USLUmbria2
Servizio Sanitario Regionale

La gestione della «privacy» nell'azienda Usl Umbria 2

Il trattamento dei dati personali alla luce degli aggiornamenti normativi.

Avv. Alessandro Frillici - Terni il 8 marzo 2019 – Foligno 22 marzo 2019

Normativa di riferimento

USL Umbria 2
Servizio Sanitario Regionale

- **Codice della Privacy** – Decreto Legislativo 196/2003

(Modificato dal 19 settembre 2018)

- **D.Lgs. 101/2018**

(Norma di raccordo)

- **Regolamento Europeo** 679/2016 - GDPR

(applicabile dal 24 maggio 2018)

Note metodologiche

In questa esposizione è utilizzato questo sistema di notazione per i riferimenti normativi:

R = Regolamento Europeo 679/2016

C = Codice Privacy – D.Lgs 196/2003

D = Decreto Legislativo 101/2018

Es. "*R.2.1*" indica l'art. 2 GDPR paragrafo 1

Approccio alla analisi

Esame tridimensionale delle norme (cosa, come, chi)

1.I dati – cosa ?

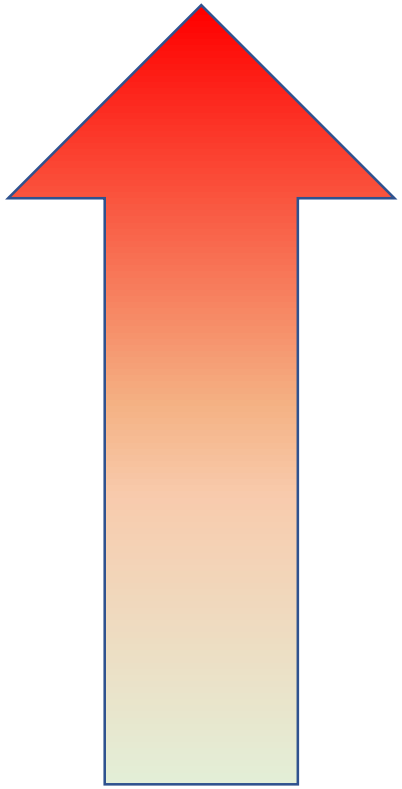
2.Le operazioni di trattamento – come?

3.I soggetti – chi?

Classificazione dei dati

Il Regolamento ripropone una classificazione dei dati sostanzialmente identica a quella del Codice, ovvero in base alla **potenzialità lesiva** dell'informazione rispetto ai diritti e le libertà delle persone fisiche.

Dati Genetici	**5**
Dati Giudiziali	**4**
Categorie Particolari	**3**
Dati Personali Comuni	**2**
Dati Anonimi	**1**



Natura dei dati – Cosa?

- **Dati anonimi** – informazioni non riconducibili a persone fisiche.

- **Dati personali** – qualsiasi informazione che possa essere collegata, direttamente o indirettamente, ad una persona fisica *R4 n.2*.

- **Dati particolari** (i vecchi dati sensibili) sono i dati personali che rivelano: l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i 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 *R9.1*. QUESTI DATI NON POSSONO ESSERE TRATTATI IN ASSENZA DELLE DEROGHE DI R9.2.

Specifiche categorie di dati

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 *R4 n.13*.

Specifiche categorie di dati

Dati biometrici: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici *R4 n.14*.

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 *R4 n.15*.

Dati giudiziali

Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire **soltanto sotto il controllo dell'autorità pubblica** o se il trattamento **è autorizzato dal diritto** dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati *R10*.

C2-octies elenca alcuni casi in cui il trattamento è consentito.

Operazioni di trattamento – Come?

Per trattamento si intende qualsiasi operazione compiuta sui dati personali:

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 *R4 n.2*.

Soggetti – Chi?

- **Interessato** – la persona della quale sono trattati i dati personali (tutti noi).
- **Titolare** – il soggetto che assume le decisioni riguardo le finalità e le modalità del trattamento (L'Azienda) *R4 n.7*.
- **Delegato del titolare** – il soggetto che rappresenta il titolare quando è persona giuridica (La Presidente).
- **Designato** – il soggetto interno cui il titolare delega compiti per il trattamento (P.es. Responsabili di posizioni organizzative) *C2-quaterdecies*.
- **Responsabile** – il soggetto esterno che svolge attività di trattamento per il titolare (fornitori di servizi) *R4 n.8*.
- **Autorizzati** – i soggetti che trattano i dati (tutti voi) *R29; C2-quaterdecies.2*.

Soggetti – Chi?

- **Responsabile della protezione dei dati** (DPO) – il soggetto garante del corretto trattamento (il sottoscritto) *R37*.

- **Terzo** - la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo **che non sia** l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile *R4 n.10*.

- **Destinatario** - la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo **che riceve comunicazione** di dati personali, che si tratti o meno di terzi. Tuttavia, **le autorità pubbliche** che possono ricevere comunicazione di dati personali **nell'ambito di una specifica indagine** conformemente al diritto dell'Unione o degli Stati membri **non sono considerate destinatari**; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento *R4 n.11*.

USLUmbria2
Servizio Sanitario Regionale

COMPITI E RESPONSABILITA' PRIVACY

CATEGORIA	COMPITI E RESPONSABILITÀ
Delegato del titolare	A questa posizione spetta la rappresentanza del titolare del trattamento, essa, ove non abbia delegato a designati: - delega i compiti e le responsabilità per i trattamenti dei dati personali; - nomina i designati del trattamento; - sottoscrive contratti, atti, dichiarazioni, notifiche inerenti al trattamento di dati personali; - sottoscrive il documento di conformità; - sottoscrive le notifiche e le comunicazioni per le violazioni dei dati personali; - interloquisce con le Autorità di controllo; - interloquisce con il Responsabile per la Protezione dei Dati; - sottoscrive le politiche approvate - formalizza gli obiettivi e le politiche per la protezione dei dati personali definiti dal CD.

