

Nuovo Regolamento Europeo in
Materia di Protezione dei Dati



Casa di Cura Privata Città di Bra S.p.A.

**INCONTRO FORMATIVO IN MATERIA DI
PROTEZIONE DEI DATI PERSONALI ALLA LUCE
DEL REG. UE N. 679/16 E DEL D.LGS. N. 101/18**

Avv. Cristiano Burdese



Che cos'è la Privacy?



Il termine, inizialmente riferito alla sfera della vita privata, negli ultimi decenni ha subito un'evoluzione estensiva, arrivando ad indicare il **DIRITTO DELLA PERSONA SUI PROPRI DATI PERSONALI**.

Quindi, il significato odierno di privacy è relativo al **DIRITTO DELLA PERSONA DI CONTROLLARE CHE LE INFORMAZIONI CHE LA RIGUARDANO VENGANO TRATTATE** da altri solo in caso di necessità ed in modo corretto.

Cornice Normativa

Regolamento Europeo

n. 679/2016

In vigore dal 25 maggio 2018

Nuovo Codice della Privacy

In vigore dal 19/09/2018

(d.lgs. n. 193/06 modificato
dal d.lgs. n. 101/18)

**Provvedimenti del Garante
della Privacy**

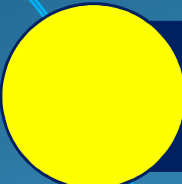
Il Regolamento Europeo n. 679/16

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI (c.d. GDPR)

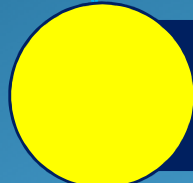
Considerando 6: «...la tecnologia attuale consente tanto alle imprese private quanto alle Autorità Pubbliche di **UTILIZZARE DATI PERSONALI, COME MAI IN PRECEDENZA**, nello svolgimento della loro attività...»

Considerando 7: «Tale evoluzione richiede un quadro più solido e coerente in materia di protezione dei dati nell'Unione...E' 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.

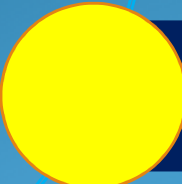
Oggetto e finalità



Il presente Regolamento stabilisce norme relative alla **protezione delle persone fisiche con riguardo al trattamento dei dati personali**, nonché norme relative alla **libera circolazione di tali dati**



Il presente Regolamento **protegge** i diritti e le libertà fondamentali delle persone fisiche, in particolare **il diritto alla protezione dei dati personali**



La **libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali**

Quali diritti e libertà degli interessati protegge?

«Diritto alla privacy, libertà di espressione e di pensiero, libertà di movimento, divieto di discriminazioni, diritto alla libertà di coscienza e di religione».

Quali sono i rischi da proteggere?

- pregiudizio e discriminazione
- furto d'identità
- invasività nella sfera privata
- danno fisico, materiale o morale
- perdita di riservatezza

Principali Definizioni del Regolamento Europeo

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile (c.d. «interessato»)



Identificabilità

Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento ad un dato 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.

Particolari Categorie di Dati e Dati Giudiziari

Particolari Categorie di Dati (art. 9 Regolamento)

Dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Dati Giudiziari (art. 10 Regolamento)

Dati relativi alle condanne penali ed ai reati ed a connesse misure di sicurezza.

Trattamento dei dati personali

Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati ed applicate ai dati personali o insiemi di dati personali, come:

- la raccolta, registrazione, organizzazione, strutturazione, conservazione
- l'adattamento o la modifica, l'estrazione, la consultazione, l'uso
- la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione
- il raffronto o l'interconnessione
- la limitazione, la cancellazione, la distruzione.

Ambito di applicazione materiale

Il presente regolamento si applica al **TRATTAMENTO** manuale o automatizzato dei **DATI PERSONALI**



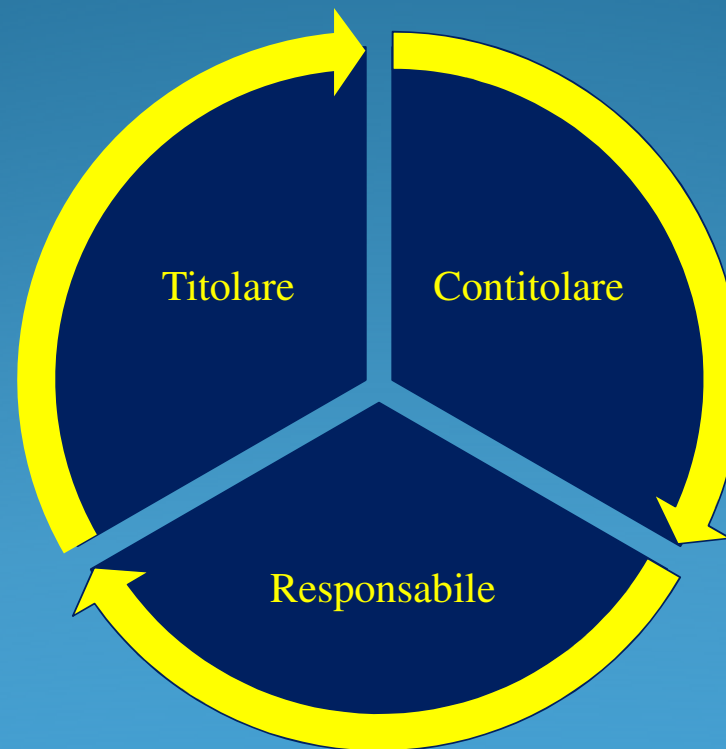
PERSONE FISICHE, NON GIURIDICHE

Casi di esclusione

Il presente regolamento **NON SI APPLICA** ai trattamenti di dati personali effettuati:

- per **attività che non rientrano nell'ambito di applicazione del diritto dell'Unione** come la Sicurezza nazionale
- dagli Stati Membri **nell'esercizio di attività che rientrano nell'ambito di applicazione del Titolo V - Capo 2, TUE** (Politica Estera e di difesa comune dell'Unione)
- dalle autorità competenti **ai fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali**
- da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o **domestico** (es. rubrica personale, mailing personale, fruizione di social network) e quindi senza una connessione con un'attività commerciale o professionale

Gli attori ed i ruoli



Il Titolare del trattamento

La **Persona fisica o Giuridica, l'Autorità Pubblica, il servizio od altro organismo** che (singolarmente o insieme ad altri):

DETERMINA le FINALITA' ed i MEZZI del trattamento di dati personali



Compiti del Titolare

- **adozione misure tecniche ed organizzative** per garantire un livello di sicurezza adeguato al rischio (es. pseudonimizzazione, cifratura, una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure adottate);
- **adozione del Registro delle attività di trattamento;**
- **nomina del DPO** nei casi previsti dal Regolamento;
- **notifica delle violazioni** dei dati personali;
- effettuazione di **valutazioni di impatto;**
- **procedure** tempestive di **rilevamento data breach;**
- **essere «accountable»:** dimostrare la conformità del trattamento con misure adeguate, tecniche ed organizzative, procedure, policy, adozione del registro del trattamento.

I nuovi imperativi del GDPR

- **Privacy by design**: i dati devono essere oggetto di protezione sin dalla progettazione



in fase di sviluppo, progettazione, selezione ed utilizzo di applicazioni, servizi e prodotti basati sul trattamento dei dati personali, si deve tener conto del diritto alla protezione dei dati.

- **Privacy by default**:

Il Regolamento impone di progettare misure e sistemi che abbiano come **impostazione predefinita** esclusivamente **l'uso** dei soli **dati necessari** per il perseguimento di una determinata finalità.

Poteri del Titolare

Il Titolare **decide** su:

- **Finalità** e mezzi (cfr. art. 4.7)
- **Profilo della sicurezza** (cfr. art. 24.1)

Può **individuare all'interno della sua struttura ruoli subordinati** (dipendenti e collaboratori) a cui affidare operazioni di trattamento, **istruendoli adeguatamente** (Soggetti Autorizzati) e può **esternalizzare attività di trattamento** designando Responsabili di trattamento ed istruendoli adeguatamente.

Il Responsabile del trattamento

La **Persona Fisica o Giuridica, l'Autorità Pubblica, il servizio od altro organismo** che **tratta** dati personali per conto del titolare del trattamento.

Responsabilità del titolare

Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che **presentino garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate** in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato (art. 28).



Nomina del Responsabile del trattamento ex art. 28 del GDPR

I trattamenti effettuati da parte di un Responsabile per conto del Titolare sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati Membri che stipuli:

- la **materia** disciplinata
- la **durata** del trattamento
- la **natura** e le **finalità** del trattamento
- il **tipo di dati** personali
- le **categorie di interessati**
- gli **obblighi** ed i **diritti del titolare** del trattamento



In base al contratto, il Responsabile del trattamento si impegna a:

- trattare i dati soltanto su istruzione documentata del titolare;
- consentire i trattamenti solo a persone autorizzate con impegno alla riservatezza o che abbiano un adeguato obbligo legale di riservatezza;
- adottare tutte le misure di sicurezza (es. cifratura, pseudonimizzazione, recupero da backup, ect.);
- rispettare le condizioni per ricorrere a un sub-responsabile del trattamento;
- assistere il titolare per dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
- cancellare o restituire tutti i dati e cancellare le copie esistenti;
- mettere a disposizione del titolare le informazioni per dimostrare il rispetto dei suddetti obblighi e consentire le ispezioni.



