GDPR:
Privacy & Realtà Socio-sanitarie obblighi di conformità & opportunità di miglioramento

MEPAIE 2018 – Cremona 19 ottobre 2018

net 4 market

GDPR: Privacy & realtà socio-sanitarie

MEPAIE 2018

Agenda

1. **Regolamento Privacy UE**:
   tempistiche e principali novità
2. **Modello Organizzativo Privacy**:
   come e perché
3. **L'implementazione nel socio-sanitario**:
   specificità
4. **Q&A**

GDPR:
Privacy & Realtà Socio-sanitarie regolamento privacy GDPR

MEPAIE 2018 – Cremona 19 ottobre 2018

DI COSA SI TRATTA?

Il GDPR, General Data Protection Regulation **UE 2016/679**, è il nuovo Regolamento emanato dalla Commissione Europea nel 2016 atto a **garantire la protezione e la libera circolazione dei dati all'interno dell'Unione**.

QUANDO?

Il GDPR è entrato in vigore il 24 maggio 2016 ed è diventato definitivamente applicabile in via diretta in tutti gli Stati membri a partire dal

25 maggio 2018

NOVITA'?

In data 4 settembre 2018 è stato pubblicato il DLGS 101/2018 di armonizzazione al GDPR: la parte generale del Codice Privacy italiano risulta sostituita quasi integralmente dalle disposizioni del Regolamento, sicché le norme su principi, basi giuridiche del trattamento, informativa e consenso previgenti sono abrogate e sostituite da quelle europee.

PRINCIPALI NOVITA' GDPR

La privacy diventa "BY-DESIGN"&"BY-DEFAULT"

BY DESIGN (Art. 25 Reg. UE 679/2016)

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche….

le organizzazioni che trattano dati personali dovranno determinare il livello adeguato di protezione da applicare ai dati nonché modellare tutti i processi che implicano un trattamento di dati in modo che fin dall'origine siano idonei a attuare in modo efficace i principi di protezione dei dati.

PRINCIPALI NOVITA' GDPR

BY DEFAULT (Art. 25 par. 2 Reg. UE 679/2016)

La tutela della protezione del dato deve diventare l'impostazione predefinita.

Il Titolare del trattamento deve adottare misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specificità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità.

Con l'impostazione predefinita si deve forzare il sistema per inserire più dati di quelli necessari per la singola finalità o per inserire dati diversi; così come si deve forzare il sistema per un trattamento diverso per qualità e quantità rispetto a quello predeterminato e coerente con le finalità; inoltre si deve forzare il sistema per conservare per un periodo eccedente quello preimpostato.

PRINCIPALI NOVITA' GDPR

Inoltre, sempre, per impostazione predefinita non deve consentirsi l'accesso di dati personali a un numero indefinite di persone fisiche senza l'intervento della persona fisica.
Questo significa avere individuato i soggetti assegnatari dei poteri di accesso e che l'accesso sia sempre selezionato con l'intervento di una persona fisica.
Non si deve lasciare una persona in balia di sistemi di raccolta automatizzata dei dati altrui: l'accesso deve essere curato da una persona fisica identificata o identificabile.
Il principio della protezione dei dati di default deve essere preso in considerazione anche nell'ambito degli appalti pubblici.

PRINCIPALI NOVITA' GDPR

Sanzioni

- fino a 10 000 000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore – per le violazioni, tranne…
- fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore – per specifiche violazioni quali:
  - Violazioni dei diritti dei soggetti interessati
  - Violazioni dei principi fondamentali (base legale trattamento, consenso, trattamento dati sensibili)
  - Violazione disciplina in materi di trasferimento dati fuori dall'UE

PRINCIPALI NOVITA' GDPR

Modalità di ricorso per i soggetti interessati

- Diritto di proporre reclamo all'autorità di controllo per violazione al Reg. UE
- Diritto a un ricorso giurisdizionale effettivo nei confronti:
  - dell'autorità di controllo e/o nei confronti del titolare o del responsabile del trattamento
- Diritto di ottenere il risarcimento del danno materiale e immateriale
  - titolare e responsabile del trattamento sono responsabili in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato
- Class actions

PRINCIPALI NOVITA' GDPR

Principio di «Accountability» (Responsabilizzazione)

Il titolare del trattamento è competente per il rispetto di tutti i principi applicabili al trattamento di dati personali ed è in grado di comprovarlo («responsabilizzazione»).