	- assicura la soddisfazione dei diritti degli interessati.
Responsabile della Protezione dei Dati	Adempie i compiti previsti dall'art. 39 del Regolamento.
Designati dal titolare	Queste posizioni, nei limiti delle proprie competenze lavorative e della autorità che rivestono, oltre agli eventuali ulteriori compiti loro affidati dal titolare: - autorizzano, dirigono e controllano coloro che trattano i dati personali; - definiscono i profili di autorizzazione degli autorizzati; - collaborano con il Privacy Manager e con il Responsabile della Protezione dei Dati; - curano il rispetto delle disposizioni ricevute dal titolare; - curano il rispetto della vigente normativa, segnalando al Privacy Manager o al Responsabile della Protezione dei Dati eventuali scorrettezze; - fungono da referenti nei confronti dei fornitori responsabili del trattamento; - si assicurano che siano date agli interessati le informazioni ex artt. 13 e 14 del Regolamento; - si assicurano che i consensi siano raccolti conformemente al Regolamento; - vigilano il rispetto delle istruzioni da parte degli autorizzati; - si assicurano che siano applicate le misure di sicurezza richieste dal Privacy Manager; - riferiscono senza indugio e tempestivamente ogni violazione di dati personali di cui vengono a conoscenza; - si assicurano che le richieste di esercizio dei diritti da parte degli interessati siano trasmesse al Privacy Manager.
Responsabili del trattamento	Queste posizioni, nei limiti del contratto di loro competenza, rispettano scrupolosamente le specifiche clausole del contratto di servizio del responsabile del trattamento o dell'addendum/allegato contrattuale corrispondente secondo quanto prescritto dall'art. 28 del regolamento e dalle specifiche istruzioni fornite dal titolare.
Autorizzati al trattamento	Queste posizioni trattano i dati personali nella responsabilità del titolare attenendosi alle istruzioni ricevute, nei limiti dei profili di autorizzazione assegnati, esclusivamente per l'adempimento di mansioni ad essi affidate.

I contitolari

Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento *R26.1.*

Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato *R26.2.*

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 *R26.3.*

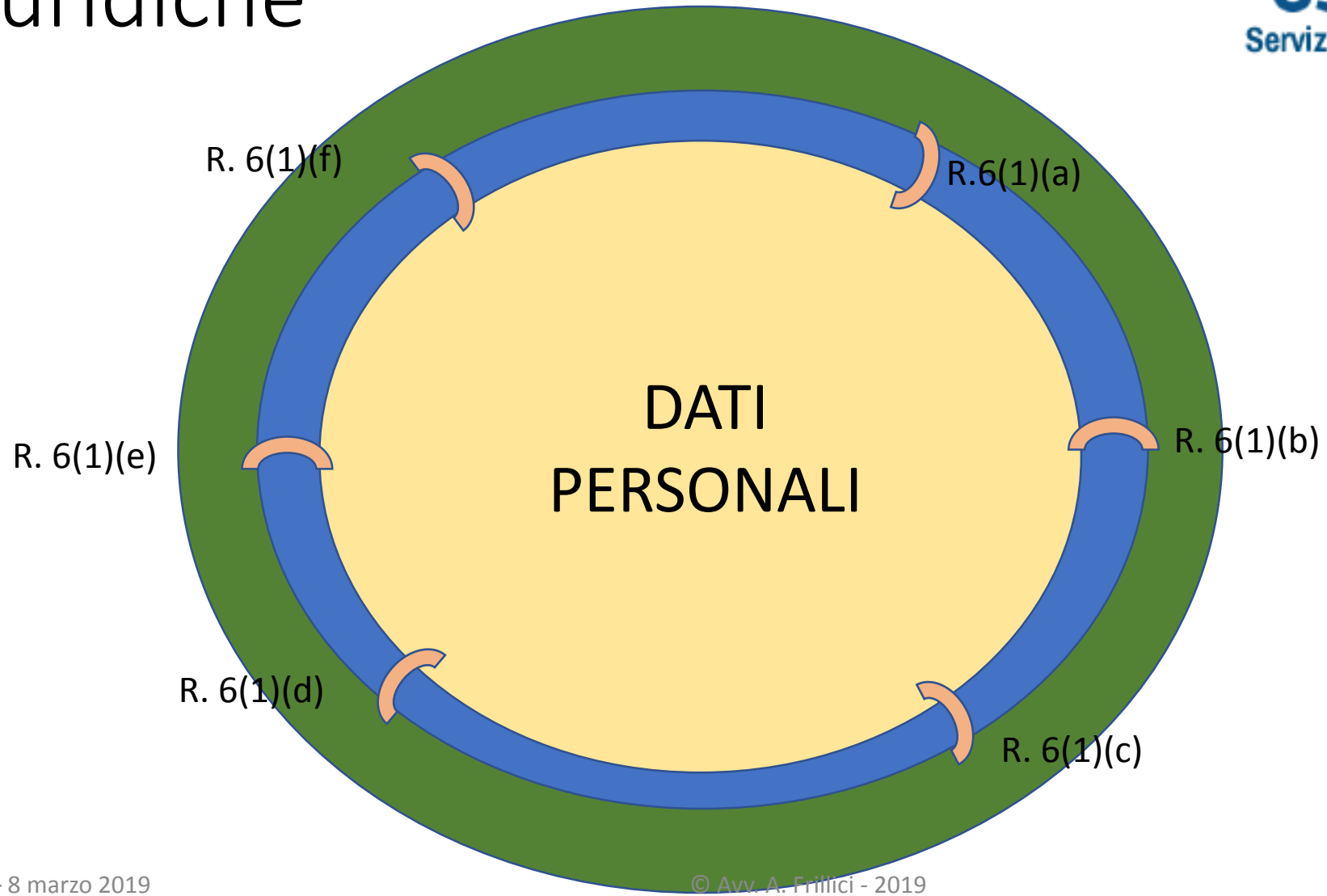
Inutilizzabilità dei dati

I dati personali trattati **in violazione della disciplina rilevante** in materia di trattamento dei dati personali **non possono essere utilizzati** *C2-decies*.

Principi applicabili al trattamento di dati personali *R5*

- Liceità, correttezza e trasparenza;
- limitazione della finalità;
- minimizzazione dei dati;
- esattezza;
- limitazione della conservazione;
- integrità e riservatezza;
- responsabilizzazione.

Liceità del trattamento – basi giuridiche



Le basi giuridiche

Ogni trattamento deve fondarsi su una delle basi giuridiche previste da R6.

Le basi giuridiche sono condizioni espressamente previste dal GDPR.