Soggetti Autorizzati al trattamento (ex incaricati)

- Persona fisica (dipendenti e collaboratori) **autorizzata a compiere operazioni di trattamento** dal Titolare o dal Responsabile
- **Chiunque** agisca sotto l'autorità del titolare o del responsabile del trattamento, e che **abbia accesso** ai dati personali **NON può** trattare tali dati **SE NON E' ISTRUITO** in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri;
- la sua **designazione** deve risultare **per iscritto** individuando puntualmente l'area di trattamento consentito (ex art. 29 del GDPR).



Principali compiti del soggetto autorizzato

- Deve **accedere** solo alle **banche dati** cui è **autorizzato**
- Deve **trattare** i dati secondo le **istruzioni impartite** dal titolare o dal responsabile
- Deve **rispettare** le misure tecniche ed organizzative adottate dal titolare



L'autorizzato riceve istruzioni per iscritto nelle quali si prescrive:

- **osservare** scrupolosamente gli **obblighi relativi alla riservatezza**, alla **comunicazione e diffusione** tanto dei dati personali trattati quanto delle credenziali di autenticazione attribuite
- mantenere **segreta la propria credenziale di autenticazione** (la password deve essere composta da almeno 8 caratteri, non deve essere riconducibile a riferimenti personali e deve essere modificata almeno ogni 6 mesi)
- **trattare i dati esclusivamente al fine di adempiere alle obbligazioni nascenti dall'incarico conferito**
- **custodire i dati - in particolare quelli «particolari» - mediante l'adozione di misure di sicurezza** disposte dal titolare al fine di evitare la perdita, la distruzione o l'accesso non autorizzato da parte di terzi

L'autorizzato riceve istruzioni per iscritto nelle quali si prescrive:

- in caso di allontanamento, anche temporaneo, dalla postazione di lavoro, verificare che non vi sia la possibilità da parte di terzi (anche se colleghi o comunque appartenenti alla struttura) di accedere ai dati personali per i quali era in corso una qualunque operazione di trattamento, mediante supporto cartaceo od informatico

salva schermo
con password

ritiro cartelle di lavoro su carta in cassetto



Sistema disciplinare

In caso di mancato rispetto delle istruzioni impartite dal Titolare del trattamento o delle misure di sicurezza adottate



verranno comminate adeguate sanzioni disciplinari a prescindere dall'effettiva realizzazione di un fatto-reato nonché dalla causazione di qualsiasi danno all'ente.





Principi applicabili al trattamento dei Dati Personali





1. Correttezza, trasparenza e liceità

- Correttezza

I soggetti interessati devono essere informati della raccolta dei loro dati, di come saranno utilizzati, della loro consultazione da parte di terzi e per quali trattamenti i dati saranno utilizzati.

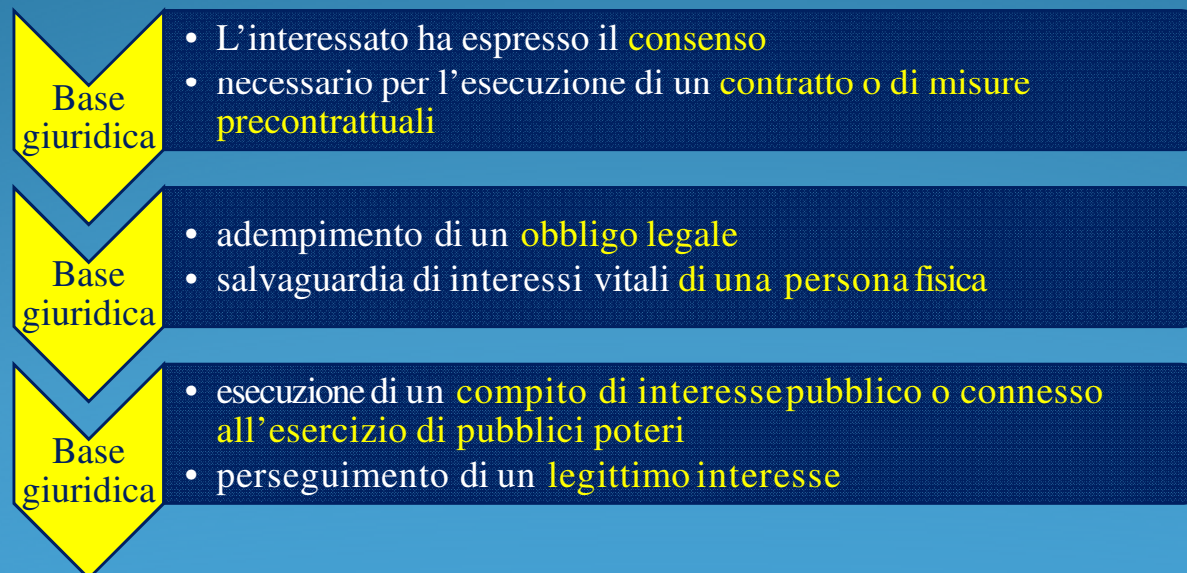
- Trasparenza

A) Le informazioni riguardanti le operazioni di trattamento devono essere fornite utilizzando un linguaggio semplice e chiaro, affinché gli interessati possano capire facilmente le norme, i rischi, le garanzie ed i diritti in questione;

B) Gli interessati hanno il diritto di accedere ai propri dati ovunque essi siano trattati.

Liceità del trattamento

Il trattamento è lecito **SOLO SE** e nella misura in cui **ricorra una delle seguenti condizioni**:



2. Limitazione della finalità

Caratteristiche delle finalità:

I dati personali devono essere raccolti per finalità determinate, esplicite e legittime.

Finalità ulteriori:

Il trattamento successivo dei dati raccolti **non potrà avvenire in modo incompatibile con le finalità originarie**.

Eventuali variazioni richiedono che il Titolare effettui una valutazione di compatibilità tra le finalità iniziali e quelle successive.

Deroga:

Un ulteriore trattamento di dati per finalità di archiviazione nel pubblico interesse o per finalità statistiche o di ricerca scientifica non è considerato incompatibile con le finalità iniziali.

2. Limitazione della finalità

Ogni nuova finalità di trattamento dei dati che non sia compatibile con le finalità iniziali deve avere la propria base giuridica specifica e NON può basarsi sul fatto che i dati fossero stati inizialmente acquisiti o trattati per un'altra finalità legittima.

Esempio: una compagnia aerea raccoglie i dati dei passeggeri per effettuare le prenotazioni e quindi i voli correttamente. A tale scopo avrà bisogno di dati relativi a numeri di posto dei passeggeri, limitazioni fisiche specifiche e richieste di pasti speciali.

Se alle compagnie aeree viene chiesto di trasmettere questi dati contenuti nel codice di prenotazione alle autorità preposte al controllo dell'immigrazione all'aeroporto di arrivo si è in presenza di un utilizzo di tali dati per finalità di controllo dell'immigrazione che differiscono dalla finalità della raccolta dei dati iniziale. La trasmissione di tali dati ad un'autorità di controllo dell'immigrazione richiederà, pertanto, una base giuridica nuova e distinta.

3. Minimizzazione dei dati

I dati personali devono essere:

adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

Pertinenza ed adeguatezza

Devono essere raccolti solo i dati che siano funzionali al perseguimento delle finalità predeterminate.

Non eccedenza e principio di necessità

Ai fini del trattamento effettuato bisogna ridurre al minimo l'uso di dati personali ed identificativi. Evitare, quindi, che vi sia identificabilità dell'interessato nel caso in cui il trattamento non lo richieda né lo imponga.

Esempio

Sito E-commerce

Se il sito richiede il nominativo e l'indirizzo di consegna, il comportamento da parte del richiedente è corretto.

Se richiede, per effettuare l'ordine, anche il rilascio di informazioni relative alla professione svolta verrebbe meno il principio di pertinenza in quanto queste informazioni saranno legate ad altre finalità (es. di marketing).

4. Esattezza

I dati personali devono essere:

- **esatti** e, se necessario, devono essere aggiornati;
- devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.

Aggiornamento

Il titolare deve trattare dati personali esatti, aggiornandoli ed organizzando la sua struttura in modo che essa sia in grado di garantire l'accuratezza delle informazioni personali.

- Sistemi di aggiornamento dei dati personali degli utenti
- Procedure periodiche di verifica e conferma dei dati

4. Esattezza

Il controllo regolare dell'esattezza dei dati, tra cui l'aggiornamento, costituisce una necessità assoluta a causa del potenziale danno per l'interessato qualora i dati dovessero rimanere inesatti.

Esempio: se un soggetto intende stipulare un contratto di finanziamento con un istituto bancario, la banca generalmente controllerà l'affidabilità creditizia del potenziale cliente. A tale fine, sono disponibili banche dati specifiche contenenti i dati sullo storico creditizio dei privati.

Se tale banca fornisce dati errati o non aggiornati riguardanti un individuo, questa persona può subire effetti negativi.

Pertanto, i titolari del trattamento di tali banche dati devono adoperarsi in modo specifico per rispettare il principio di esattezza.

5. Limitazione della conservazione

I dati personali devono essere:

conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;

I dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, ...fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato.

Limitazione della conservazione

I dati vanno conservati in modalità che renda identificabile l'interessato solo per il tempo strettamente necessario per le finalità del trattamento (i dati devono essere cancellati o anonimizzati non appena questi non siano più necessari alle finalità per cui sono stati raccolti)



Se fossero usati in forma identificativa anche successivamente al raggiungimento delle finalità prefissate al momento della raccolta, ne conseguirebbe un loro abuso.

Limitazione della conservazione

Il tempo di conservazione va valutato in relazione alla finalità del trattamento (alcuni tempi sono stabiliti dalle leggi o obblighi contrattuali, altri sono stabili direttamente dal titolare. Il Garante ha emanato dei provvedimenti che aiutano il titolare nella fissazione dei tempi di conservazione).

