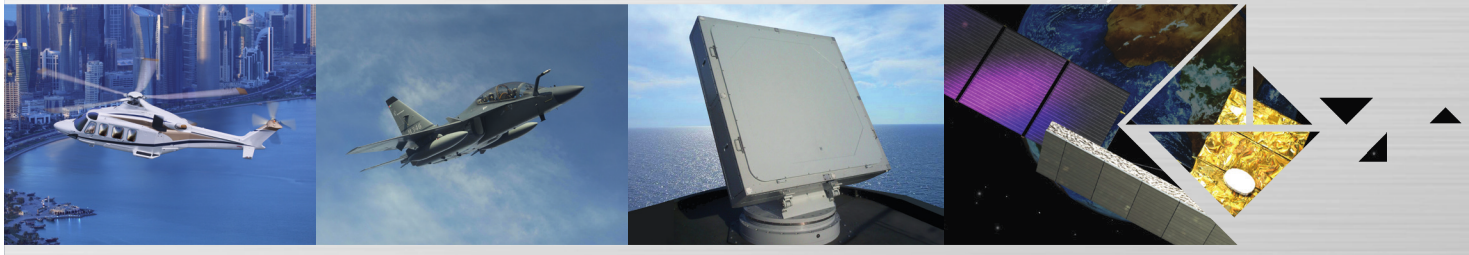
PRIVACY: REGOLAMENTO UE 2016/679 E IMPATTO SULL'ASL AL

Data, 7 e 12 NOVEMBRE 2019

Alessandria



LEONARDO
CYBER SECURITY

1948 • 2018

REGOLAMENTO UE 2016/679 E IMPATTO SULL'ASL AL

Agenda

Ora inizio	Ora fine	Argomento
14:00	14:10	• Introduzione sul GDPR o Premesse e programma evento
14:10	14:20	• Aspetti salienti della normativa o Le principali novità
14:20	14:40	• Impatto del GDPR sull'ASL AL o L'approccio, i Processi e il sistema di Governance per la Data Protection o Attività realizzate
14:40	14:50	• GDPR: Violazioni e responsabilità o Emesse le prime sanzioni
14:50	15:00	• Conclusioni

INTRODUZIONE: REGOLAMENTO UE 2016/679

Premesse

L'Azienda Sanitaria Locale Alessandria ("ASL AL"), considera la tutela della privacy dei propri assistiti, nonché del personale dipendente e dei collaboratori un elemento essenziale e prioritario per il conseguimento degli obiettivi dell'Azienda.

In tal senso, l'ASL AL è costantemente impegnata ai fini dell'adeguamento al nuovo Regolamento Europeo sulla Protezione dei Dati Personali (General Data Privacy Regulation), pienamente applicabile **a decorrere dal 25 Maggio 2018**, ivi comprese le disposizioni per l'adeguamento dell'ordinamento nazionale al GDPR introdotte dal D.Lgs. 10 agosto 2018, n.101.

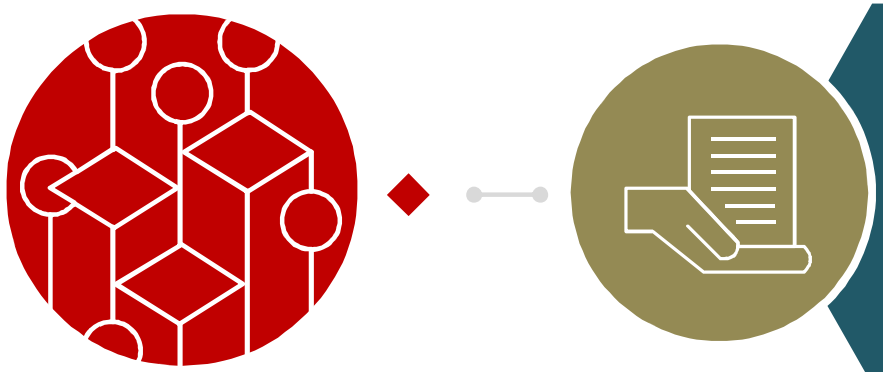
L'impostazione del GDPR pone l'accento sulla tutela dei diritti dell'interessato, ponendo modifiche ed integrazioni alla precedente normativa in materia di tutela dei dati personali.

N.B. Si precisa che, in merito alla normativa nazionale, trova attuazione sia il D.Lgs. 30/06/2013, n. 196, così come modificato dagli artt. da 1 a 16 e 27 del D.Lgs. 101/2018, sia le ulteriori prescrizioni contenute negli artt. da 17 a 26 del D.Lgs. 101/2018.