Per affrontare il nuovo

Regolamento occorre un

Modello Organizzativo Privacy

net4market

GDPR:
Privacy & Realtà Socio-sanitarie modello organizzazione privacy

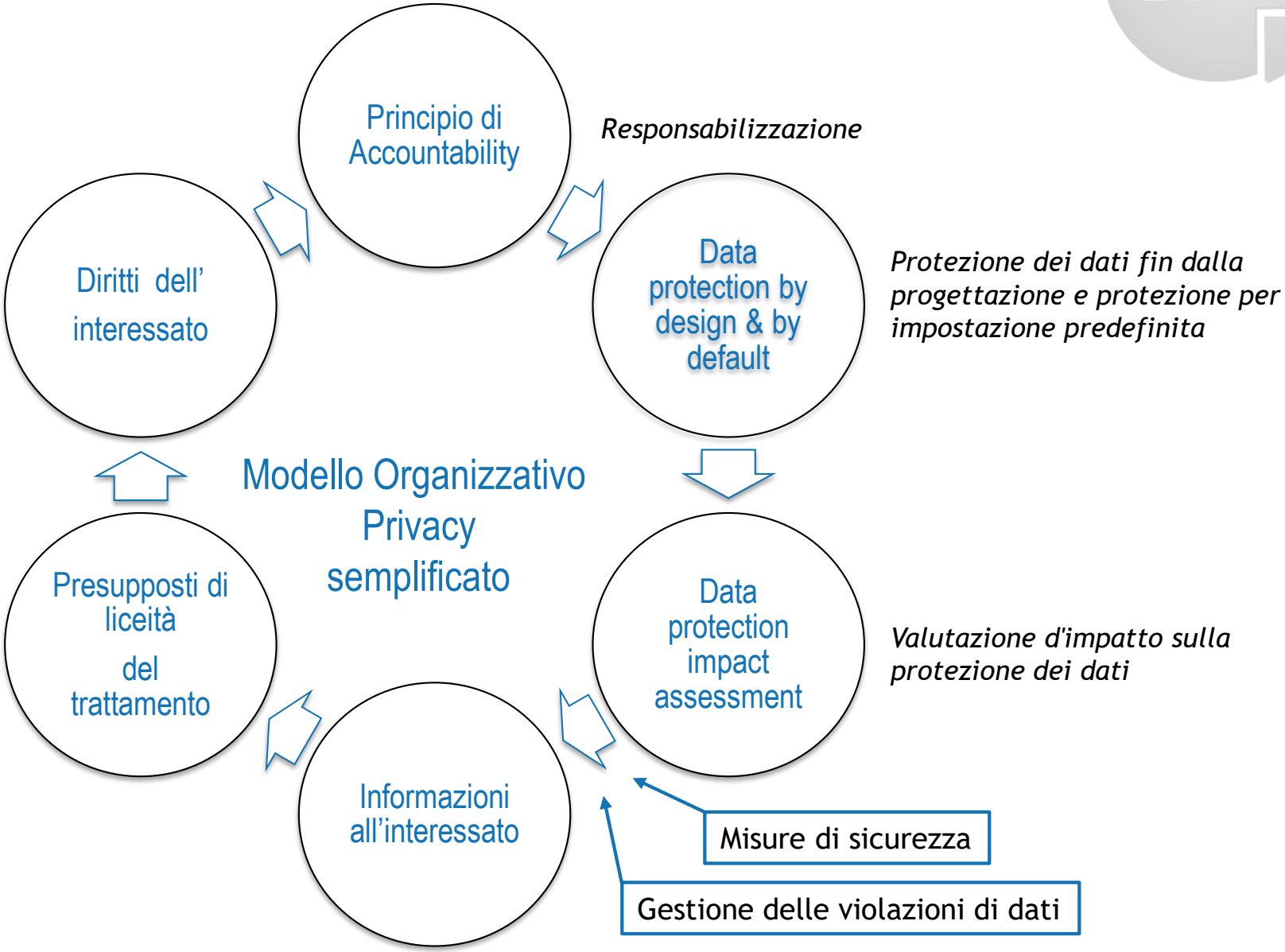
MEPAIE 2018 – Cremona 19 ottobre 2018

net 4 market

GDPR: Privacy & realtà socio-sanitarie

MEPAIE 2018

Necessità di un Modello Organizzativo Privacy …e dunque di un DPO (Responsabile della protezione dei dati)