Il Titolare deve stabilire un termine per la cancellazione o per la verifica periodica per garantire che i dati non siano conservati più a lungo del necessario.



6. Integrità e riservatezza

I dati personali devono essere:

trattati in maniera da **garantirne un'adeguata sicurezza**, compresa la protezione, mediante misure tecniche ed organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

Adeguatezza sicurezza

Adeguatezza sicurezza si traduce in:

- **misure tecniche** (adozione di misure di sicurezza, uso della pseudonimizzazione, data protection by design e by default, cifratura dei dati, codici di condotta, certificazioni, ..)
- **misure organizzative** (procedure di autorizzazione per l'accesso ai dati, separazione delle informazioni funzionali alla reidentificazione in caso di pseudonimizzazione, procedure di controllo, procedure di backup e disaster recovery, DPIA, ..)

Violazioni della sicurezza ed integrità dei dati

Ai sensi dell'art. 4.12) del GDPR «**violazione dei dati personali**» è

«la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati»

L'adeguata sicurezza deve essere garantita **ex ante** per evitare eventi dannosi, ma anche **ex post** per sanare le anomalie riscontrate.

Misure ex ante

Vanno considerate tutte le misure previste dall'art.32, tra cui:

- pseudonimizzazione
- valutazione dei Rischi (DPIA: Data Protection Impact Assessment)
- il rispetto delle istruzioni impartite dal Titolare

Misure ex post

Oltre a tutte le attività informatiche necessarie va ricordato:

- il procedimento di notifica della violazione dei dati all'autorità di controllo
- comunicazione della violazione agli interessati

Riservatezza

Il Considerando 83 menziona esplicitamente la **riservatezza** come **adeguato livello di sicurezza dei dati**



L'obiettivo del Titolare deve essere quello di impedire anche l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento.

Responsabilizzazione del Titolare – Principio di Accountability

La PRINCIPALE NOVITA' introdotta dal regolamento è il **PRINCIPIO** di «**RESPONSABILIZZAZIONE**» (cd. *accountability*), che attribuisce direttamente ai titolari del trattamento il compito di assicurare - ed essere in grado di comprovare - il rispetto dei principi applicabili al trattamento dei dati personali (art. 24).



Il titolare è **competente per il rispetto dei principi applicabili al trattamento dei dati**
e deve essere **in grado di provarlo**



Principio di Accountability – Punti salienti

- 1) La responsabilizzazione richiede da parte dei Titolari e dei Responsabili del trattamento di adottare attivamente ed in modo permanente misure finalizzate alla promozione ed alla salvaguardia della protezione dei dati nelle attività di trattamento;
- 2) i Titolari ed i Responsabili del trattamento sono responsabili della conformità alla normativa in materia di protezione dei dati nell'ambito delle operazioni di trattamento e dei rispettivi obblighi;
- 3) I Titolari del trattamento devono essere in grado di dimostrare in qualsiasi momento agli interessati ed alle autorità di controllo che essi operano in conformità alle disposizioni sulla protezione dei dati.

Principio di Accountability – Approccio sostanziale

Il titolare è tenuto a predisporre tutti gli accorgimenti necessari per garantire la sicurezza dei dati in relazione agli specifici trattamenti che ha il compito di presidiare.

Inoltre è chiamato a saper render conto delle scelte fatte e delle soluzioni adottate, così da dimostrare di aver adempiuto correttamente a quanto prescritto dal Regolamento



Il Regolamento predilige un approccio di tipo sostanziale in grado di rispondere alle situazioni concrete cercando di volta in volta le soluzioni più adeguate e non limitandosi a riprodurre meccanicamente degli adempimenti prescritti.

Come garantire il rispetto del Principio di Accountability?

- Tenere un **registro delle attività di trattamento** e, su richiesta, metterlo a disposizione dell'autorità di controllo;
- designare il responsabile della protezione dei dati («**DPO**») che è coinvolto in tutte le questioni connesse alla protezione dei dati personali;
- svolgere **valutazioni d'impatto sulla protezione dei dati** per i tipi di trattamento che presentano un rischio elevato per i diritti e le libertà delle persone fisiche;
- **garantire la protezione dei dati fin dalla progettazione**;
- **mettere in atto misure tecniche ed organizzative adeguate** per garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al Regolamento;
- **disporre di documentazione atta a dimostrare** agli interessati ed alle autorità di controllo le **misure adottate** per conseguire il rispetto delle norme in materia di protezione dei dati;
- prevedere **modalità e procedure per l'esercizio dei diritti degli interessati**;
- **aderire a codici di condotta approvati o a meccanismi di certificazione**.

Principali Diritti dell'Interessato (art. 12-22 del Regolamento)





GDPR e Misure idonee di sicurezza

Obblighi di sicurezza – Le novità

Non si parla più di «misure minime» ma di «misure idonee». Tenere un registro delle attività di trattamento e, su richiesta, metterlo a disposizione dell'autorità di controllo;

- pseudonimizzazione e cifratura dei dati: anonimizzare l'identità del soggetto e/o usare sistemi di cifratura del dato
- assicurare riservatezza, integrità, disponibilità e resilienza dei sistemi: politiche di accesso ai dati, di backup e di alta affidabilità
- assicurare tempestivamente la disponibilità e l'accesso ai dati in caso di incidente: procedure per la ri-messa in produzione dei sistemi e dei software che permettono l'accesso ai dati
- meccanismi di monitoraggio dell'efficacia

Framework Nazionale per la Cybersecurity

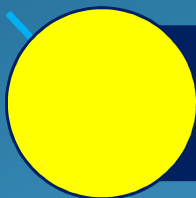
Il **Framework Nazionale** ha delineato un quadro di riferimento con linee guida di comportamento atte a prevenire attacchi informatici.



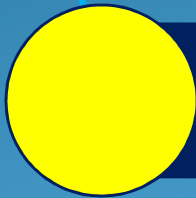
Le misure minime che le imprese devono adottare («controlli essenziali di cybersecurity») sono le seguenti:



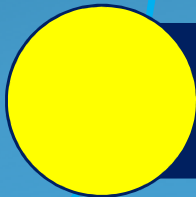
Framework Nazionale per la Cybersecurity – «Controlli Essenziali di Cybersecurity»



Le **password sono diverse per ogni account**, della complessità adeguata e viene valutato l'utilizzo dei sistemi di autenticazione più sicuri offerti dal provider di servizio

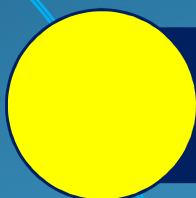


Il personale autorizzato all'accesso, remoto o locale, ai servizi informatici dispone di utenze personali non condivise con altri; **l'accesso è opportunamente protetto** i vecchi account non più utilizzati sono disattivati

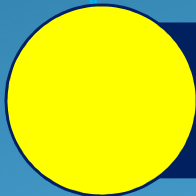


Ogni utente può accedere solo alle informazioni ed ai sistemi di cui necessita e/o di sua competenza

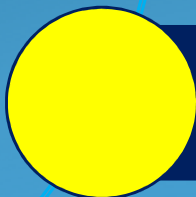
Framework Nazionale per la Cybersecurity – «Controlli Essenziali di Cybersecurity»



Il personale è adeguatamente sensibilizzato e formato sui rischi di cybersecurity e sulle pratiche da adottare per l'impiego sicuro degli strumenti aziendali. I vertici aziendali hanno cura di predisporre per tutto il personale aziendale la formazione necessaria a fornire almeno le nozioni basilari di sicurezza

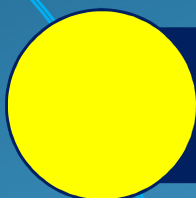


La configurazione iniziale di tutti i dispositivi è svolta da personale esperto, responsabile per la configurazione sicura degli stessi. Le credenziali di default di accesso sono sempre sostituite

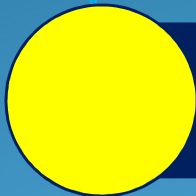


Sono eseguiti periodicamente backup delle informazioni e dei dati critici per l'azienda. I backup sono conservati in modo sicuro e verificati periodicamente

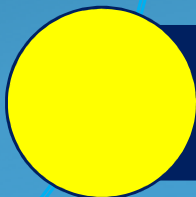
Framework Nazionale per la Cybersecurity – «Controlli Essenziali di Cybersecurity»



Le reti ed i sistemi sono protetti da accessi non autorizzati attraverso strumenti specifici



In caso di incidente, vengono informati i responsabili della sicurezza ed i sistemi vengono messi in sicurezza da personale esperto



Tutti i software in uso (inclusi i firmware) sono aggiornati all'ultima versione consigliata dal produttore. I dispositivi o i software obsoleti e non più aggiornabili sono dismessi.

Obblighi di sicurezza – DATA BREACH (violazione dei dati personali)

Qualsiasi **violazione di sicurezza** che **comporta accidentalmente** (es. smarrimento fascicoli, furto pc) **o in modo illecito** (es. attacco informatico):

la **distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali** trasmessi, conservati o comunque trattati.

Quali rischi per l'interessato?

- furto o usurpazione d'identità
- perdite finanziarie
- pregiudizio alla reputazione
- perdita di riservatezza o qualsiasi altro danno economico e sociale significativo alla persona fisica interessata



Alcuni possibili esempi di Data Breach



Alcuni esempi possibili:

- accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware etc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.