ASPETTI SALIENTI DELLA NORMATIVA

DATA PROTECTION - ASPETTI SALIENTI DELLA NORMATIVA

Significato di trattamento



Trattamento (art. 4.2, GDPR)

Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la 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 o la distruzione

DATA PROTECTION - ASPETTI SALIENTI DELLA NORMATIVA

Definizioni

Dato personale (art. 4.1, GDPR)

Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»)..., direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Categorie particolari di Dati Personali (art. 9, GDPR)

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 a identificare in modo univoco una persona fisica, **dati relativi alla salute** o alla vita sessuale o all'orientamento sessuale della persona.

Dati personali relativi a condanne penali e reati (art. 10, GDPR)

Dati personali relativi a condanne penali e reati o a connesse misure di sicurezza.

DATA PROTECTION - ASPETTI SALIENTI DELLA NORMATIVA

Le principali novità 1/2

Il principio di Accountability

Il titolare dovrà dimostrare l'adozione di politiche privacy e misure adeguate in conformità al Regolamento anche attraverso l'adesione a Codici di condotta e meccanismi di certificazione.

Il Data Breach

Gli obblighi di notifica seguente a data breach vengono estesi a qualsiasi caso in cui vi sia violazione dei dati personali. Viene poi esteso l'obbligo di darne comunicazione all'interessato nel caso in cui vi sia rischio elevato per i diritti e le libertà dello stesso.

Data Protection Officer (DPO o RDP)

La principale Responsabilità del DPO è quella di osservare, valutare e organizzare la gestione del trattamento di dati personali (e dunque la loro protezione) all'interno dell'Azienda affinché questi siano trattati nel rispetto delle normative privacy europee e nazionali.

Privacy Impact Assessment

Il GDPR prevede un approccio riskbased. È necesario effettuare un Privacy Impact Assessment, ovvero una valutazione dei rischi per i trattamenti previsti. L'implementazione delle misure di sicurezza adottate terrà conto dell'analisi dei rischi e dei costi di attuazione.

La Privacy By Design e By Default

Il GDPR disciplina l'obbligo di assicurare che le misure adottate attuino efficacemente i principi di privacy by design (protezione dei dati fin dalla progettazione) e privacy by default (impostazione predefinita che preveda il trattamento dei soli dati necessari al perseguimento delle finalità dichiarate).

Registri delle attività di trattamento

Il Titolare deve redigere e conservare un Registro delle attività di trattamento dei dati personali all'interno del quale descrivere le finalità e le modalità dei trattamenti. Il registro adottato dall'ASL ha forma scritta, anche elettronica, e dovrà essere esibito su richiesta al Garante Privacy.

DATA PROTECTION - ASPETTI SALIENTI DELLA NORMATIVA

Le principali novità 2/2

One-stop Shop

Il Regolamento si applica al trattamento effettuato nell'ambito delle attività di uno stabilimento, di un Titolare o di un Responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione. Altresì se non stabiliti nell'Unione ma trattando dati di cittadini europei.

Portabilità dei dati

Il GDPR sancisce l'obbligo di garantire all'interessato la trasmissione diretta dei dati personali da un Titolare all'altro, se tecnicamente fattibile, senza impedimenti.

Diritto all'oblio

Il Titolare del trattamento deve garantire all'interessato la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo (Right to be forgotten).

Gestione filiera Responsabili esterni

Il Responsabile esterno del trattamento deve dichiarare fin dall'inizio delle operazioni di trattamento la filiera di sub fornitori di cui intenderà avvalersi. Qualora vi sia la necessità di sostituire un sub fornitore, tale variazione dovrà essere comunicata al Titolare, pena l'annullabilità del contratto tra le parti.

Comitato Europeo protezione dati

Il Comitato è tenuto a consigliare la Commissione europea in merito a qualsiasi questione relativa alla protezione dei dati personali dell'UE, comprese eventuali proposte di modifica del Nuovo Regolamento europeo,

Sanzioni

Sono previste sanzioni amministrative pecuniarie e penali. Si precisa che le sanzioni penali sono state definite e comminate dall'ordinamento nazionale con D.Lgs. n.101/2018.

DATA PROTECTION - ASPETTI SALIENTI DELLA NORMATIVA

L’informativa nel Regolamento

L'art. 12 del Regolamento definisce "informativa", quel nucleo di informazioni che il titolare del trattamento è tenuto a fornire ai soggetti di cui si appresta a trattare i dati.