net 4 market

GAP ANALISYS

La Gap Analysis è finalizzata all'individuazione delle possibili azioni correttive ex Reg. 679/2016 con riferimento al sistema privacy adottato nell'organizzazione.
Il Titolare la utilizza, allo scopo di prepararsi consapevolmente – anche in termini di valutazione del potenziale rischio sanzionatorio connesso all'inadempimento – all'approccio richiesto dalla normativa.
Il risultato deve essere un Report pratico e dettagliato in cui indicare:

- trattamento censito & obblighi,
- adempimento/inadempimento,
- livello di priorità (secondo criteri di rischio-sanzione),
- azione raccomandata.

Questo documento costituirà l'indispensabile strumento di orientamento per i passi di compliance privacy successivi.

net4market

AUDIT TECNOLOGICO

Audit tecnologico sulle misure di sicurezza alla luce della nuova disciplina: una valutazione generale di appropriatezza del modello di data security adottato nel perimetro del Titolare o Responsabile del trattamento.

Non ci sono più «liste della spesa» come l'Allegato B al Codice. Ci si basa su standard internazionali e checklist create ad hoc per l'Azienda.

Indispensabile il coinvolgimento di ingegneri informatici ed esperti di cybersecurity.

DATA PROTECTION OFFICER

Organizzazione del nuovo Data Protection Office(r) aziendale/dell'ente, anche esternalizzato. Si tratta di un team con competenze privacy e di IT security ("Data Protection Office") a supporto dell'operatività quotidiana della nuova figura di Responsabile della protezione dei dati personali, Data Protection Officer, (obbligatoria per chi faccia monitoraggio o tratti dati sensibili/giudiziari su larga scala e per tutti gli enti pubblici).

Designazione del Data Protection Officer che, supportato dal team di cui sopra, svolgerà in maniera proattiva e il più possibile autonoma le necessarie attività privacy per conto dell'azienda/ente.

DATA PROTECTION IMPACT ASSESSMENT

Esecuzione delle Valutazioni d'impatto sulla protezione dei dati per i trattamenti di dati che presentano rischi specifici per i diritti e le libertà delle persone fisiche, da operarsi dopo avere individuato tali trattamenti in fase di due diligence/gap analysis. Tale analisi può essere svolta anche a mezzo dell'adozione di sistemi software di analisi dei rischi privacy (possibilmente combinati con ISO 27001).

INFORMATIVE & CONSENSI

Revisione dei testi delle informative e dei consensi per il trattamento di dati personali, on line e off line, rendendoli già compatibili con i requisiti di cui al Reg. 679/2016.

Revisione dei testi degli incarichi, delle nomine e dei data processing agreements necessari per i soggetti che trattano dati personali, per renderli già conformi ai requisiti previsti dal Reg. 679/2016.

DOCUMENTAZIONE

Impostazione e redazione delle ulteriori nuove documentazioni obbligatorie, con armonizzazione delle vecchie documentazioni presenti nella struttura del Titolare/Responsabile del trattamento e loro trasformazione nei Registri di cui ai nuovi artt. 30 e ss. del Reg. 679/2016.

La realizzazione e successiva tenuta dei registri obbligatori possono essere svolte anche attraverso un software di gestione documentale privacy, disegnato in ossequio ai requisiti di cui al Reg. 679/2016.

DATA BREACH

Data Breach (Notification/Communication) Management (Detection e Gestione della violazione dei dati personali e relativa notifica all'Autorità e comunicazione agli interessati).

Predisposizione di una dettagliata procedura per gestire le eventuali violazioni dei dati personali al fine di individuarne prontamente le cause, mitigarne gli effetti, valutare la necessità di notifica all'Autorità e di comunicazione agli interessati nonché svolgere correttamente tali adempimenti.

PROCEDURE

Predisposizione di procedure per facilitare i diritti dell'interessato (ad es. nel caso di diritto alla portabilità ex art. 20.1 e del diritto all'oblio ex art. 17.2).

Diversi diritti sono già presenti dai tempi del Codice della Privacy (196/2003), ma altri sono nuovi o delineati in maniera innovativa.

