomina**». Il regolamento prevede espressamente la presenza del **responsabile esterno**: potrebbe essere dunque il commercialista, l'avvocato o il consulente informatico. Anche, ad esempio, la cooperativa che gestisce per il medico la segreteria rientra in questo tipo di

casistica. I compiti, le possibilità di manovra, i limiti di applicazione del responsabile esterno devono essere **chiaramente delineati** nel suo contratto di incarico.

Una figura nuova: il data protection officer (DPO)

C'è poi una figura professionale **completamente nuova** per l'Italia, ma che in Germania e in America è attiva ormai da tempo, di cui si sente molto parlare quando si fa riferimento al GDPR: il **data processor officer**. Tra i requisiti che deve avere: un'elevata conoscenza del diritto, competenze in ambito procedurale dell'azienda (di risk e project manager) e conoscenze informatiche. «Il DPO – ha spiegato Cassisa – deve svolgere la sua attività **in piena indipendenza e in assenza di conflitto di interessi**. Per questo deve essere fornito di risorse economiche ed organizzative adeguate».

Il DPO, infatti, deve **informare e consigliare** il titolare del trattamento sugli obblighi di legge, ma anche **formare il personale**, verificare e controllare l'attuazione del GDPR, **fornire pareri** sulla valutazione dei rischi. «È una specie di anello di congiunzione – ha aggiunto – tra l'autorità di controllo, cioè il Garante della privacy, e il titolare del trattamento». Una figura, in sostanza, che non deve e non può coincidere con quella del consulente privacy – altrimenti sarebbe controllato e controllore allo stesso tempo – e serve a controllare che il titolare del trattamento abbia adempiuto a ciò che il regolamento chiede di fare.

I singoli studi, quelli cioè in cui lavora un solo medico, non sono obbligati ad assumere un DPO, ma in una categoria come quella sanitaria, almeno secondo i consulenti legali, è utile averlo: la discriminante è data dal numero di professionisti che lavora nella struttura. Nelle piccole realtà che abbiano omogeneità nelle esigenze e nel tipo di clientela, ne può essere nominato uno in comune.

Una figura questa che, però, non è piaciuta troppo ai professionisti presenti in sala, preoccupati soprattutto dalla **gravosità economica** che questa e le altre nuove professionalità stabilite dal GDPR potrebbero comportare in particolare per chi lavora da solo o in strutture piuttosto piccole.

La sicurezza informatica

Pur occupandosi anche di sicurezza legata ai documenti cartacei, il GDPR si concentra in particolare sulle misure per garantirla per il materiale **in formato elettronico**. Tutto sommato poche le novità contenute nel nuovo regolamento europeo, ma tanti gli accorgimenti informatici che si possono adottare per evitare la violazione dei dati personali di clienti e pazienti.

«Dobbiamo capire – ha spiegato **Massimo Amoruso**, esperto informatico di Tecsìs, responsabile assistenza sistemica, applicativa e procedurale nonché DPO certificato – **quale rischi corre la nostra struttura**, chiederci dove sono custoditi i nostri dati, chi può accedervi, cosa succede ai dati in caso di eventi avversi (il server in tilt, un black out, un incendio...), se un malintenzionato che li ruba possa o meno usarli».

Due gli accorgimenti da considerare subito **sul fronte della rete.**

«Bisogna **fare attenzione** – ha aggiunto – **al firewall**, una porta che controlla tutto ciò che entra e ciò che esce e su cui bisogna stabilire dei limiti, e **al wi-fi**. Internet accessibile ovunque è bellissimo, ma chiedetevi: davvero vi serve nel vostro studio? A che scopo? Chi si collega cosa può fare?».

Questi alcuni degli strumenti più utili a cui, secondo l'esperto, si può fare ricorso per garantire una reale protezione delle informazioni:

- **PSEUDOMIZZAZIONE:** i dati non sono direttamente attribuibili a un interessato specifico perché sono scissi e vengono conservati in punti separati. Solo riuniti possono identificare una persona.
- **CIFRATURA:** per leggere e capire i dati serve una "chiave" di codifica. Chi non la conosce non può accedere.
- **MONITORAGGIO PROATTIVO:** serve a controllare da remoto tutto ciò che avviene nella nostra rete.
- **DATA GOVERNANCE:** controllo costante delle modifiche, delle configurazioni e dell'accesso ai dati, attraverso notifiche delle anomalie e delle eventuali situazioni a rischio.
- **POSTA SICURA:** l'attivazione di antispam, antivirus e antimalware rende la posta più sicura. Ma, volendo, la si può far navigare anche su canali criptati. Meglio garantire un sistema di archiviazione adatto e un SandBoxing, sistema virtualizzato di controllo delle e-mail e di individuazione di sistemi di criptaggio.
- **BACKUP:** l'esperto consiglia la regola del 3/2/1, cioè creare 3 copie di dati su 2 differenti supporti di memoria, di cui 1 lontano dal proprio pc.
- **SITO INTERNET:** è una vetrina accessibile da chiunque e non può essere lasciato senza sicurezze.

Un'attenzione particolare, poi, va prestata anche ai **fotocopiatori** che di solito sono noleggiati da aziende esterne. «Sono, però – ha concluso Massimo Amoruso – un punto di accesso all'interno della vostra struttura perché spesso sono collegati in rete per il controllo da remoto. Infine non dimentichiamoci della carta: è fondamentale anche preoccuparsi di come sono tenuti scrivanie e archivi perché, nonostante la sempre maggiore diffusione digitale, contengono dati che non possono essere "a vista"».

I consigli pratici per il percorso di adeguamento

- Costituire una **squadra multidisciplinare** composta da esperti di diritto, di informatica e della vostra struttura aziendale.
- Fare un **mappatura dei dati** per compilare in modo corretto informative e registro.
- Fare un'**analisi dei rischi**.
- Redigere nelle strutture più complesse un **organigramma privacy**.
- **Formare gli incaricati** sui principi di responsabilizzazione e di rendicontazione.
- **Adeguare** le informative e i consensi.

- Definire ed adottare le misure di sicurezza più adeguate.
- Revisionare e, in caso, **redigere nuovi contratti** con i fornitori informatici.
- **Nominare un DPO su base volontaria:** è considerato un elemento di implementazione, di adeguamento delle strutture tecniche e organizzative per risultare conformi al GDPR.
- **Pseudonimizzazione dei dati:** i dati non sono direttamente attribuibili a un interessato perché sono scissi e vengono conservati in punti separati. Solo riuniti possono identificare una persona.
- **Sistemi di cifratura:** processi di codifica dei dati che non si possono leggere se non si possiede la "chiave"..
- Garantire su base permanente la riservatezza, l'integrità e la disponibilità del dato anche, magari, se c'è un attacco informatico, un improvviso black out, un incendio o il server che va in tilt. La procedura più semplice è il **backup fatto in modo continuo,** almeno una volta alla settimana, o se light, una volta ogni due giorni.
- Individuare procedure per **testare e verificare periodicamente il livello di adeguamento** al GDPR: il feedback che ne deriva può essere un documento da consegnare all'autorità in caso di controllo.
- Adottare **codici di condotta** e certificazioni.