Alcuni possibili esempi di Data Breach

Anche una perdita temporanea di disponibilità può costituire una violazione di dati personali:

Esempio

In ambito ospedaliero, se i dati clinici cruciali di un paziente risultano non disponibili, anche solo momentaneamente, questa situazione può mettere a rischio i diritti e le libertà del singolo; un intervento chirurgico, ad esempio, può essere cancellato a rischio della vita.



UK: clinica per l'identità di genere divulga per errore quasi 2000 indirizzi email

Una clinica per l'identità di genere vicino Londra ha inviato una email per un concorso d'arte ai propri pazienti, mettendo in CC quasi 2000 indirizzi email. Accortasi dell'errore, la clinica non è più riuscita ad annullare l'invio.

La violazione, che verrà notificata al Garante UK, è un esempio di data breach imputabile a un errore umano all'interno all'organizzazione.



In caso di VIOLAZIONE DATI PERSONALI (C.D. DATA BREACH)

- Segnalare al titolare del trattamento (o al proprio responsabile gerarchico) eventuali situazioni di rischio per la sicurezza dei dati di cui è venuto a conoscenza (es. violazione della password, il tentativo di accesso non autorizzato ai sistemi)

- **AVVISARE TEMPESTIVAMENTE IL TITOLARE (O IL PROPRIO RESPONSABILE GERARCHICO) QUALORA SI ABBIA EVIDENZA O ANCHE SOLO IL SOSPETTO CHE SIA IN CORSO UNA VIOLAZIONE DI DATI (C.D. «DATA BREACH»)**



Notifica DATA BREACH (art. 33 del Regolamento)

Il **Titolare del trattamento**, non appena viene a conoscenza di un'avvenuta violazione di dati personali, **DEVE NOTIFICARE LA VIOLAZIONE AL GARANTE** ove possibile (e nei casi previsti dall'art. 34 anche all'interessato – rischio elevato per diritti e libertà), **entro 72 ore** dal momento in cui ne è venuto a conoscenza, **a meno che non sia in grado di dimostrare che**, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati presenti un rischio per i diritti e le libertà delle persone fisiche.

Il Titolare del trattamento **DOCUMENTA** tutte le violazioni (a prescindere dalla notifica al Garante) di **dati personali**, ad esempio predisponendo un apposito registro.



Oggetto della notifica Data Breach:

- Descrizione della **natura della violazione** e delle **categorie** (ed il numero approssimativo) di **interessati** in questione
- indicazione del **nome e dei dati di contatto del DPO** (Responsabile della Protezione Dati)
- descrizione delle **probabili conseguenze della violazione** dei dati personali
- descrizione delle **misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione** dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi



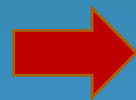
Sistema sanzionatorio nella nuova disciplina Privacy



Responsabilità connesse al trattamento dei dati personali

Il mancato rispetto degli obblighi previsti dal Regolamento e dal Codice della Privacy

ESPONE IL TITOLARE, IL RESPONSABILE ED I SINGOLI SOGGETTI AUTORIZZATI A RISCHI SUL PIANO DELLE RESPONSABILITA' E DELLE SANZIONI A LIVELLO



CIVILE

AMMINISTRATIVO

PENALE



SANZIONI AMMINISTRATIVE PECUNIARIE EX ART. 83 DEL GDPR

Sanzione amministrativa fino ad un massimo di 10.000.000 Euro o, nel caso di imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore

In caso di violazione degli obblighi:

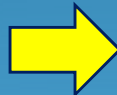
- del Titolare del trattamento e del Responsabile del trattamento
 - dell'organismo di certificazione
 - dell'organismo di controllo
-

Esempi di illeciti rilevanti:

- Violazione del principio della privacy by design e by default
- Violazione della disciplina in tema di data breach notification
- Violazione della disciplina in tema di comunicazione di un data breach all'interessato
- Violazione della disciplina in tema di data protection impact assessment
- Mancata nomina del DPO nei casi previsti dal Regolamento

SANZIONI AMMINISTRATIVE PECUNIARIE EX ART. 83 DEL GDPR

Sanzione amministrativa
fino ad un massimo di
20.000.000 Euro o, nel
caso di imprese fino al 4%
del fatturato mondiale
annuo dell'esercizio
precedente, se superiore,



In caso di violazione di:

- i principi di base del trattamento, comprese le condizioni relative al consenso
- i diritti degli interessati
- i trasferimenti di dati personali ad un destinatario in un paese terzo o un'organizzazione internazionale
- qualsiasi obbligo ai sensi delle legislazioni degli Stati Membri adottate a norma del Capo IX
- inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'Autorità di Controllo (Garante)

SANZIONI AMMINISTRATIVE PECUNIARIE EX ART. 83 DEL GDPR

Esempi di illeciti rilevanti:

- Violazione dei principi «privacy»
 - Violazione della disciplina sulla liceità del trattamento
 - Violazione della disciplina sul consenso
 - Violazione della disciplina sulle particolari categorie di dati
 - Violazione della disciplina in tema di informativa, comunicazione e modalità di esercizio dei diritti
- Violazione della disciplina in tema di diritto di opposizione al trattamento
 - Violazione della disciplina sul trattamento nell'ambito del rapporto di lavoro
 - Violazione della disciplina in tema di obblighi di sicurezza
 - Inosservanza di un ordine dell'Autorità di Controllo

SANZIONI AMMINISTRATIVE PECUNIARIE

Le Sanzioni Amministrative Pecuniarie di cui all'art. 83 del GDPR **SI APPLICANO ANCHE NEI SEGUENTI CASI:**

- Violazione disposizioni di cui all'art. 166 del D.lgs. n. 101/18;
- Violazione delle misure di garanzia e delle regole deontologiche previste rispettivamente dagli artt. 2 septies e 2 quater del D.lgs. n. 101/18
- Violazioni di cui all'art. 1, co. 9 e 10 della L. 11 gennaio 2018 n. 5 e violazioni di cui all'art. 5 ter del D.lgs. n. 33/2013.

WP29 (Article 29 Data Protection Working Party) “Linee guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del Reg. Ue n. 679/16” adottate il 3 ottobre 2017

Le sanzioni sono inflitte «*in funzione delle circostanze di ogni singolo caso*», sia in aggiunta che anche in sostituzione ad una «*misura correttiva*»

Poteri correttivi ex art. 58 co. 2 del Gdpr:

- a) rivolgere **avvertimenti** al titolare o al responsabile sul fatto che i trattamenti previsti possono verosimilmente violare le disposizioni del presente regolamento (nel caso in cui la violazione non è ancora avvenuta);
- b) rivolgere **ammonimenti** al titolare o al responsabile ove i trattamenti abbiano violato le disposizioni del GDPR;
- c) **ingiungere** al titolare o al responsabile di **soddisfare le richieste dell'interessato di esercitare i diritti** loro derivanti dal GDPR;
- d) **ingiungere** al titolare o al responsabile di **conformare i trattamenti alle disposizioni del GDPR**, se del caso, in una determinata maniera ed entro un determinato termine;
- e) **ingiungere** al titolare di **comunicare all'interessato una violazione dei dati personali**;

WP29 (Article 29 Data Protection Working Party) “Linee guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del Reg. Ue n. 679/16” adottate il 3 ottobre 2017

- f) imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento;
- g) ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento a norma degli articoli 16, 17 e 18 e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali ai sensi dell'articolo 17, paragrafo 2, e dell'articolo 19;
- h) revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti;
- i) ordinare la sospensione dei flussi di dati extra UE.

PROCEDIMENTO SANZIONATORIO (art. 166 del Codice della Privacy)

L'Autorità può adottare un provvedimento sanzionatorio di tipo amministrativo in tre specifiche situazioni:



Reclamo dell'interessato



Attività istruttoria di iniziativa del Garante



Accessi, ispezioni e/o verifiche del Garante

PROCEDIMENTO

- Il procedimento per l'adozione dei provvedimenti ex art. 58 e delle sanzioni amministrative inizia con la **notifica al titolare o al responsabile del trattamento e delle presunte violazioni**.
- **Entro trenta giorni** dal ricevimento di tale notifica il contravventore può inviare al Garante scritti difensivi o documenti e può chiedere di essere sentito.
- Il Garante, dopo aver accertato la violazione, **sarà chiamato a decidere l'ammontare della sanzione valutando caso per caso la situazione**.

APPLICAZIONE LEGGE 689/'81

SANZIONI PENALI PREVISTE DAL NUOVO CODICE DELLA PRIVACY

TRATTAMENTO ILLECITO DI DATI (art. 167)

COMUNICAZIONE E DIFFUSIONE ILLECITA DI DATI PERSONALI OGGETTO DI TRATTAMENTO SU LARGA SCALA (art. 167 bis)

ACQUISIZIONE FRAUDOLENTA DI DATI PERSONALI OGGETTO DI TRATTAMENTO SU LARGA SCALA (art. 167 ter)

FALSITA' NELLE DICHIARAZIONI AL GARANTE ED INTERRUZIONE NELL'ESECUZIONE DEI COMPITI O DELL'ESERCIZIO DEI POTERI DEL GARANTE (art. 168)

INOSSERVANZA DEI PROVVEDIMENTI DEL GARANTE (art. 170)



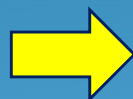
Estensione dell'applicazione delle sanzioni penali non solo ai casi in cui si accerti il dolo dell'agente volto a trarre per sé o per altri profitto (come era previsto ante riforma)
MA ANCHE AI CASI IN CUI L'AGENTE ABBA AGITO ALLO SCOPO DI ARRECARE AD ALTRI UN DANNO



Le prime sanzioni a livello europeo

Garante privacy francese VS Google

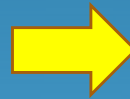
A seguito di due denunce presentate in data 25 e 28 maggio 2018 dall'organizzazione NOYB («None of Your Business»), Google è stata condannata al pagamento di una **sanzione pari a 50 milioni di Euro** per violazione del GDPR, ed in particolare per:



- 1) **Violazione degli obblighi di trasparenza ed informazioni:** le informazioni sulle modalità di trattamento dei dati degli utenti non sono state fornite in modo chiaro e facilmente accessibile (in particolare, alcune informazioni essenziali, quali, le finalità di trattamento, il periodo di conservazione, le varie tipologie di dati trattati erano sparse in vari documenti e non era agevole per l'utente accedere alle informazioni utili);
- 2) **Consenso inidoneo:** l'utilizzo dei dati finalizzato alla personalizzazione dei messaggi pubblicitari è fondato su un consenso inidoneo in quanto non sufficientemente informato e neppure specifico e chiaro (in particolare, la casella del consenso era preflaggata e l'utente, se contrario alla profilazione pubblicitaria, avrebbe dovuto procedere alla deselegione, pratica contraria al GDPR secondo cui il consenso deve provenire dall'interessato tramite un'azione positiva e chiara).