Esse sono:

a) l'interessato ha espresso **il consenso** al trattamento dei propri dati personali per una o più specifiche finalità;

b) il trattamento è necessario all'esecuzione di un **contratto** di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per adempiere un **obbligo legale** al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la **salvaguardia degli interessi vitali** dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un **compito di interesse pubblico** o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il perseguimento del **legittimo interesse del titolare** del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Nelle informative sono sempre indicate le basi giuridiche, l'assenza di una base giuridica determina l'**illiceità** del trattamento.

Le basi giuridiche

I trattamenti della AUSL Umbria2 usano tutte le basi giuridiche:

a) – consenso – in tutti i casi in cui non sussiste una base giuridica p.es. progetti di ricerca farmacologica.

b) – **contratto** – ad es. per erogare un servizio.

c) - **obbligo legale** – ad es. per la fatturazione;

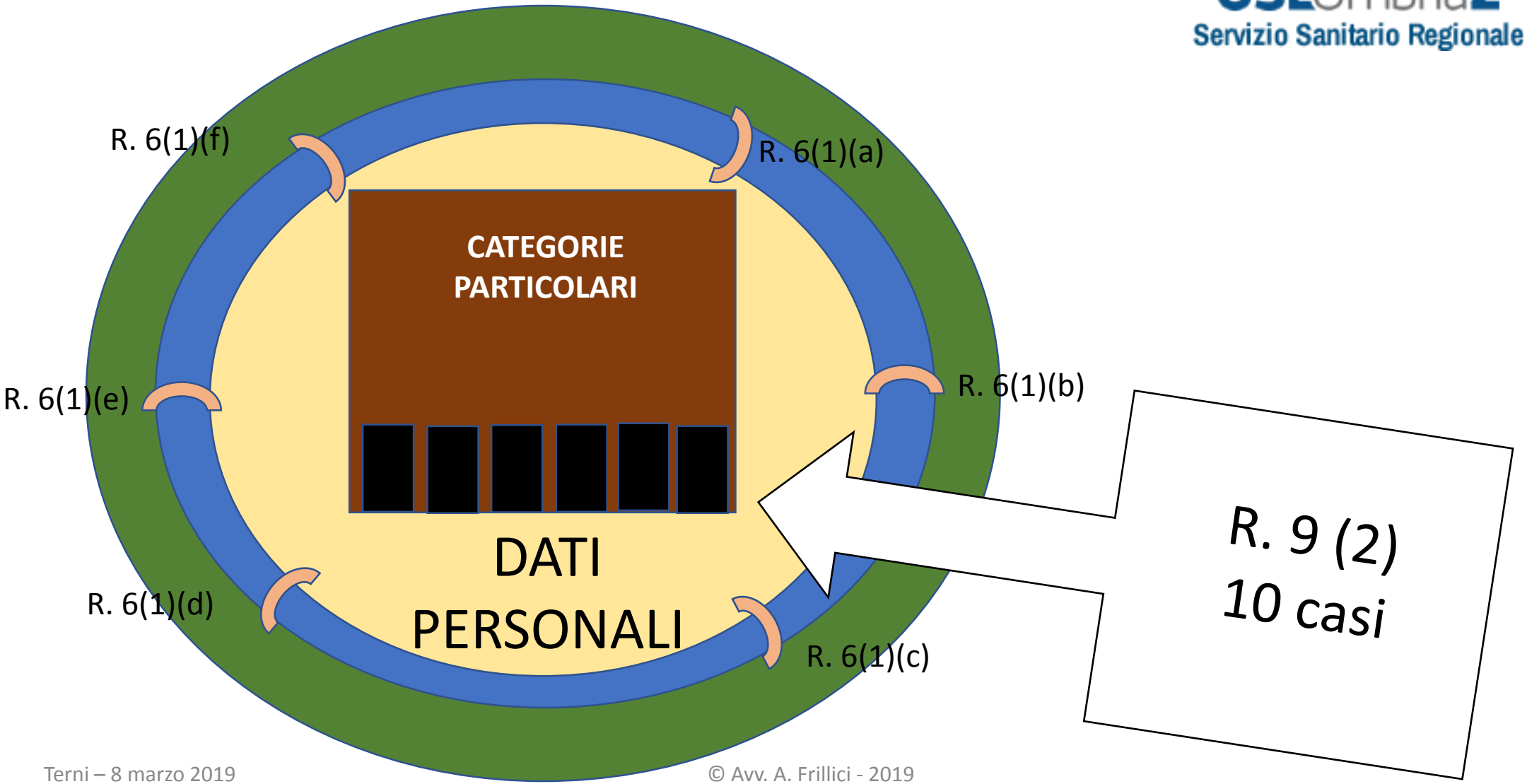
d) - **salvaguardia degli interessi vitali** – in caso di emergenza;

e) - **compito di interesse pubblico** – per le attività in accreditamento;

f) - **legittimo interesse del titolare** – p.es. per la protezione dei beni e delle persone - videosorveglianza.

NB. Il consenso è una base giuridica residuale, deve essere richiesto solo se non c'è alcuna altra base.

Liceità del trattamento – Deroghe



Deroghe al divieto per i dati particolari *R9.2* applicabili alla AUSL Umbria 2

a) l'interessato ha prestato il proprio **consenso esplicito** al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone la non utilizzabilità;

b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di **diritto del lavoro e della sicurezza sociale e protezione sociale**, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;

c) il trattamento è necessario per tutelare un **interesse vitale dell'interessato** o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;

f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;

Specifiche condizioni in ambito sanitario C75

Il trattamento dei dati personali effettuato per **finalità di tutela della salute e incolumità fisica dell'interessato o di terzi o della collettività** deve essere effettuato ai sensi dell'articolo 9, paragrafi 2, **lettere h) ed i)**, e 3 del regolamento, dell'articolo **2-septies del presente codice**, nonchè nel rispetto delle specifiche disposizioni di settore.

Deroghe al divieto per i dati particolari *R9.2* applicabili a la AUSL Umbria 2

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 servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità.

Tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale *R9.3*.

g) il trattamento è necessario per **motivi di interesse pubblico rilevante** sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;

i) il trattamento è necessario per **motivi di interesse pubblico nel settore della sanità pubblica**, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;

j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di **ricerca scientifica** o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Il trattamento di dati particolari per motivi di interesse pubblico rilevante *C2-sexies*

In relazione alla base giuridica di R9.2.g) si considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono **compiti di interesse pubblico** o connessi all'esercizio di pubblici poteri :

s) attività **socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci**;

t) **attività amministrative e certificatorie correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale**, ivi incluse quelle correlate ai trapianti d'organo e di tessuti nonché alle trasfusioni di sangue umano;

u) 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**, protezione civile, salvaguardia della vita e incolumità fisica;

Il trattamento di dati particolari per motivi di interesse pubblico rilevante *C2-sexies*

In relazione alla base giuridica di R9.2.g) si considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono **compiti di interesse pubblico** o connessi all'esercizio di pubblici poteri :

v) **programmazione, gestione, controllo e valutazione dell'assistenza sanitaria**, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale;

z) **Vigilanza sulle sperimentazioni**, farmacovigilanza, autorizzazione all'immissione in commercio e all'importazione di medicinali e di altri prodotti di rilevanza sanitaria;

aa) tutela sociale della maternità ed interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili;

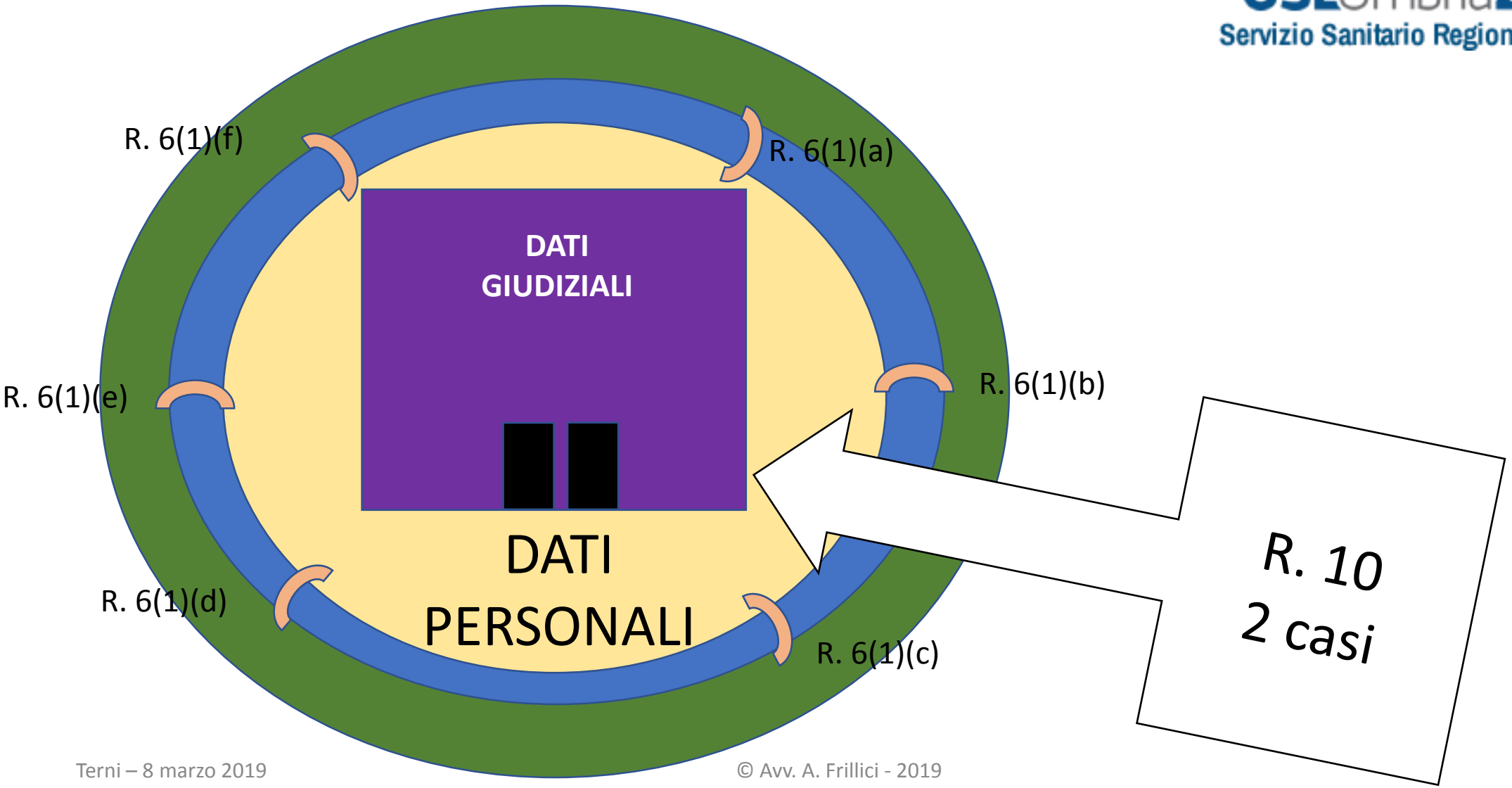
Il trattamento di dati particolari per motivi di interesse pubblico rilevante *C2-sexies*

In relazione alla base giuridica di R9.2.g) si considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono **compiti di interesse pubblico** o connessi all'esercizio di pubblici poteri :

bb) **istruzione e formazione** in ambito scolastico, professionale, superiore o universitario;

dd) **instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo**, anche non retribuito o onorario, e di altre forme di impiego, **materia sindacale**, occupazione e collocamento obbligatorio, **previdenza e assistenza**, tutela delle minoranze e pari opportunità nell'ambito dei rapporti di lavoro, **adempimento degli obblighi retributivi, fiscali e contabili**, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della **responsabilità civile, disciplinare e contabile, attività ispettiva**.