Secondo la normativa comunitaria, infatti, l'informativa deve esser concisa, trasparente, intellegibile e facilmente accessibile.

Il Regolamento ha previsto due ipotesi diverse di informativa, a seconda che i dati siano o meno raccolti presso l'interessato:

I dati sono raccolti dal Titolare del trattamento

I dati vengano raccolti presso soggetti diversi dall'interessato

DATA PROTECTION - ASPETTI SALIENTI DELLA NORMATIVA

Diritti dell'interessato – Diritto di accesso e diritto di rettifica

Diritto di accesso (Art. 15 Regolamento UE 2016/679)

L'art. 1 5 del Regolamento UE 2016/679 garantisce il diritto dell'Interessato di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai propri dati personali.

Diritto di rettifica (Art. 16 Regolamento UE 2016/679)

L'art. 16 del Regolamento UE 2016/679 stabilisce che l'interessato ha il diritto di ottenere la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo.
L'interessato ha altresì il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

DATA PROTECTION – DIRITTI DELL'INTERESSATO

Diritti dell'interessato

Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato (Art. 12 Regolamento UE 2016/679, commi 3, 4 e 5)

L'art. 12 del Regolamento UE 2016/679 (commi 3, 4 e 5) stabilisce che il Titolare del trattamento fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta ai sensi degli artt. da 15 a 22 senza ingiustificato ritardo e, comunque, al più tardi **entro un mese** dal ricevimento della richiesta stessa.
Tale termine può essere prorogato di **due mesi**, se necessario, tenuto conto della complessità e del numero di richieste. Il titolare deve informare l'interessato di tale proroga e dei motivi del ritardo, entro un mese dal ricevimento della richiesta.

Le informazioni rese ai sensi degli artt. 13 e 15, dal 15 al 22 sono gratuite. Se le richieste dell'interessato sono manifestatamente infondate o eccessive, il titolare può attribuire un contributo spese.

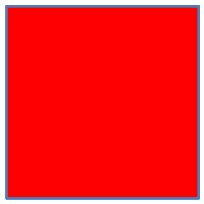
FACCIAMO UN QUIZ: VERO O FALSO?

Domanda e risposte

I dati personali si distinguono in: Anagrafici e comuni, particolari o sensibili e/o giudiziari?

Risposta esatta

Sì



No

FACCIAMO UN QUIZ: VERO O FALSO?

Domanda e risposte

La retribuzione è un dato personale di tipo particolare ovvero sensibile?

Sì

Risposta esatta

No

IMPATTO DEL GDPR SULL'ASL AL

DATA PROTECTION - IL REGISTRO DEI TRATTAMENTI

Articolo 30 del GDPR, comma 1

"1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

Le finalità del trattamento

Una descrizione delle categorie di interessati e delle categorie di dati personali

Le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali

Ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati

Ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale

Ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'Art. 32, Par. 1

DATA PROTECTION: IL SISTEMA DI GOVERNANCE IN ASL AL

Il Registro dell'ASL AL

IL SISTEMA DI GOVERNANCE IN ASL AL: I PROCESSI

Alcune delle principali attività realizzate (1/2)

Realizzato il "Registro delle attività di trattamento"

Realizzato il "Registro delle attività di trattamento", **ai sensi ed in conformità dell'art. 30 del GDPR.**
In considerazione dell'applicazione del REGOLAMENTO (UE) 2016/679, l'ASL AL ha ritenuto necessario effettuare, in primis, un'attività di assessment privacy per la verifica dei trattamenti dei dati i cui risultati sono riportati nel documento. L'applicazione del documento riguarda la rete ospedaliera, la rete territoriale, il Dipartimento di Prevenzione e l'area Amministrativa dell'ASL AL.

Disegnato il processo per la valutazione d'impatto privacy ("DPIA")

Prodotto una metodologia per la conduzione delle attività di **Data Protection Impact Assessment** ("D*PIA*"), **di cui all'art. 35 del GDPR**.
Secondo la legge è necessario che il titolare effettui attività di valutazione d'impatto sulla protezione dei dati personali (PIA), al fine della preventiva identificazione dei rischi specifici connessi al trattamento da effettuare.
L'approccio metodologico scelto dall'ASL AL per definire il processo di PIA si basa su quanto disposto dalla norma ISO/IEC 29134:2017.

.