Nuovi tempi di riscontro: 30 gg + 30 gg

FORMAZIONE

Formazione degli incaricati sulla nuova disciplina privacy europea, ex Reg. 679/2016.

Formazione d'aula per soggetti apicali e dirigenti.

Formazione on the job per incaricati «sensibili».

Formazione a distanza on line per popolazioni aziendali vaste.

MIX TRA NORME & CODICI DEONTOLOGICI

Corretta integrazione fra adempimenti settoriali (ancora di competenza nazionale, es. privacy e Jobs Act, informazioni commerciali, ecc.) e nuova compliance generale europea.
I provvedimenti generali settoriali del Garante restano validi e applicabili, in tutte le parti compatibili con il GDPR (es. Codici deontologici A5/A7), in attesa della loro riedizione com eprevisto dal DLGS 101/2018.

Attenzione alle sanzioni: per talune norme nazionali si applica comunque l'art. 83 GDPR fino al 4% del fatturato mondiale annuo dell'esercizio precedente.

SICUREZZA TECNICA & ORGANIZZATIVA

Realizzazione di un Piano di Sicurezza dei Dati che garantisca un livello di sicurezza adeguato al rischio, avendo la capacità di:

- cifrare, pseudonimizzare o anonimizzare i dati;
- assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Si tratta di realizzare un Piano continuativo di prevenzione e reazione.

GDPR:
Privacy & Realtà Socio-sanitarie
l'implementazione nel socio-sanitario

MEPAIE 2018 – Cremona 19 ottobre 2018

GDPR «considerando n.10» – RINVIO AGLI STATI MEMBRI

Per precisarne le norme, anche con riguardo al trattamento di categorie particolari di dati personali («dati sensibili»).

Per stabilire le condizioni per specifiche situazioni di trattamento, anche determinando con maggiore precisione le condizioni alle quali il trattamento di dati personali è lecito.

GDPR «considerando n.35» – NOZIONE DATI SANITARI

Nei dati personali relativi alla salute dovrebbero rientrare tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso.

GDPR «considerando n.35» – CASISTICHE DATI SANITARI

- informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria
- un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari;
- le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici;
- qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale, ad esempio, un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro.

GDPR «considerando n.51» – DEROGHE AI DIVIETO DI TRATTAMENTO

- consenso esplicito dell'interessato
- in relazione a esigenze specifiche,
- trattamento è eseguito nel corso di legittime attività di talune associazioni o fondazioni il cui scopo sia permettere l'esercizio delle libertà fondamentali.

GDPR «considerando n.54» – CONSENSO AL TRATTAMENTO

Il trattamento di categorie particolari di dati personali può essere necessario per motivi di interesse pubblico nei settori della sanità pubblica, senza il consenso dell'interessato. Tale trattamento dovrebbe essere soggetto a misure appropriate e specifiche a tutela dei diritti e delle libertà delle persone fisiche

GDPR «considerando n.54» – NOZIONE SANITA' PUBBLICA

Tutti gli elementi relativi alla salute, ossia lo stato di salute, morbilità e disabilità incluse, i determinanti aventi un effetto su tale stato di salute, le necessità in materia di assistenza sanitaria, le risorse destinate all'assistenza sanitaria, la prestazione di assistenza sanitaria e l'accesso universale a essa, la spesa sanitaria e il relativo finanziamento e le cause di mortalità. Il trattamento dei dati relativi alla salute effettuato per motivi di interesse pubblico non dovrebbe comportare il trattamento dei dati personali per altre finalità da parte di terzi, quali datori di lavoro, compagnie di assicurazione e istituti di credito.

GDPR «considerando n.63» - DIRITTI DEGLI INTERESSATI & CARTELLE SANITARIE

Un interessato dovrebbe avere il diritto di accedere ai dati personali raccolti che la riguardano e di esercitare tale diritto facilmente e a intervalli ragionevoli, per essere consapevole del trattamento e verificarne la liceità. Ciò include il diritto di accedere ai dati relativi alla salute, ad esempio le cartelle mediche contenenti informazioni quali diagnosi, risultati di esami, pareri di medici curanti o eventuali terapie o interventi praticati.

GDPR «Art. 9» - TRATTAMENTO CATEGORIE DATI PARTICOLARI

- «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

- «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

GDPR «Art. 4» - DEFINIZIONI

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

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.