Garante privacy austriaco

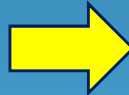
In Austria, nel mese di ottobre 2018, l'Autorità Garante ha erogato, a seguito di apposita ispezione, una sanzione da 4 mila Euro ad una azienda che utilizzava il sistema di videosorveglianza in modo non appropriato, ed in particolare:



Le telecamere erano direzionate su parte del marciapiede esterno al perimetro aziendale tanto da riprendere senza alcuna giustificata motivazione e senza idonea informativa rilasciata con apposita cartellonistica, in violazione dei principi della privacy più comuni, in quanto venivano ripresi i volti dei passanti senza che essi ne fossero debitamente informati.

Garante privacy tedesco

In data 22/11/18 il Garante per la protezione dei dati, sanzionava un sito di chat online al pagamento di una multa di 20 mila Euro.

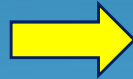


La contestazione mossa dal Garante ha come oggetto la **violazione dell'art. 32 del GDPR**, posto che, per carenza di adeguate misure di sicurezza, il sito subiva una **perdita di circa 2 milioni di username/password e di più di 800 mila indirizzi e-mail, oltre ai recapiti di residenza degli utenti e di altri tipi di dati.**

In sede di applicazione della sanzione, nel determinare l'ammontare della stessa, il Garante valutava positivamente il comportamento collaborativo dell'azienda la quale aveva provveduto ad informare immediatamente i suoi utenti ed aveva apportato modifiche alla sua infrastruttura IT per accrescere il livello di sicurezza.

Garante privacy italiano VS. Associazione Rousseau

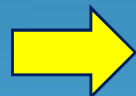
Con provvedimento n. 83 del 4 aprile 2019, il Garante per la protezione dei dati personali ha comminato all'Associazione Rousseau, quale responsabile del trattamento ed in tale qualità trasgressore, il pagamento di Euro 50 mila a titolo di sanzione per la violazione di cui al combinato disposto degli artt. 32 ed 83, par. 4 lett. a) del Reg. Ue n. 679/16. In particolare, a seguito di attività ispettiva, il Garante ha accertato:



- il mancato completo tracciamento degli accessi al database del sistema Rousseau e delle operazioni sullo stesso compiute che configura la violazione di quel generale dovere di controllo sulla liceità dei trattamenti gravante sul titolare del trattamento e, in particolare, dell'obbligo di assicurare più adeguate garanzie di riservatezza agli iscritti alla piattaforma medesima;
- la condivisione delle credenziali di autenticazione da parte di più incaricati dotati di elevati privilegi per la gestione della piattaforma Rousseau e la mancata definizione e configurazione dei differenti profili di autorizzazione in modo da limitare l'accesso ai soli dati necessari nei diversi ambiti di operatività. In tal caso, quindi si configura una violazione dell'obbligo di predisposizione, da parte del responsabile del trattamento, di misure tecniche e organizzative adeguate.

Garante privacy italiano

Con provvedimento del 14/02/19 il Garante per la protezione dei dati ha comminato una sanzione di **16 mila Euro ad un medico per trattamento illecito di dati.**



A seguito di apposita istruttoria, il Garante per la privacy ha ritenuto sussistente la responsabilità del medico sotto due distinti profili:

- il professionista **non ha reso l'informativa** né al momento della registrazione dei dati dei pazienti né alla prima comunicazione in violazione dell'art. 14 del GDPR;
- il medico **ha utilizzato i dati dei pazienti per finalità diverse da quelle di cura per le quali erano stati raccolti** (i dati raccolti nell'ambito dell'attività di tutela della salute erano stati utilizzati per fini di propaganda elettorale).

SANITA' E PRIVACY



Trattamento di particolari categorie di dati – art. 9 GDPR

1.E' vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare **dati genetici, dati biometrici** intesi ad identificare in modo univoco una persona fisica, **dati relativi alla salute** o alla vita sessuale o all'orientamento sessuale della persona.

Il paragrafo 1 non si applica se si verifica uno dei casi indicati al comma 2 del predetto articolo:

Es. Art. 9, co. 2, lett. h):

Il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, **diagnosi, assistenza o terapia sanitaria** o sociale ovvero gestione dei sistemi e dei servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3.

Trattamento di particolari categorie di dati – art. 9 GDPR

Es. Art. 9, co. 2, lett. i):

Il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri (es. compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione; tutela sociale della maternità ed interruzione volontaria di gravidanza; attività socio-assistenziali a tutela di minori e soggetti bisognosi, non autosufficienti ed incapaci etc., ex art. 2 sexies del Codice).

Misure di Garanzia per il trattamento di dati genetici, biometrici e relativi alla salute

GDPR, art. 9 par. 4:

Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute.

Nuovo Codice Privacy, art. 2 - septies:

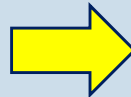
I dati genetici, biometrici e relativi alla salute, possono essere oggetto di trattamento...in conformità alle **misure di garanzia disposte dal Garante, nel rispetto di quanto previsto dal presente articolo.**

Nuovo Codice Privacy –Poteri Garante, art. 2-septies:

Il Garante dispone **misure di garanzia**

Misure di Garanzia (art. 2-septies)

Il Provvedimento che stabilisce le misure di garanzia di cui al comma 1 è adottato con **cadenza almeno biennale** e tenendo conto:



- Delle **linee guida, delle raccomandazioni e delle migliori prassi** pubblicate dal **Comitato Europeo per la protezione dei dati** e delle migliori prassi in materia di trattamento dei dati personali;
- Dell'**evoluzione scientifica e tecnologica** nel settore oggetto delle misure;
- Dell'**interesse alla libera circolazione dei dati personali** nel territorio dell'Unione Europea.

Misure di Garanzia (art. 2-septies)

Le misure di garanzia sono **adottate in relazione a ciascuna categoria di dati personali, avendo riguardo alle specifiche finalità del trattamento** e possono individuare, in conformità a quanto previsto al comma 2, ulteriori condizioni sulla base delle quali il trattamento dei dati è consentito.

In particolare, **le misure di garanzie individuano:**

- le misure di sicurezza, ivi comprese quelle tecniche di cifratura, di pseudonimizzazione e di minimizzazione;
- le specifiche modalità per l'accesso selettivo ai dati e per rendere le informazioni agli interessati;
- nonché le eventuali altre misure necessarie a garantire i diritti degli interessati.

Misure di Garanzia (art. 2-septies)

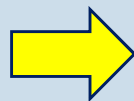
Le misure di garanzia che riguardano i dati genetici ed il trattamento dei dati relativi alla salute per finalità di prevenzione, diagnosi e cura, nonché quelle di cui al comma 4, lett. b), c) e d), sono adottate sentito il Ministro della Salute che, a tal fine, acquisisce il parere del Consiglio Superiore di Sanità.

Limitatamente ai **dati genetici**, le misure di garanzia possono individuare, in caso di particolare ed elevato livello di rischio, il consenso come ulteriore misura di protezione dei diritti dell'interessato...o altre cautele specifiche.

Nel rispetto dei principi in materia di protezione dei dati personali, con riferimento agli obblighi di cui all'art. 32 del Regolamento, è ammesso l'utilizzo dei dati biometrici con riguardo alle procedure di accesso fisico e logico ai dati da parte dei soggetti autorizzati, nel rispetto delle misure di garanzia di cui al presente articolo.

Trattamento dei dati in ambito sanitario

Il trattamento dei dati personali in ambito sanitario è disciplinato dal:



Titolo V – Artt. 75 – 92 del Nuovo Codice della Privacy (D.lgs. n. 196/03 così come modificato dal D.lgs. n. 101/2018)

Art. 92 Nuovo Codice Privacy- Cartelle Cliniche

Art. 92, co. 2:

Eventuali richieste di presa visione o di rilascio di copia della cartella e dell'acclusa scheda di dimissione ospedaliera da parte di soggetti diversi dall'interessato possono essere accolte, in tutto o in parte, solo se la richiesta è giustificata da documentata necessità:

- di esercitare o difendere un diritto in sede giudiziaria ai sensi dell'art. 9, par. 2, lett. f) del Regolamento, di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale;
- di tutelare, in conformità alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante di rango pari a quella dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale.