IL SISTEMA DI GOVERNANCE IN ASL AL: I PROCESSI

Alcune delle principali attività realizzate (2/2)

Realizzata procedura per la gestione delle violazioni dei dati (Data Breach)

Definito il processo di gestione Data Breach.
Obiettivo della procedura è quello di disciplinare il processo di violazione dei dati personali (Personal Data Breach), ai sensi degli artt. 33 " Notifica di una violazione dei dati personali all'autorità di controllo" e 34 "Comunicazione di una violazione dei dati personali all'interessato", del GDPR, ossia di tutte le attività di analisi e valutazione, notifica/comunicazione, risposta e follow-up per la gestione del Personal Data Breach

Elaborata della nuova modulistica in sostituzione della precedente

Realizzata, ad esempio, la nuova modulistica relativa all'informativa sul trattamento dei dati e alla prestazione del consenso. In particolare, il titolare ha modificato il modello standard adottato dalla Direzione Sanitaria e relativo all'ambito sanitario ospedaliero (prestazioni di ricovero ospedaliero e ambulatoriali), adottando un nuovo fac-simile in coerenza con i nuovi contenuti previsti dal GDPR.

RIEPILOGO DELLE PRINCIPALI ATTIVITA' REALIZZATE

Effettuata un'attività di "Assessment Privacy", la cui applicazione, ha riguardato la rete ospedaliera, la rete territoriale, il Dipartimento di Prevenzione e l'area Amministrativa.

Realizzato il "Registro delle attività di trattamento", ai sensi ed in conformità dell'art. 30 del GDPR.

Designato un Data Protection Officer ("DPO") – in proroga fino al 31/12/2019. Deliberazione del DG n.2018/441 del 27/06/2018 ad oggetto: Designazione del Responsabile della Protezione dei Dati Personali (RDP/DPO) ai sensi dell'art. 37 del Reg. UE 2016/679.

Prodotto adeguamento in materia di **Dossier Sanitario Elettronico** ("DSE"), mediante produzione della necessaria modulistica di Informativa sul trattamento dei dati, ai sensi dell'art. 13 del GDPR e di richiesta del consenso.

Redatta della **nuova modulistica** (ad esempio modello standard di Informativa e consenso in ambito privacy) in conformità al GDPR.

Definito il processo per la gestione del **Personal Data Breach**. Obiettivo della procedura è quello di disciplinare il processo di violazione dei dati personali, ai sensi degli artt. 33 e 34 del Regolamento UE 2016/679.

Acquisita una metodologia per la conduzione delle attività di **Data Protection Impact Assessment** ("DPIA"), di cui all'art. 35 del Regolamento UE 2016/679.

FACCIAMO UN QUIZ: VERO O FALSO?

Domanda e risposte

La tenuta del Registro dei trattamenti è obbligatoria?

Risposta esatta 

Sì

No

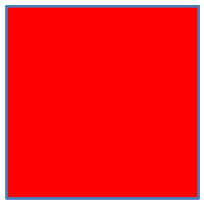
FACCIAMO UN QUIZ: VERO O FALSO?

Domanda e risposte

E’ obbligatorio fornire al paziente le informazioni sul trattamento dei dati?

Risposta esatta

Sì



No

GDPR: VIOLAZIONI E RESPONSABILITA’

DATA PROTECTION - RESPONSABILITA' E SANZIONI

Sanzioni amministrative

<u>Chiunque</u> ha il diritto di ottenere il *risarcimento del danno* dal titolare del trattamento o dal responsabile del trattamento, qualora subisca un danno materiale o immateriale causato da una violazione del GDPR.

Sono previste sanzioni amministrative pecuniarie e penali.
Le sanzioni penali sono state definite e comminate dall'ordinamento nazionale con D.Lgs. n.101/2018.

Sanzioni amministrative pecuniarie.
Devono essere effettive, proporzionate e dissuasive. Entità.

- **Fino a 10 000 000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore,** in caso di violazione delle seguenti disposizioni riguardanti:
  - **gli obblighi del titolare del trattamento e del responsabile del trattamento** a norma degli articoli 8 (Liceità del trattamento), 11 (Processo decisionale automatizzato relativo alle persone fisiche)
- **Fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore,** in caso di violazione delle seguenti disposizioni concernenti**:**
  - **i principi di base del trattamento** applicabili al trattamento di dati personali (ad esempio, di "liceità, correttezza e trasparenza"), a norma degli articoli 5, 6, comprese le condizioni relative al **consenso**, articoli 7 (Condizioni per il consenso) e 9 (Trattamento di categorie particolari di dati personali);
  - **i diritti degli interessati** a norma degli articoli da 12 a 22;
  - **i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale** a norma degli articoli da 44 a 49;
  - **qualsiasi obbligo ai sensi delle legislazioni degli Stati membri**
  - **l'inosservanza di un ordine, di una limitazione** provvisoria o definitiva di trattamento.