GDPR: Privacy & realtà socio-sanitarie

MEPAIE 2018

Ridefinizione dei rapporti tra i soggetti

Controllo delle misure di sicurezza informatiche

SOGGETTI COINVOLTI NEL TRATTAMENTO

- Contitolari (art. 26 Reg. UE 2016/679)
- Responsabili (art. 28 co. 3 Reg. UE 2016/679)
- Sub Responsabili

RAPPORTI TRA SOGGETTI COINVOLTI NELLA SANITA'

Titolari del trattamento dei dati nel Servizio Sanitario Regionale:

- Regione di pertinenza;
- Aziende Sanitarie;
- Strutture sanitarie e socio-sanitarie del SSR;
- Medici di medicina generale e i pediatri di libera scelta.

Si dovrebbe prevedere una clausola che regolamenta i rapporti tra di loro, secondo la quale i Titolari del trattamento si impegnano a formare adeguatamente il personale coinvolto anche al fine di rendere più efficace il rapporto con gli interessati.

RAPPORTI TRA SOGGETTI COINVOLTI NELLA SANITA'

Responsabili del trattamento nel Servizio Sanitario Regionale:

- Società in house della Regione di pertinenza;
- Soggetti che eseguono i progetti gestiti dalle Società in house;
- Altri soggetti designati dalla Regione;
- Soggetti che operano nell'interesse delle Aziende Sanitarie e delle strutture sanitarie e sociosanitarie del SSR e degli esercenti professioni sanitarie.

ACCORDI INTERNI TRA CONTITOLARI

Determinazione delle proprie responsabilità per il rispetto del norme sul trattamento ed in particolare:

- esercizio dei diritti dell'interessato;
- rispettive funzioni di comunicazione delle informazioni;
- designare un punto di contatto per gli interessati.

Definizione dei rispettivi ruoli e i rapporti con gli interessati L'accordo deve essere messo a disposizione dell'interessato.

Indipendentemente dalle disposizioni dell'accordo, l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento.

ART. 26 CONTITOLARI DEL TRATTAMENTO

Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento.

Essi determinano, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione di cui agli articoli 13 e 14, a meno che le rispettive responsabilità siano determinate dal diritto (Unione o Stato membro) cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati.

ART. 26 CONTITOLARI DEL TRATTAMENTO

L'accordo citato riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

Indipendentemente dalle disposizioni dell'accordo di cui sopra, l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento

RAPPORTI TRA TITOLARE & RESPONSABILE

Deve essere regolamentato con esplicitazione di:

- materia disciplinata
- durata del trattamento
- natura e finalità del trattamento
- tipo di dati personali
- categorie di interessati
- obblighi e i diritti del titolare del trattamento

Si vedano le Linee guida pubblicati delle autorità per la protezione dei dati, che discriminano i rapporto tra i due soggetti (Cfr: Francia; Spagna; UK).

RAPPORTI TRA TITOLARE & RESPONSABILE

Notifica delle violazioni di dati personali

Il responsabile del trattamento deve comunicare al titolare del trattamento le violazioni di dati personali nel momento in cui vengano a conoscenza, fornendo gli elementi necessari per valutare se tale violazione derivino rischi per i diritti e le libertà degli interessati, al fine di adempiere quanto disposto dall'artt. 33 e 34 del Regolamento (UE) 2016/679.

REGISTRO DEI TRATTAMENTI

Il Documento Registro delle Attività di Trattamento (art. 30 del GDPR), con tutti i suoi allegati, ha lo scopo di elencare i trattamenti di dati e le misure di sicurezza implementate per far fronte ai rischi individuati.

Per la redazione si fa riferimento al Regolamento Europeo 2016/679 ed ai provvedimenti generali o linee guida emanate dal garante della privacy.

Si tiene conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, individuando e descrivendo le misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento.

Dette misure devono essere riesaminate e aggiornate qualora necessario.

ESEMPI DI TRATTAMENTI IN R.S.A.