DPIA – Data Protection Impact Assessment



E' un processo ciclico che prevede **l'analisi continua dei possibili rischi elevati** gravanti sul trattamento di dati personali e l'adozione delle misure necessarie alla riduzione dei rischi per i diritti e le libertà fondamentali delle persone fisiche.

Il DPIA è un importante strumento per il Titolare per raggiungere e dimostrare la *compliance* al Gdpr.



Fattori che indicano un «rischio elevato» (Linee guida sulla DPIA del WP29)

1) Dati sensibili o dati aventi carattere altamente personale

2) Monitoraggio sistematico

3) Dati relativi ad interessati vulnerabili (minori, dipendenti, pazienti ed ogni caso in cui sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del titolare del trattamento)

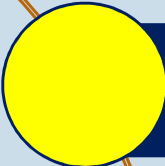
Esempi:

1) Un ospedale che conserva le cartelle cliniche dei pazienti

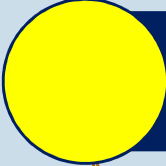
2) Utilizzo di sistemi di videosorveglianza e geolocalizzazione che consentono la sorveglianza remota delle attività svolte dai dipendenti



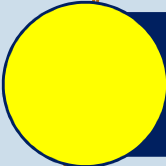
DPIA – Esempi di trattamenti che richiedono una DPIA



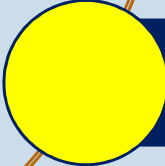
Trattamenti non occasionali di **dati relativi a soggetti vulnerabili** (minori, disabili, infermi di mente, pazienti etc.)



Trattamenti effettuati **nell'ambito del rapporto di lavoro mediante sistemi tecnologici** (es. videosorveglianza e geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti;



Trattamento di **particolari categorie di dati ai sensi dell'art. 9 del Gdpr** (es. dati relativi alla salute) oppure di dati relativi a condanne penali ed a reati di cui all'art. 10 del Gdpr;



Trattamenti sistematici di **dati genetici**, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

Provvedimenti adottati dal Garante per la protezione dei dati personali in ambito sanitario



Provvedimento n. 55 del 7 marzo 2019:

«Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario»

Trattare «categorie particolari di dati» in ambito sanitario è sempre vietato, **TRANNE CHE PER:**



- a) Motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri (art. 9, par. 2, lett.g) del Regolamento ed art. 2 sexies del Codice);
- b) Motivi di interesse pubblico nel settore della sanità pubblica (es. emergenze sanitarie – art. 9, par. 2, lett. i) del Regolamento);
- c) **Finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria o sociale** ovvero gestione dei sistemi e servizi sanitari o sociali («finalità di cura», ex art. 9, par. 2, lett. h) del Regolamento).

Provvedimento n. 55 del 7 marzo 2019

I TRATTAMENTI
NECESSARI
AL PERSEGUIMENTO DI
SPECIFICHE
FINALITA' DI CURA, ossia:

ESSENZIALI PER IL
RAGGIUNGIMENTO DI UNA O
PIU' FINALITA'
DETERMINATE ED
ESPLICITAMENTE
CONNESSE ALLA CURA DELLA
SALUTE

EFFETTUATI DA O SOTTO LA
RESPONSABILITA' DI UN
PROFESSIONISTA SANITARIO
SOGGETTO AL SEGRETO
PROFESSIONALE O DA ALTRA
PERSONA ANCH'ESSA
SOGGETTA ALL'OBBLIGO DI
SEGRETEZZA



NON RICHIEDONO
IL CONSENSO
DELL'INTERESSATO

Provvedimento n. 55 del 7 marzo 2019



Adobe Acrobat
Document

IL CONSENSO E' SEMPRE NECESSARIO

PER I TRATTAMENTI
ATTINENTI IN SENSO
LATO ALLA CURA

E

NON STRETTAMENTE
NECESSARI

ESEMPI

➤ CONSULTAZIONE DEL
FASCICOLO SANITARIO
ELETTRONICO (D.L. 18/10/12 n.
179, art. 12, co.5)

➤ CONSEGNA DEL REFERTO
ONLINE (DPCM dell'8/8/13, art.5)

➤ DOSSIER SANITARIO (Linee
Guida del 4 giugno 2015)



Regione Piemonte,
Prot. 25775/A1416B del
12/12/18: «le soluzioni
aziendali dovranno
acquisire
preventivamente (prima
dell'atto di refertazione)
l'eventuale volontà
manifestata dal paziente
di alimentare il proprio
fascicolo sanitario in
modalità oscurata.



Provvedimento n. 55 del 7 marzo 2019

Tempi di conservazione dei Dati personali:



I tempi di conservazione devono sempre essere indicati nell'informativa



Qualora i tempi non siano fissati da specifiche norme, spetta al Titolare definirli in base alle finalità di trattamento

Provvedimento n. 55 del 7 marzo 2019



I tempi di conservazione della documentazione sanitaria non sono stati modificati dalla disciplina sulla protezione dei dati personali e rimangono pienamente in vigore.

Ad esempio:

- le **Cartelle cliniche, unitamente ai relativi referti**, vanno conservate illimitatamente (Circolare del Ministero della Sanità del 19 dicembre 1986 n. 900)
- la **documentazione iconografica radiologica** deve essere conservata per un periodo non inferiore a 10 anni (art. 4, d.m. 14 febbraio 1997).



Provvedimento n. 55 del 7 marzo 2019

Ulteriori prescrizioni impartite dal Garante nel provvedimento in oggetto:



L'**informativa** deve essere concisa, trasparente, intelligibile e facilmente accessibile, scritta con linguaggio semplice e chiaro



La **nomina del DPO** è obbligatoria per gli organismi pubblici e nel caso di trattamenti su larga scala (es. ospedali e case di cura)



La **tenuta del registro dei trattamenti** è obbligatoria (strumento di *accountability* e di gestione del rischio)

Parere del 10 gennaio 2019

Nel parere del 10 gennaio 2019 reso ad un'azienda sanitaria nell'ambito del riesame di un provvedimento di rigetto riguardante un accesso civico ai dati sanitari di un paziente deceduto,

il Garante ha affermato

il principio secondo cui le persone decedute continuano a godere delle tutele previste dalla disciplina nazionale in materia di protezione dei dati personali anche dopo l'applicazione del Gdpr.

L'istanza di accesso era stata rivolta ai sensi del d.lgs. n. 33/13 (c.d. decreto Trasparenza) all'azienda sanitaria da una persona che, in relazione ad un presunto caso di *maltpractice*, attraverso il c.d. Foia, intendeva avere accesso agli atti di audit clinico ed agli approfondimenti condotti dal risk manager, quindi ad una documentazione contenente informazioni particolarmente riservate relative ad un paziente deceduto (ricovero, sintomi, anamnesi, diagnosi, esami effettuati, alcuni particolarmente invasivi, terapia, farmaci somministrati, credo professato).

Il Legislatore Italiano, con il d.lgs. n. 101/18 ha sancito che i diritti relativi ai dati personali dei defunti possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione. Di conseguenza, ai dati delle persone decedute continuano ad applicarsi le tutele previste dalla disciplina nazionale sulla protezione dei dati.

Parere del 10 gennaio 2019



Inoltre, per quanto riguarda la richiesta di accesso alla documentazione sanitaria, il Garante ha affermato che questo tipo di informazioni non sono accessibili con il Foia.

Il Codice sulla protezione dei dati personali prevede infatti un espresso «divieto di diffusione» di dati relativi alla salute per cui è impossibile darne «conoscenza a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione».

La vicenda rientra dunque in una delle ipotesi di esclusione dell'accesso civico previste dalla normativa sulla trasparenza, che prevede espressamente come l'accesso civico debba essere escluso nei casi di «divieto di accesso o divulgazione previsti dalla legge»; il Garante ha quindi concluso che l'Azienda sanitaria ha correttamente respinto l'istanza di accesso.

Provvedimento del 16 gennaio 2019

Il Garante ha fornito indicazioni ad un'azienda ospedaliera che chiedeva di poter trasmettere,

pur in mancanza di una sufficiente base normativa per la comunicazione,

i dati di tutto il personale infermieristico al relativo ordine professionale il quale intendeva effettuare controlli sulle iscrizioni e verificare che tutti gli infermieri in servizio rispettassero i requisiti previsti dalla l. n.3/18 (c.d. legge Lorenzin).

Il Garante **ha escluso che le strutture sanitarie possano trasmettere in modo massivo i dati** di tutto il loro personale infermieristico all'Ordine professionale di riferimento,

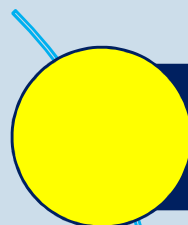
evidenziando che l'attuale quadro normativo non attribuisce agli Ordini – pur dotati di specifici poteri disciplinari e di vigilanza – **competenze per generalizzate attività di ricerca e raccolta di informazioni personali riferite al personale infermieristico.**

Spetta invece al datore di lavoro l'obbligo di effettuare le necessarie verifiche sul possesso di particolari requisiti previsti per l'accesso a specifici impieghi,

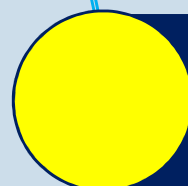
inclusa l'iscrizione del singolo professionista al relativo albo che, tra l'altro, è pubblico e reperibile anche online.