Liceità del trattamento – Deroghe



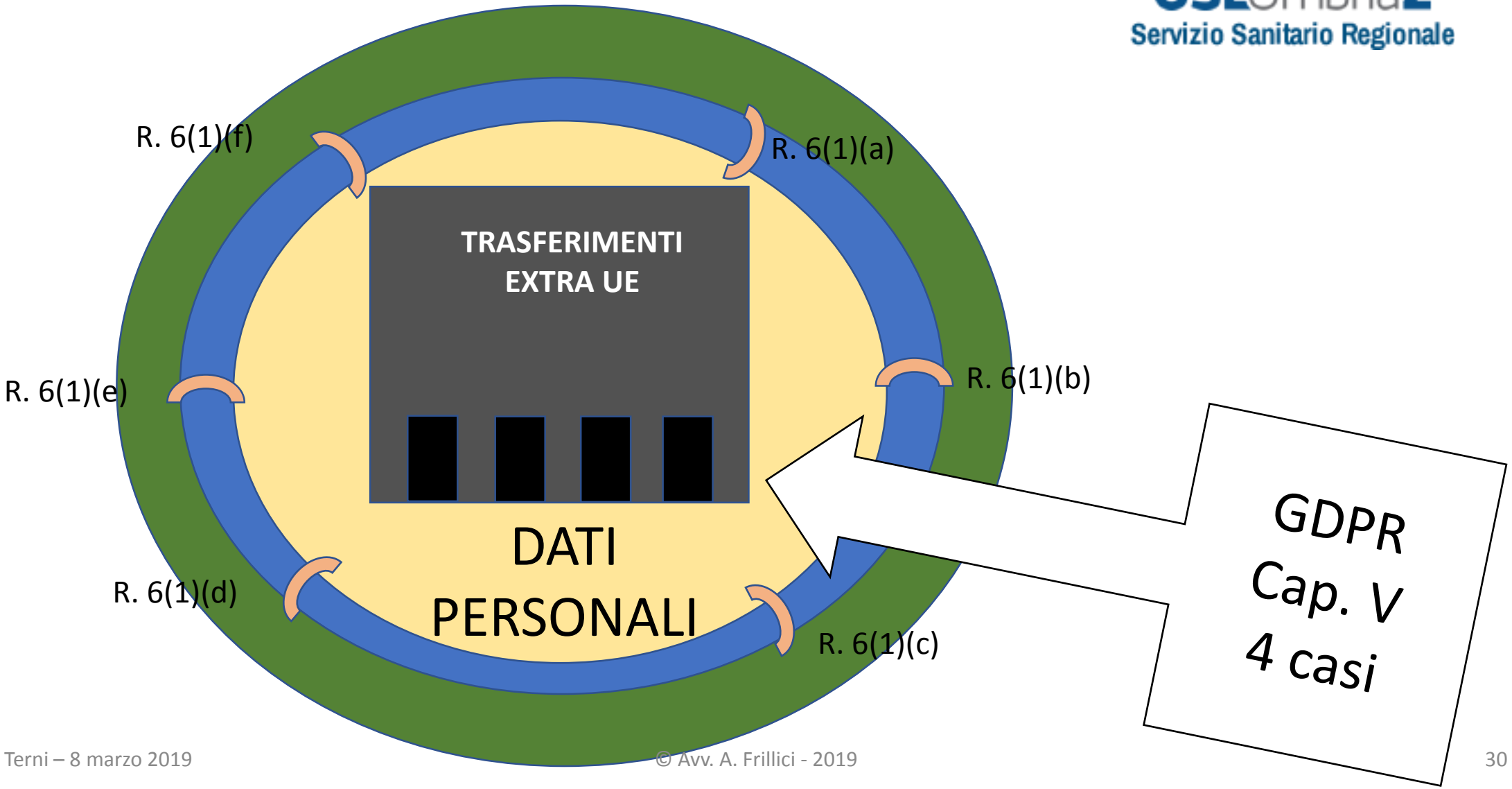
Dati giudiziali

Il trattamento dei dati personali relativi alle **condanne penali e ai reati o a connesse misure di sicurezza** sulla base dell'articolo 6, paragrafo 1, deve avvenire **soltanto:**

1. sotto il controllo dell'autorità pubblica;
2. se il trattamento è **autorizzato** dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.

Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.

Liceità del trattamento – Deroghe



Trasferimenti extra UE

R.44 **Qualunque trasferimento di dati personali** oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, ha luogo **soltanto** se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di cui al presente capo, fatte salve le altre disposizioni del presente regolamento. Tutte le disposizioni del presente capo sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal presente regolamento non sia pregiudicato.

Trasferimenti extra UE

1. Sulla base di una decisione di adeguatezza R.45.
2. Trasferimento soggetto a garanzie adeguate R.46
   a. Strumento giuridicamente vincolante tra P.A.
   b. Norme Vincolanti d'Impresa R.47
   c. Clausole tipo
   d. Codice di condotta
   e. Meccanismo di certificazione
3. Deroghe
   a. Esplicito consenso dell'interessato
   b. Contratto tra titolare e interessato
   c. Contratto a favore interessato
   d. Importanti motivi di interesse pubblico
   e. Accertare, esercitare, difendere un diritto in sede giudiziaria
   f. Interessi vitali
   g. Registro pubblico
4. Trasferimenti eccezionali e limitati

Le basi giuridiche nell'informativa

FINALITÀ *(Perchè trattiamo i suoi dati)*	**BASE GIURIDICA** *(Sulla base di quale disposizione di legge li trattiamo.)*	**CONSEGUENZE IN CASO DI RIFIUTO AL TRATTAMENTO** *(Cosa accade se lei rifiuta di conferire i dati personali e/o di autorizzare il trattamento)*
Tutelare la sua salute con finalità di prevenzione, diagnosi, assistenza sanitaria, terapia sanitaria, riabilitazione.	Art. 9 par. 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 servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità.	Non occorre il consenso, tuttavia se lei rifiuta di conferire i suoi dati personali non potremo svolgere le attività connesse a questa finalità, salvo che il trattamento sia necessario per tutelare un interesse vitale di un'altra persona fisica, ovvero che il trattamento sia necessario per motivi di interesse pubblico nel settore della sanità pubblica.
Per svolgere gli adempimenti amministrativi, contabili e fiscali relativi alle prestazioni di cui alla superiore finalità.	Limitatamente ai dati che non appartengono a categorie particolari (p.es. dati sulla salute). Art. 6 par. 1 lett. b) "il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso". Art. 6 par. 1 lett. c) "il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento".	Non occorre il consenso, tuttavia se lei rifiuta di conferire i suoi dati personali non potremo svolgere le attività connesse a questa finalità, salvo che il trattamento sia necessario per tutelare un interesse vitale di un'altra persona fisica, ovvero che il trattamento sia necessario per motivi di interesse pubblico nel settore della sanità pubblica.
Per rilasciare certificazioni relative al suo stato di salute.	Art. 9 par. 2 lett. a) "l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche".	Nel caso in cui lei non presti il suo consenso non potremo rilasciare le certificazioni.

Il consenso oggi

Salvo pochi casi particolari, generalmente, il consenso non è più richiesto (a maggior motivo quando si parla di dati particolari perché esso è una deroga al divieto generale).

Qualora il trattamento sia basato sul consenso, il titolare del trattamento **deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso** al trattamento dei propri dati personali *R7.1*.

Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente **distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro** *R7.2*.

L'interessato ha il diritto di **revocare il proprio consenso** in qualsiasi momento *R7.3*.

I diritti dell'interessato

Il GDPR dedica l'intero capo III ai diritti dell'interessato.

Primo fra tutti le informazioni (si tratta delle vecchie informative).

Attenzione, con il calo di importanza del consenso, l'informativa assume particolare valore.

Diritto di essere informato

Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli R13 se i dati sono raccolti direttamente dall'interessato

R14 in caso contrario. [*R12.1]*

La AUSL Umbria 2 ha predisposto specifica documentazione che garantisce il rispetto delle prescrizioni del GDPR.

SI RACCOMANDA DI UTILIZZARE ESCLUSIVAMENTE I MODELLI APPROVATI.

Una informativa inidonea può comportare la illiceità dell'intero trattamento ed esporre l'ente a sanzioni fino a 10 milioni.

Modalità particolari C77

Le strutture pubbliche e private, che erogano prestazioni sanitarie e socio-sanitarie possono avvalersi delle modalità

particolari di cui all'articolo 78 in riferimento ad una **pluralità di prestazioni erogate anche da distinti reparti ed unità della stessa struttura o di sue articolazioni ospedaliere o territoriali** specificamente identificate R79.

Le informazioni possono essere fornite **per il complessivo trattamento dei dati personali necessario per attività di diagnosi, assistenza e terapia sanitaria**, svolte dalla struttura a tutela della salute o dell'incolumità fisica dell'interessato, su richiesta dello stesso o di cui questi è informato in quanto effettuate nel suo interesse.

Annotazione.

La ricerca

USLUmbria2
Servizio Sanitario Regionale

Tipo di ricerca	Descrizione	Basi e Deroghe
Valutazione della cura*	Studi sull'esito delle cure prestate, risultati raggiunti, effetti non desiderati, ecc…	R.6.1.b + R.9.2.h.
Basata su norme	Ricerca che trova il suo fondamento nell'ordinamento giuridico.	R.6.1.c + R.9.2.J
Pubblico Interesse	Ricerca per finalità di pubblico interesse.	R.6.1.e + R.9.2.g
Standard Qualità - Gravi Minacce	Ricerche necessarie per la protezione da gravi minacce per la salute o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria, dei medicinali e dei dispositivi medici.	R.6.1.e + R.9.2.i
Altri tipi	Ricerche che non rientrano nelle categorie precedenti.	R.6.1.a + R.9.2.a

(*) R5.1.b. - un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali .

La ricerca - Garanzie

R.89.1 Il trattamento a fini di ricerca scientifica è soggetto a **garanzie adeguate per i diritti e le libertà dell'interessato**, in conformità del GDPR. Tali garanzie **assicurano** che siano state predisposte misure tecniche e organizzative, in particolare al fine di garantire il rispetto del principio **della minimizzazione dei dati**. Tali misure possono includere la **pseudonimizzazione**, purché le finalità in questione possano essere conseguite in tal modo. Qualora possano essere conseguite attraverso il trattamento ulteriore che non consenta o non consenta più di identificare l'interessato, tali finalità devono essere conseguite in tal modo.

Ricerca per interesse pubblico

C.2-sexies.1.cc. Riguardo alla deroga prevista da R.9.2.g (trattamenti necessari per motivi di interesse pubblico rilevante) si considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri e precisamente i trattamenti effettuati per fini di ricerca scientifica.

C.99.1. Il trattamento di dati personali a fini di ricerca scientifica può essere effettuato anche **oltre il periodo di tempo necessario per conseguire i diversi scopi per i quali i dati sono stati in precedenza raccolti o trattati**.

Condizioni

Oltre al sussistere delle prescritte basi giuridiche e delle corrispondenti deroghe, occorre:

- C.105.2. I fini di ricerca scientifica devono essere **chiaramente determinati e resi noti all'interessato**.
- C.110.1. Deve essere condotta e resa pubblica una **valutazione d'impatto** ai sensi degli articoli 35 e 36 del Regolamento.

Ricerca medica, biomedica ed epidemiologica C.110.

Il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico non è necessario quando:

- la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea in conformità all'articolo 9, paragrafo 2, lettera j).
- la ricerca rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-bis del decreto legislativo 30 dicembre 1992, n. 50
- a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca.

Modalità di trattamento

C.107.1 Fermo restando quanto previsto dall'articolo 2-sexies e fuori dei casi di particolari indagini di ricerca scientifica previste dalla legge, il consenso dell'interessato al trattamento di dati di cui all'articolo 9 del Regolamento, quando è richiesto, può essere prestato con modalità semplificate, individuate dalle regole deontologiche di cui all'articolo 106 o dalle misure di cui all'articolo 2-septies.

Dispositivi medici

Dispositivo medico (93/42/CE, 2007/47/CE): qualsiasi strumento, apparecchio, impianto, sostanza o altro prodotto, utilizzato da solo o in combinazione, compreso il software informatico impiegato per il corretto funzionamento e destinato ad essere impiegato nell'uomo a scopo di:

- diagnosi, prevenzione, controllo, terapia o attenuazione di una malattia;
- diagnosi, controllo, terapia, attenuazione o compensazione di una ferita o di un handicap;
- studio, sostituzione o modifica dell'anatomia o di un processo fisiologico;
- intervento sul concepimento, la cui azione principale voluta nel o sul corpo umano non sia conseguita con mezzi farmacologici né immunologici né mediante processo metabolico, ma la cui funzione possa essere assistita da tali mezzi.

Le apparecchiature elettromedicali

(CEI 62.5) si intende un sottoinsieme dei Dispositivi Medici che, in accordo a quanto indicato dalla Direttiva 93/42/CEE, rispondono alla seguente definizione: "**Dispositivo medico munito di non più di una connessione ad una particolare sorgente di alimentazione destinato alla diagnosi, al trattamento o alla sorveglianza del paziente e che entra in contatto fisico o elettrico col paziente e/o trasferisce energia verso o dal paziente e/o rileva un determinato trasferimento di energia verso o dal paziente**. Il dispositivo comprende anche quegli accessori, definiti dal costruttore, che sono necessari per permettere l'uso normale del dispositivo". La definizione comprende anche i sistemi elettromedicali, ossia quei sistemi che comprendono apparecchi elettromedicali ed eventualmente anche apparecchi non elettromedicali, interconnessi permanentemente o temporaneamente a scopo diagnostico o di trattamento del paziente.