Nome del trattamento	**Trattamento obbligatorio dei dati dei lavoratori**
Contitolari del Trattamento	**(Studio paghe)** **(Servizio di medicina del lavoro)**
Responsabile del trattamento esterno	**(amministratore sistema informatico)**
Responsabile del trattamento interno	**Direzione Amministrativa - sanitaria**
Art. 30 b): Descrizione delle Finalità perseguite	Adempimenti legati all'osservanza di specifici obblighi di legge. Elaborazione e trasmissione cedolini paga. Assolvimento degli obblighi contributivi assicurativi e previdenziali. Effettuazione di corsi di formazione. Indicazione dei nominativi su documenti o atti emessi dalla Società in ottemperanza di obblighi di legge o per esigenze imprescindibili ai fini dello svolgimento del servizio. Adempimenti legati all'osservanza di leggi riguardanti la sicurezza sul lavoro, sorveglianza sanitaria ex D.lgs. 81/08. Gestione e organizzazione del servizio specifico. Comunicazioni ad eventuali organi di controllo ispettivi. Analisi statistica interna. Invio newsletter. Eventuale contenzioso. Eventuali richieste di pignoramenti presso terzi. Eventuali provvedimenti disciplinari. Relazioni sindacali. Nomine RSA e RSU.

ESEMPI DI TRATTAMENTI IN R.S.A.

<table>
<tr><td>Art. 30 c): Descrizione delle categorie di dati personali</td><td colspan="2">La gestione di tutte le attività e le pratiche dei dipendenti o assimilabili (tirocinanti, collaboratori, …), nonché il trattamento di dati anagrafici, presenze, pagamenti al personale, dossier dipendenti, assunzioni, cessazioni, denunce di infortunio, idoneità al lavoro, verbali riunioni sindacali, buste paga, 770 viene effettuata direttamente dall’ente gestore
I dati dei dipendenti sono trattati in forma cartacea ed archiviati nell'ufficio personale
Le buste paga sono elaborate da XXX. Le ore lavorate dal personale presso la RSA vengono registrate tramite cartellino manuale
Il personale dipendente è soggetto a visita medica da parte dell’ente gestore, e conseguentemente è nominato un medico competente. il quale consegna tutto la pratica in via cartacea.</td></tr>
<tr><td></td><td>Dati personali</td><td>SI</td></tr>
<tr><td></td><td>Dati relativi alla salute</td><td>SI</td></tr>
<tr><td></td><td>Dati genetici</td><td>NO</td></tr>
<tr><td></td><td>Dati biometrici</td><td>NO</td></tr>
<tr><td></td><td>Altri dati particolari</td><td>SI</td></tr>
<tr><td></td><td>Dati giudiziari</td><td>SI</td></tr>
</table>

ESEMPI DI TRATTAMENTI IN R.S.A.

Art. 30 d): Categorie di destinatari a cui i dati vengono comunicati:	Soggetti privati; Soggetti pubblici; Amministrazioni dello Stato; Amministrazioni regionali; Enti locali (comuni e province); Autorità giudiziaria; Organismi sindacali o patronali; Organismi paritetici in materia di lavoro; Banche; Intermediari finanziari, Consulenti per la sicurezza nei luoghi di lavoro; Consulente del Lavoro; eventuali altri entri preposti.	
Art. 30 e): Paesi terzi verso cui sono trasferiti i dati o organizzazione internazionale	**Nome del paese**	Nessuno
	Nome dell'organizzazione	//
	Documentazione garanzie appropriate	//
Art. 30 f): Termini ultimi previsti per la cancellazione	Termini di legge per la conservazione dei dati dei dipendenti.	
Art. 30 g) Descrizione generale delle misure di sicurezza tecniche ed organizzative	Appositi armadi chiusi o locali chiusi a chiave quando non presidiati. Struttura informatica aziendale che comprende sicuramente: presenza antivirus, firewall, backup, aggiornamento software e manutenzione hardware. Procedura operative - Continuità assistenziale eventi tecnologici.	

ESEMPI DI TRATTAMENTI IN R.S.A.

Art. 32 paragrafo 1 – Misure di sicurezza applicate	
a) la pseudonimizzazione e la cifratura dei dati personali;	NO
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;	SI
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;	Non necessario
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.	Verifiche sicurezza informatica fatte da amministratore di sistema

ESEMPI DI TRATTAMENTI IN R.S.A.