Provvedimento n. 146 del 5 giugno 2019

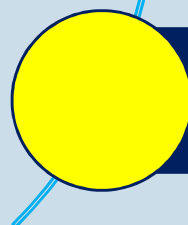
*«Prescrizioni relative al trattamento di categorie particolari di dati»
riguardanti, in particolare:*



Il trattamento di categorie particolari di dati nei rapporti di lavoro

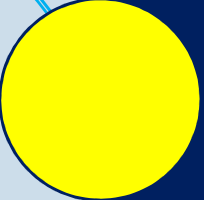


I dati genetici

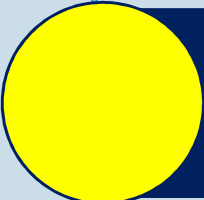


I dati personali per scopi di ricerca scientifica

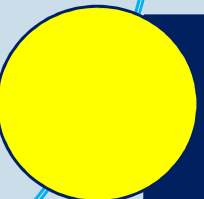
Provvedimento n. 146 del 5 giugno 2019: Esempi di Prescrizioni specifiche sul trattamento dei dati genetici



L'accesso ai locali deve avvenire secondo una documentata procedura prestabilita dal titolare del trattamento che preveda l'identificazione delle persone preventivamente autorizzate (è ammesso l'utilizzo di dati biometrici);



La **conservazione, l'utilizzo ed il trasporto** dei campioni biologici sono posti in essere con modalità volte a garantirne la qualità, l'integrità, la disponibilità, la tracciabilità;



I dati sono trattati con tecniche di cifratura o di pseudonimizzazione o di altre soluzioni che li rendano temporaneamente intelligibili anche a chi è autorizzato ad accedervi e permettano di identificare l'interessato solo in caso di necessità.

Provvedimento n. 146 del 5 giugno 2019: casi in cui è necessario il CONSENSO al trattamento dei dati genetici

- Finalità di tutela della salute di un soggetto terzo
- Lo svolgimento di test genetici nell'ambito di investigazioni difensive o per l'esercizio di un diritto in sede giudiziaria, salvo che un'espressa disposizione di legge, o un provvedimento dell'autorità giudiziaria in conformità alla legge, disponga altrimenti
- I trattamenti effettuati mediante test genetici, compreso lo screening, ai fini di ricerca o di ricongiungimento familiare
- Finalità di ricerca scientifica e statistica non previste dalla legge o da altro requisito specifico di cui all'art. 9 del Regolamento.

Ai sensi dell'art. 75 del Nuovo Codice della Privacy **restano salve le disposizioni di settore precedenti all'applicazione del Regolamento.**

Sanzioni applicate ad oggi dopo il nuovo GDPR





Il Caso dell'Ospedale Portoghese (Deliberazione CNPD 984/2018 – Procedimento 9932/2018 - i trattamenti contestati riguardano i dati sanitari dei pazienti)

E' stata comminata una sanzione di Euro 400.000 in ragione del **non corretto accesso ai dati dei pazienti da parte dei dipendenti interni che non avrebbero dovuto essere autorizzati.**

In particolare, nell'ambito dell'ispezione eseguita dall'Autorità Garante relativamente al sistema informativo e di gestione dell'ospedale, **veniva contestata:**

- 1) la totale **manca** di un qualsiasi **documento/procedura dove fosse prevista la corrispondenza o i criteri per stabilire tale corrispondenza tra le competenze funzionali degli utenti del sistema informatico ed i relativi profili di accesso;**
- 2) la totale **manca** anche di un **documento/procedura dove fossero stabilite le regole per la creazione degli account degli utenti del sistema informatico dell'ospedale;**
- 3) il **non corretto utilizzo dei profili e dei codici di accesso previsti nei sistemi gestionali utilizzati dall'ospedale.** In particolare, l'ospedale utilizza due sistemi gestionali messi a disposizione del Ministero della Salute, uno (SONHO) per la gestione amministrativa, l'altro (Scclinico) dove vengono registrate le informazioni cliniche dei pazienti.



Il Caso dell'Ospedale Portoghese

L'applicazione SONHO prevede la creazione di account personali degli utilizzatori, con l'associazione di codici preimpostati per cui a ciascun codice corrispondono diversi profili di accesso ai dati.

Nella gestione ordinaria dell'ospedale alcuni degli utenti «tecnici» avevano associato anche il codice riservato ai medici, di fatto accedendo all'intero fascicolo clinico dei pazienti.

Al momento dell'ispezione risultavano quasi 1000 utenti cui era associato il profilo di accesso ai dati riservato ai medici, a fronte di un numero di medici in servizio effettivo di 296; l'Autorità riscontrava l'esistenza di molti profili di fatto inattivi collegati ad utenti che avevano operato nell'ospedale in forza di contratti a termine, mai disabilitati.



Il Caso dell'Ospedale Portoghese

L'Autorità Garante alla luce delle rilevanze di fatto ha quindi contestato:

- la **violazione del principio di minimizzazione**, a causa dell'accesso indiscriminato ai dati personali e particolari dei pazienti anche da parte di soggetti che non avrebbero avuto alcuna necessità di accesso al fine di svolgere i propri compiti professionali;
- la **violazione dei principi di integrità e riservatezza** a causa della mancata adozione di misure tecniche e soprattutto organizzative volte ad impedire l'accesso indiscriminato ai dati;
- la **mancata adozione da parte del Titolare del trattamento di misure tecniche ed organizzative adeguate al rischio**, nonché di **procedure idonee a garantire un monitoraggio costante del sistema di trattamento dei dati**.



Il Caso dell'Ospedale Portoghese

L'ammontare della sanzione è stato determinato ai sensi dell'art. 83 del Reg. Ue n. 679/16 tenendo conto:

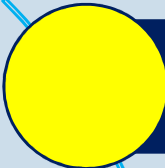
- della **tipologia di dati coinvolti**, della **durata di tempo della violazione**, del **numero di interessati coinvolti** e della **gravità dei danni dagli stessi subiti**;
- della **negligenza nell'adozione delle misure organizzative e tecniche da parte dell'Ospedale**, che per l'Autorità sfociano nel dolo eventuale nel momento in cui il Titolare ha permesso coscientemente l'associazione di profili di accesso al sistema informativo con profili operativi/funzionali non corrispondenti;
- è stato invece valutato positivamente l'atteggiamento collaborativo del Titolare volto ad attenuare le conseguenze negative delle violazioni.

Considerazioni alla luce del Caso dell'Ospedale Portoghese

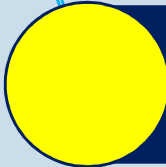
La questione del corretto accesso ai dati personali dei pazienti deve essere affrontata sia sotto l'aspetto organizzativo che tecnico:

1) Profilo organizzativo: la struttura sanitaria deve avere sotto controllo il personale attivo, indipendentemente che si tratti di subordinati, consulenti o dipendenti dei fornitori, il che significa conoscerne l'identità ed il ruolo che ricopre (es. amministrativo, operatore sanitario, controllo clinico e di gestione, etc.).

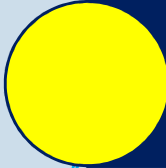
Esempi Misure Organizzative



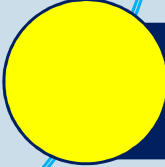
L'accesso agli armadi/locali dove sono conservati i documenti cartacei è filtrato (es. le chiavi sono in gestione solo ad alcune persone);



Le operazioni compiute in archivio (es. consultazione, copia, estrazione, restituzione) sono annotate sul registro degli accessi (es. nome, ora e data, operazione, documento);



L'accesso agli archivi informatizzati gestiti da diversi applicativi software è consentito solo alle persone il cui ruolo è coerente con il processo aziendale supportato dai sistemi;



Le operazioni compiute con i diversi applicativi software sono tracciate e registrate.

Considerazioni alla luce del Caso dell'Ospedale Portoghese

2) Profilo tecnico: relativamente a questo aspetto si possono presentare due diverse soluzioni:

1. Ogni applicativo software gestisce gli accessi attraverso l'identificazione dell'utente (che inserisce la coppia di credenziali di cui è in possesso), **il meccanismo di autenticazione** (che verifica l'identità presentata dall'utente - PIN, password, dato biometrico – e concede l'accesso alle risorse), **il meccanismo di autorizzazione** (che filtra l'accesso alle risorse secondo i privilegi accordati all'utente autenticato, in base al profilo che gli è stato attribuito; la profilazione può arrivare a determinare quali operazioni informatiche di trattamento dei dati l'utente può compiere o meno: registrazione, adattamento o modifica, consultazione, stampa, estrazione, cancellazione).

2. La struttura sanitaria è dotata di un sistema centralizzato (ed unico) di gestione degli accessi ai diversi applicativi software.

Considerazioni alla luce del Caso dell'Ospedale Portoghese

Nel primo caso, ogni utente dovrà utilizzare una coppia di credenziali per ogni applicativo software che intende utilizzare; l'amministratore di sistema dovrà attribuire ad ogni utente il profilo coerente con il ruolo in ogni applicativo software, in sincronia con le risultanze dell'Ufficio del Personale e della Direzione Sanitaria.

Nel secondo caso, l'amministratore di sistema definisce a quali applicativi software ogni utente può accedere e quali operazioni può compiere (es. solo consultazione, estrazione e stampa inibita etc.); l'utente userà una sola coppia di credenziali per accedere agli applicativi software.

Il Caso dell'Ospedale dell'Aia

Un'elevata **sanzione, pari a 460 mila euro**, è stata comminata dal Garante privacy olandese all'ospedale di Haga, situato a L'Aia,
per un'insufficiente protezione dei file dei pazienti.



La violazione dell'art. 32 del GDPR è stata rilevata quando è emerso che decine di membri del personale ospedaliero avevano controllato le cartelle cliniche di un noto personaggio olandese, star di un reality televisivo, senza necessità, in quanto non coinvolti nella terapia del paziente.