Criticità

Quando i dispositivi e/o le apparecchiature elettromedicali raccolgono dati personali, occorre tenere conto delle seguenti criticità:

- Responsabilità nel trattamento dei dati - posizioni;
- Attività di manutenzione – accesso alla rete;
- Equilibrio tra misure di sicurezza e «dichiarazioni di conformità» dello strumento;
- Riuso e smaltimento.

Nel rispetto dei principi della privacy by design e by default è necessario che siano coinvolte le funzioni privacy (incluso il DPO) sin dalla fase di selezione del fornitore.

Diritti degli interessati

Le richieste di esercizio dei diritti possono pervenire nei modi più disparati, in tali casi chi riceve la richiesta deve immediatamente darne comunicazione al superiore gerarchico.

La tempestività è cruciale perché entro 30 giorni deve essere data risposta *R12.4.*

E’ importante che le richieste pervengano all’ufficio privacy perché deve essere preliminarmente valutata la legittimità della richiesta, la correttezza e la fondatezza.

Diritti degli interessati

- Diritto alle informazioni - R13 e R14
- Diritto di accesso - R15
- Diritto di rettifica - R16
- Diritto alla cancellazione - R17
- Diritto alla limitazione - R18
- Diritto alla portabilità - R20
- Diritto di opposizione - R21

Limitazione dei diritti degli interessati C2-undecies

I diritti di cui agli articoli da 15 a 22 del Regolamento **non possono essere esercitati** con richiesta al titolare del trattamento ovvero con reclamo ai sensi dell'articolo 77 del Regolamento qualora dall'esercizio di tali diritti possa derivare un **pregiudizio effettivo e concreto**:

e) Allo svolgimento delle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria;

f)alla riservatezza dell'identità del dipendente che segnala ai sensi della legge 30 novembre 2017, n. 179, l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio.

La responsabilità del titolare del trattamento R24 – R25. Privacy by design e by default

Tenuto conto

della **natura**, **dell'ambito di applicazione**, del **contesto** e delle **finalità del trattamento**, nonchè dei **rischi** aventi probabilità e gravità diverse per i diritti e le libertà delle **persone fisiche**, il titolare del trattamento **mette in atto misure tecniche e organizzative adeguate** per **garantire**, ed **essere in grado di dimostrare**, che il trattamento è effettuato conformemente al presente regolamento.

Dette misure sono **riesaminate e aggiornate** qualora necessario.

Sia **al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso** il titolare del trattamento mette in atto misure tecniche e organizzative adeguate volte ad attuare in modo efficace i principi di protezione dei dati e a **integrare nel trattamento le necessarie garanzie** al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per **impostazione predefinita**, solo i dati personali necessari per ogni specifica finalità del trattamento

Il Responsabile del trattamento

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 e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato *R28.1*.

I trattamenti da parte di un responsabile del trattamento **sono disciplinati da un contratto o da altro atto giuridico** a norma del diritto dell'Unione o degli Stati membri, che **vincoli il responsabile del trattamento al titolare del trattamento** e che **stipuli la materia disciplinata e la durata del trattamento**, la **natura** e la **finalità** del trattamento, il **tipo di dati personali** e **le categorie di interessati**, gli **obblighi e i diritti del titolare del trattamento** *R28.3*.

Se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione *R28.10*.

Sicurezza dei dati

Il titolare deve proteggere adeguatamente i dati personali che tratta *R32*.

La AUSL Umbria2 ha elaborato misure di sicurezza per proteggere i dati personali.

E’ dovere di ciascuno rispettare le istruzioni ricevute.

Livelli di sicurezza

USLUmbria2
Servizio Sanitario Regionale

a. LIVELLO 1

CONDIZIONE
Il processo, l'attività, l'operazione di trattamento riguarda dati anonimi e non critici per l'Ente.

IDENTIFICATIVO	DESCRIZIONE	1	2	3	NATURA
M1_01	Sistema di autenticazione per accedere a risorse e sistemi				L
M1_02	Istruzioni per l'uso delle credenziali di autenticazione				O
M1_03	Procedura di accesso forzato al sistema				O
M1_04	Controllo delle credenziali di autenticazione				O
M1_05	Sistema di autorizzazione per accedere a risorse e sistemi				L
M1_06	Profili di autorizzazione				L
M1_07	Controllo dei profili di autorizzazione				O
M1_08	Antivirus aggiornato				L
M1_09	Aggiornamento del Sistema Operativo				L
M1_10	Aggiornamento degli applicativi				O
M1_11	Scrivanie ordinate				O

Violazione di dati

Chiunque viene a conoscenza di un incidente o sospetta un incidente deve riferire **immediatamente** al proprio superiore gerarchico.

Per incidente si intende qualsiasi avvento avverso che può interessare i dati (p.es. furto di un PC).

Violazione di dati personali

La tempestiva comunicazione è importantissima perché, se è probabile che la violazione comporti rischi per i diritti e le libertà delle persone fisiche, **entro 72 ore** deve essere fatta notifica al Garante.

Se poi, i rischi fossero alti, senza indugio, deve esserne data comunicazione agli interessati coinvolti dalla violazione. *R33*

Violazione di dati personali

Spetta all'Ufficio privacy valutare se ricorrono gli estremi per la notifica o meno, come pure se si debba fare comunicazione agli interessati.

Valutazione d’impatto

Quando un tipo di trattamento, allorchè prevede in particolare **l'uso di nuove tecnologie**, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare **un rischio elevato per i diritti e le libertà delle persone fisiche**, il titolare del trattamento effettua, **prima di procedere al trattamento**, una **valutazione dell'impatto** dei trattamenti previsti sulla protezione dei dati personali *R35*.

E’ obbligatoria se c’è:

- una **valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato**, compresa la profilazione, e **sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche**;

- il **trattamento, su larga scala, di categorie particolari di dati personali** di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o

- la **sorveglianza sistematica su larga scala di una zona accessibile al pubblico**.

Valutazione d'impatto

Il Garante Italiano con l'allegato 1 al Provv. 467 del 11/10/2018 n. 467, ha individuato le ulteriori seguenti tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto, tra gli altri, quelli di maggiore interesse:

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

6) Trattamenti non occasionali di dati relativi a **soggetti vulnerabili** (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).