- Trattamento dati dei Tirocinanti, Stagisti, servizio civile, alternanza scuola lavoro, volontari
- Trattamento obbligatorio dei dati del personale della cooperativa (per i servizi socio-sanitari)
- Trattamento dati anagrafici e sanitari del possibile ospite/utente che vuole usufruire di un servizio ed essere inserito in lista d'attesa e dati anagrafici del parente di riferimento o tutore legale
- Trattamento dati anagrafici degli ospiti di struttura e dei parenti di riferimento o tutori legali e loro recapiti
- Trattamento dati sanitari degli ospiti di struttura
- Trattamento dati aziende fornitrici e loro referenti
- Trattamento dei dati delle telecamere in struttura, etc.…

ANALISI DEL RISCHIO

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mette in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

ANALISI DEL RISCHIO

Nel valutare l'adeguato livello di sicurezza, si deve tener conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
L'organizzazione per adempiere a quanto previsto dal Regolamento e dal principio di responsabilizzazione (accountability), deve quindi effettuare un'analisi dei rischi relativi ai trattamenti svolti ed individuato le misure tecniche ed organizzative per minimizzare i rischi stessi.

L'entità del rischio è rappresentata come prodotto della gravità del Danno potenziale (D) per la probabilità (P) che quel rischio si verifichi:
(R=PxD)

ESEMPIO DI ANALISI DEL RISCHIO IN R.S.A.

R8 – Rischi relativi alle banche dati digitali.		
Possibilità non riuscire a ripristinare tempestivamente i dati del FSE.		
VALUTAZIONE DEL RISCHIO PRIMA DELLE MISURE		
P	**D**	**R**
3	4	12
VALUTAZIONE DEL RISCHIO DOPO L'INTRODUZIONE DELLE MISURE		
P	**D**	**R**
1	4	4

Procedure correlate:

- La terapia è sempre recuperabile tramite mail
- Backup dei dati
- Gruppo di continuità per il server
- Procedura operative - Continuità assistenziale eventi tecnologici
- Manutenzione periodica degli apparati hardware e loro eventuale sostituzione ai primi cenni di deterioramento

Periodicità backup:	**Giornaliero**
Altri controlli	**Controllo costante dei sistemi da parte dell'amministratore del sistema informatico**

ESEMPIO DI ANALISI DEL RISCHIO IN R.S.A.

A fronte dell'analisi dei rischi sono state implementate le seguenti procedure organizzative, già richiamate all'interno della valutazione:

- Procedura operative - Continuità assistenziale eventi tecnologici
- Consegna informativa e raccolta consenso

CERTIFICAZIONI ART.25

La certificazione ISO 27001 (sistema di gestione della sicurezza delle informazioni) rappresenta un esempio di best practice.

Non copre direttamente alcuni requisiti previsti dal Regolamento Privacy (quali il diritto ad essere informati; il diritto di far eliminare i propri dati; la portabilità dei dati), ma allo stesso tempo identifica i dati personali come asset di sicurezza informativa e fornisce i mezzi per garantire questa protezione.

GDPR:
Privacy & Realtà Socio-sanitarie
il metodo IPQ

MEPAIE 2018 – Cremona 19 ottobre 2018

3 PASSI:

1. AUDIT
2. ATTUAZIONE

PIANO D'INTERVENTO

3. COMPLIANCE E

MANTENIMENTO

1° PASSO: AUDIT

Attività iniziale di ricerca delle informazioni, di analisi dei rischi, di definizione dei rimedi, del piano formativo e di sensibilizzazione del personale.

Uno dei risultati sarà il piano "d'intervento" con indicate tutte **le implementazioni necessarie** alla messa a norma dell'attività, dando risalto agli interventi di maggiore priorità.

2° PASSO: ATTUAZIONE PIANO DI INTERVENTO

- Aree di intervento su titolare, responsabile, DPO
- Adeguamenti necessari per il rispetto della normativa (informative differenziate, consensi, policy, ecc.)
- Garantire esercizio dei diritti degli interessati (clienti, dipendenti, fornitori)
- Garantire Cancellazione, Limitazione, Portabilità

3° PASSO: COMPLIANCE E MANTENIMENTO

- Informativa privacy, policy sui cookies, moduli consenso, accordi trasferimento anche infragruppo, policy sicurezza, policy conservazione dei documenti, moduli richiesta di accesso da parte degli interessati, accordi con DPO
- Formazione
- Verifiche periodiche su adeguatezza e stato dell'arte

DOMANDE E RISPOSTE

GDPR:
Privacy & Realtà Socio-sanitarie obblighi di conformità & opportunità di miglioramento

MEPAIE 2018 – Cremona 19 ottobre 2018