Per spingere l'ospedale a migliorare la sicurezza dei file dei pazienti, il Garante olandese ha ingiunto all'ospedale l'implementazione di adeguate misure di sicurezza entro il 2 ottobre 2019, pena il pagamento di 100 mila euro ogni due settimane per un massimo di 300 mila euro.

Il Caso dell'Azienda Sanitaria Locale di Alessandria

Un'attività di controllo presso l'Ospedale Santo Spirito di Casale Monferrato quale presidio ospedaliero dell'Azienda Sanitaria Locale di Alessandria ha consentito di accertare che l'Azienda in oggetto ha effettuato, quale titolare, un trattamento di dati personali attraverso il dossier sanitario senza che, alla data degli accertamenti ispettivi effettuati in data 29 e 30 novembre 2017 (quindi prima della data di piena applicazione del Regolamento) fosse resa un'idonea informativa e raccolto uno specifico consenso degli interessati.



E' stata comminata una sanzione pari a 16.000 Euro (ai fini della determinazione della sanzione si è tenuto conto della normativa vigente all'epoca dei fatti e, dunque, del vecchio Codice della Privacy).

Uso Illecito dei Dati degli accertamenti medici



Il Garante ha ritenuto **illecito** il trattamento effettuato da un'azienda sanitaria che ha messo a disposizione di una società che fornisce apparecchiature per l'alta diagnostica le immagini Tac dei pazienti determinando così una «**comunicazione di informazioni**» **sulla salute di alcuni pazienti identificati in assenza di un'adeguata base normativa.** Parimenti illecito è stato ritenuto il trattamento svolto dalla società in questione.

La designazione della stessa come «responsabile del trattamento» da parte dell'azienda sanitaria non giustifica l'acquisizione delle immagini della Tac.

Le operazioni eseguite perseguono, infatti, finalità proprie della società (partecipazione alla gara e difesa in giudizio) non riconducibili a quelle per le quali era stata designata **responsabile. Tra queste rientrano, ad esempio, le attività di manutenzione per garantire l'efficienza dell'apparecchiatura e la qualità delle immagini della Tac.**

Il Garante rilevati gli illeciti amministrativi svolti dall'azienda sanitaria e dalla società ha avviato i relativi procedimenti sanzionatori.

«I rischi del furto di dati? Errori e discriminazioni anche nelle cure», intervista al Presidente del Garante Privacy

Principali violazioni accertate:

«In alcune Regioni il software del dossier sanitario elettronico metteva a disposizione di tutti i medici dell'ASL (e non solo a quello curante) i dati di tutti i pazienti.

*Un'altra **Regione** è stata **sanzionata per aver pubblicato, sul sito istituzionale, informazioni sensibili su 5 mila disabili che avevano usufruito di sussidi per l'acquisto di computer.***

*Una **struttura sanitaria privata** è stata **sanzionata per aver comunicato i dati dei pazienti – senza aver richiesto il consenso – alle case farmaceutiche** (i dati degli interessati erano stati raccolti nell'ambito di una campagna di prevenzione obbligatoria)».*

«I rischi del furto di dati? Errori e discriminazioni anche nelle cure», intervista al Presidente del Garante Privacy

Conseguenze dei furti:

«I dati sanitari se illecitamente trattati o «rubati» sono suscettibili di esporre l'interessato a forme di discriminazione pericolose, rese possibili dalla conoscenza degli aspetti più intimi della persona, come quelli «idonei a rivelare lo stato di salute dell'interessato».

«La sottrazione o l'alterazione di un dato sanitario rende vulnerabili anche dati essenziali per il governo del nostro Paese, si pensi ai sistemi informativi sanitari delle ASL, delle Regioni o del Ministero della Salute che sono indispensabili per la gestione della sanità pubblica;

MA SOPRATTUTTO, la vulnerabilità rischia di determinare errori diagnostici o terapeutici, con conseguenze anche letali per l'interessato e gravi responsabilità per gli stessi operatori sanitari».

«I rischi del furto di dati? Errori e discriminazioni anche nelle cure», intervista al Presidente del Garante Privacy

OBBLIGO GENERALE DI COMUNICARE EVENTUALI DATA BREACH ALL'AUTORITA' NAZIONALE DI PROTEZIONE DEI DATI, E, NEI CASI PIU' GRAVI, A TUTTE LE PERSONE COINVOLTE, INDICANDO ANCHE LE MISURE ADOTTATE PER LIMITARE LE POSSIBILI CONSEGUENZE NEGATIVE.

Il Sole **24 ORE**

15 marzo 2018

...i primi hacker avevano come unico scopo quello dimostrativo, trovare falle in un sistema e farsi beffe di chi lo aveva sviluppato. Adesso, la stragrande maggioranza degli attacchi informatici avviene per motivi molto meno ideologici o goliardici. Si può trattare di gruppi indipendenti di criminali, di squadre governative o lupi solitari, ma ognuno mira a un obiettivo ben preciso: **soldi, dati o sabotaggio.**

Una dimostrazione l'abbiamo avuta con quanto è accaduto con i ransomware. Questo tipo di attacco su vasta scala ha avuto così tanto successo che alcuni gruppi hanno deciso di farne la propria principale fonte di introiti, **spingendosi sui bersagli più sensibili: gli ospedali.**

I PUNTI CRITICI/2

Se gli ospedali e i ministeri diventano i target preferiti

di **Giancarlo Calzetta**

Il cybercriminale ha mille volti e ognuno di questi ha mille sfaccettature. I primi hacker avevano come unico scopo quello dimostrativo, trovare falle in un sistema e farsi beffe di chi lo aveva sviluppato. Adesso, la stragrande maggioranza degli attacchi informatici avviene per motivi molto meno ideologici o goliardici: i pirati informatici moderni sono più fedeli al proprio nome e agiscono solo per un personale tornaconto. Si può trattare di gruppi indipendenti di criminali, di squadre governative, lupi solitari o aggregati fluidi, ma ognuno mira a un obiettivo ben preciso: soldi, dati o sabotaggio.

Una dimostrazione di quanto possano essere determinati e "criminali" gli intenti dei gruppi indipendenti o dei lupi solitari lo si ha analizzando quanto è accaduto con i ransomware. Questo tipo di attacco su vasta scala ha avuto così tanto successo che alcuni gruppi hanno deciso di farne la propria principale fonte di introiti, spingendosi sui bersagli più sensibili: gli ospedali.

Il servizio nazionale inglese sembra particolarmente vulnerabile al proble-

ma dato che ha subito diversi attacchi mirati. Il ransomware Bit Paymer è stato sviluppato appositamente per attaccare gli ospedali della Scozia. La sua diffusione sembra sia stata effettuata mirando direttamente ai computer interni ai vari reparti, forzando le password dei terminali esposti su Internet. Una tecnica molto diversa da quella che "spara nel mucchio" tramite l'invio di milioni di email a quanti più indirizzi internet possibile. Del resto, una volta che si è riusciti a prendere possesso dei dati dei pazienti, i criminali hanno il coltello dalla parte del manico. Nel 2016, per esempio, un ospedale del Kansas ha deciso di pagare troppo velocemente una richiesta di riscatto per liberare i propri sistemi informatici da un ransomware, ma i pirati, intuita la fretta dei responsabili, invece di consegnare la chiave di decrittazione come pattuito, hanno alzato la richiesta, raddoppiandola. A questo punto, l'ospedale ha capito che non si trovava davanti a persone affidabili e ha deciso di non pagare ulteriormente, ma l'evento ha ricordato a tutti che quando si ha a che fare con dei cybercriminali, la levatura morale non è diversa da quella dei criminali di strada.

La soluzione? A volte pagare

Purtroppo, gli ospedali sono bersagli molto sensibili e un attacco ransomware che va a segno porta sempre conseguenze gravi. Del resto, la frenesia che caratterizza ogni procedura è tale che applicare le regole di sicurezza rallenterebbe l'operato di medici e infermieri al pun-

Il furto dei dati sanitari

IN ITALIA



8.400

Gli attacchi noti di particolare gravità, avvenuti nel mondo,
inclusa quindi l'Italia (1/1/2011 - 31/12/2018)

di cui

1.536

nel 2018
(+36% rispetto
al 2017)



150

Gli attacchi
noti nel settore
«Health»

23

di particolare
gravità

Siti della sanità pubblica hackerati
dai movimenti Anonymous Italia,
LulzSecIta e AntiSecIta*



Attacchi gravi

- Osp. S. Andrea (Rm)



Attacchi dimostrativi

- Azienda Sanitaria Provinciale (RC)
- Sistema Informativo Veterinario Ministero della salute (Rm)
- Federazione Italiana Medici Medicina Generale (Pi)
- Azienda sanitaria locale Ciriè, Chivasso e Ivrea (To)
- Portale Cure Primarie Ulss 21 Legnago (Vr)
- Istituto di Ricovero e Cura a Carattere Scientifico (An)
- Sistema Sanitario Sardegna Ospedale Brotzu (Ca)
- Asl (Ri)
- Asl (Vt)
- Osp. S. Giovanni (Rm)
- Istituto superiore di sanità (Rm)
- Agenzia nazionale per i servizi sanitari regionali (Rm)
- Difarma (distribuzione farmaceutica in Sardegna)
- Federsanità
- Asst Lariana (Co)
- Asl (Cs)

* Sul blog di Anonymous Italia sono stati pubblicati «dati sensibili» (12.143 email, username e password) solo dell'ospedale S. Andrea di Roma; per tutti gli altri sono state pubblicate solo le strutture dei database

Fonte: Rapporto Clusit 2019; Anonymous Italia

La Privacy è CULTURA