10) Trattamenti di **categorie particolari di dati** ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.

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

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

Valutazione d’impatto

Se ritenete di aver individuato situazioni che richiedono una valutazione d’impatto, comunicatelo all’Ufficio Privacy.

Registro delle attività di trattamento

R.30 Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità.

Spetta a ciascun designato mantenere aggiornato il registro riguardo alle attività di trattamento di dati personali condotte nell'area di propria responsabilità.

Ogni modifica deve essere tempestivamente comunicata all'Ufficio Privacy cui spetta tenere il registro dell'intera azienda.

Il registro aziendale tenuto dall'Ufficio Privacy fa prova verso i terzi.

USLUmbria2
Servizio Sanitario Regionale

USLUmbria2
Servizio Sanitario Regionale

DOCUMENTO DI CONFORMITÀ DEI TRATTAMENTI DEI DATI PERSONALI

REGOLAMENTO EUROPEO 679/2016 - GDPR

DI

AZIENDA UNITÀ SANITARIA LOCALE UMBRIA N. 2

La scheda della attività di trattamento

DOCUMENTO DI CONFORMITA' DEI TRATTAMENTI DEI DATI PERSONALI

POSIZIONE ORGANIZZATIVA	AFFARI LEGALI	DATA	24/05/2018
RESPONSABILE DELLA POSIZIONE ORGANIZZATIVA	Dott. Piero Carsili		
ID PROCESSO	Gestione richieste risarcimento danni		
ID ATTIVITÀ	Gestione richieste risarcimento danni		
RESPONSABILE ATTIVITÀ	Dott. Piero Carsili		
DESCRIZIONE	Attività di gestione dell'istruttoria delle pratiche relative a presunta responsabilità sanitaria, su richiesta del Comitato gestione sinistri e assicurazioni e, più in generale, a tutti gli eventi avversi di interesse.		
FINALITÀ DEL TRATTAMENTO	Gestione delle richieste risarcimento danni		
BASI GIURIDICHE	Art.6 par.1 lett e) GDPR Art.6 par.1 lett c) GDPR Art. 9 par. 2 lett. f) GDPR		
OPERAZIONI DI TRATTAMENTO	Registrazione, uso, consultazione, conservazione, comunicazione		
CATEGORIE DI DATI TRATTATI	Identificativi, anagrafici, mansioni, dati di servizio, dati sanitari dei pazienti, dati assicurativi		
NATURA DEI DATI TRATTATI	Personali, particolari		
CATEGORIE INTERESSATI	Personale sanitario, pazienti, rappresentanti di Enti e Persone Giuridiche		
STRUMENTI DI TRATTAMENTO	Cartacei ed elettronici		
LIVELLO DI SICUREZZA	3		
ARCHIVI ANALOGICI			
CATEGORIA DOCUMENTO	Fascicolo dei dipendenti, registri, cartelle cliniche		
DESCRIZIONE	Si tratta della documentazione necessaria alla gestione delle richieste di risarcimento danni		
DURATA CONSERVAZIONE	Fino alla durata dell'ente		
ARCHIVI INFORMATICI			
ID BANCA DATI			
DESCRIZIONE			
OWNER			
PROCESSI COLLEGATI			
STRUMENTI DI TRATTAMENTO			

Responsabile per la protezione dei dati R37 – R38 – R39

USLUmbria2
Servizio Sanitario Regionale

Il Responsabile per la protezione dei dati (DPO) ha i compiti di:

a) **informare e fornire consulenza** al titolare del trattamento o al responsabile del trattamento nonchè ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonchè da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) **sorvegliare** l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonchè delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

c) fornire, se richiesto, un **parere** in merito alla **valutazione d'impatto** sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;

d) **cooperare** con l'autorità di controllo; e

e) fungere da **punto di contatto** per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Gli interessati **possono contattare** il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento R38.4.

Il responsabile della protezione dei dati **è tenuto al segreto o alla riservatezza** in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri R38.5.

Come contattare il DPO

- Per email - dpo@uslumbria2.it

- Per posta tradizionale – in busta chiusa indirizzata «Al D.P.O. – Riservato» presso la sede di Terni o di Foligno.

- Possono essere richiesti incontri facendone richiesta e concordando con l'ufficio privacy un appuntamento.

Risarcimento dei danni

Chiunque subisca un **danno materiale o immateriale** causato da una violazione del GDPR ha il **diritto di ottenere il risarcimento del danno** dal titolare del trattamento o dal responsabile del trattamento R82.1.

Un **titolare** del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un **responsabile** del trattamento risponde per il danno causato dal trattamento **solo se** non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento R82.2.

Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 **se dimostra che l'evento dannoso non gli è in alcun modo imputabile** R82.3.

Sanzioni amministrative

Le sanzioni pecuniarie sono due.

Il GDPR si limita a definirne il massimo: fino a 10 milioni per le violazioni minori;

fino a 20 milioni per quelle più gravi.

Il penale

Trattamento illecito di dati C167

Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per se' o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2-sexies e 2-octies, o delle misure di garanzia di cui all'articolo 2-septies ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2quinquiesdecies arreca nocumento all'interessato, è punito con la reclusione da uno a tre anni.

Penale privacy

Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala C167-bis.

Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala C167-ter.

Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante C168.

Inosservanza di provvedimenti del Garante C170.

Decalogo

I. Assicurarsi che l'interessato abbia ricevuto l'informativa.

II. Se è previsto il consenso l'interessato deve decidere in completa libertà.

III. Custodire gelosamente ogni informazione che riguarda i pazienti (anche il riferire verbalmente informazioni o usare i social network può costituire violazione).

IV. Non lasciare mai documenti incustoditi nelle aree pubbliche. Se trovate documenti abbandonati raccoglieteli e consegnateli al superiore gerarchico.

V. Rispettare scrupolosamente le istruzioni sui trattamenti.

Decalogo

VI. Riferire immediatamente ogni incidente o sospetto tale.

VII. Riferire immediatamente ogni richiesta di esercizio dei diritti che dovesse pervenire da un interessato.

VIII. Non rivelare ad alcuno la propria password. Compilare la password secondo la complessità richiesta. Avvisare immediatamente se si sospetta che sia stata violata.

IX. Offrire la massima collaborazione alle Autorità ed al personale interno di controllo.

X. In caso di dubbio chiedere sempre al superiore gerarchico.