NOTA BENE. La normativa italiana dispone (Art. 166 del Codice Privacy)i «Criteri di applicazione delle sanzioni amministrative pecuniarie e procedimento per l'adozione dei provvedimenti correttivi e sanzionatori».

DATA PROTECTION - RESPONSABILITA' E SANZIONI

Sanzioni penali

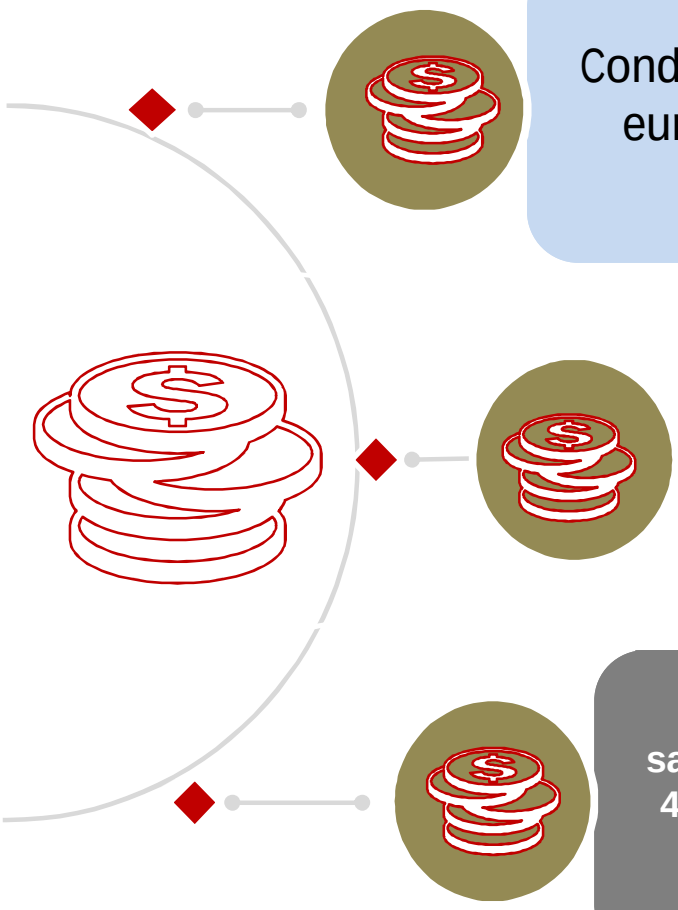
Sono previste sanzioni amministrative pecuniarie e penali.
Si precisa che le sanzioni penali sono state definite e comminate dall'ordinamento nazionale con D.Lgs. n.101/2018.

Illeciti penali.
Adeguamento delle disposizioni penali in coerenza con il GDPR.
Nuove fattispecie di reato.
Quadro sanzionatorio.

- **Art. 167 Trattamento illecito dei dati** (sanzione reclusione da 6 mesi a 1 e 6 mesi)
- **Art. 167 - bis Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala** (sanzione reclusione da 1 a 6 anni)
- **Art. 167 - ter Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala**
- **Art. 168 Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante**
- **Art. 169 Misure di sicurezza - abrogato**
- **Art. 170 Inosservanza di provvedimenti del Garante** (sanzione reclusione da 3 mesi a 2 anni)
- **Art. 171 Violazione delle disposizioni in materia di controllo a distanza e indagini sulle opinioni dei lavoratori**
- **Art. 172 Pene accessorie** (in caso di condanna pubblicazione della sentenza)**.**

GDPR: COMMINATE SANZIONI DAI GARANTI EUROPEI

Infrazioni e sanzioni



Garante francese vs Google

Condannata Google ad una sanzione da 50 milioni di euro per violazione del GDPR, con riferimento al sistema Android per dispositivi mobili.

Garante italiano vs Medico

Stabilito la sanzione di €. 16.000 ad un medico per trattamento illecito di dati personali. Punita la condotta del professionista consistente nell'aver utilizzato gli indirizzi di circa 3.500 ex-pazienti per inviare lettere a sostegno di un candidato alle elezioni politiche, senza che gli interessati avessero espresso specifico consenso.

Garante portoghese vs Ospedale

sanzionata una struttura ospedaliera per un importo di 400 mila euro. Accertato un accesso indiscriminato e ingiustificato di quasi seicento dipendenti ai dati sanitari dei pazienti.

THANK **YOU** FOR YOUR ATTENTION

LEONARDO
CYBER SECURITY