Linee Guida per la gestione del Registro delle Attività di Trattamento

Versioni del documento

Versione	Data di redazione	Autore	Modifiche
bozza	17/05/2018		

Approvazione documento

Ruolo	Nome	Firma	Data
Redattore			XX/XX/XXXX
Revisore			
Approvatore			

Sommari

Figure

Tabelle

1 Introduzione

Il GDPR ('General Data Protection Regulation') è un Regolamento, steso dalla Commissione Europea e pubblicato sulla "Gazzetta Ufficiale" dell'Unione Europea in data 4 maggio 2016, che ha il fine di armonizzare all'interno dell'UE le norme relative alla gestione dei dati personali.

Il presente documento si inquadra nel contesto degli aspetti inerenti alla gestione del Registro delle Attività di Trattamento, con lo scopo di descrivere le attività necessarie alla sua compilazione e successiva gestione.

1.1 Finalità del documento

IL GDPR introduce la necessità da parte del Titolare del trattamento e, dove applicabile, del proprio rappresentante, di avere un Registro delle Attività di Trattamento (di seguito Registro dei Trattamenti) svolte sotto la propria responsabilità (Art. 30).

Scopo del presente documento è quello di fornire le linee guida per facilitare la redazione e l'aggiornamento del Registro dei Trattamenti, da parte della struttura sanitaria, come richiesto dal Regolamento Europeo.

1.1.1 Documenti di riferimento

Il presente paragrafo contiene la lista dei documenti di riferimento.

[1] Regolamento (UE) 2016/679 (GDPR)
[2] Template del Registro dei Trattamenti (in allegato)

1.2 Glossario

Acronimo/Definizione	Descrizione
GDPR	General Data Protection Regulation
RAT	Registro delle Attività di Trattamento
DPIA	Data Protection Impact Analysis
DPO	Data Processor Officer
RPD	Responsabile della Protezione dei Dati

Tabella 1 – Glossario

2 Registro delle Attività di Trattamento

Il registro dei trattamenti è uno strumento fondamentale non soltanto per disporre di un quadro aggiornato dei trattamenti in essere all'interno di una organizzazione, ma è anche la fonte primaria di riferimento per lo svolgimento delle attività di analisi e valutazione degli impatti sulla privacy e sui rischi di sicurezza delle informazioni trattate.

Secondo il regolamento (Art. 30 par. 1), il Registro delle Attività di Trattamento deve contenere perlomeno le seguenti informazioni:

- Il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
- 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 applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
- Ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- Ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, par 1.

La struttura sanitaria ha scelto di adottare un Registro dei Trattamenti, in formato microsoft excel, che contiene ulteriori informazioni rispetto a quelle minime indicate, evidenziate con una colorazione di sfondo azzurra più scura, ed è strutturato nelle seguenti sezioni:

1. Informazioni generali
2. Registro Trattamenti Titolare
3. Misure di sicurezza
4. Liste

Nei paragrafi successivi vengono fornite le indicazioni per la compilazione dei singoli campi (celle excell) relativi alle suddette sezioni.

2.1 Informazioni Generali

Nella prima sezione sono esplicitate alcune informazioni generali quali:

- **Dati del Titolare**: devono essere indicati i dati identificativi del Titolare (la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali) e i suoi dati di contatto;
- **Dati del Referente** (qualora nominato): devono essere indicati i dati identificativi del Referente (persona fisica nominata dal Titolare con la responsabilità di svolgere i compiti a lui assegnati) e i suoi dati di contatto;
- **Dati del DPO** (qualora nominato): devono essere indicati i dati identificativi del Responsabile della Protezione dei Dati (RPD o DPO) e i suoi dati di contatto;
- **Data di creazione**: deve essere indicata la data di creazione del Registro dei Trattamenti;
- **Data di aggiornamento**: deve essere indicata l'ultima data in cui il Registro dei Trattamenti è stato aggiornato.

Nella Figura 1 sono mostrati i campi della sezione.

Figura 1 - Informazioni Generali

2.2 Registro dei trattamenti

Il registro dei trattamenti è uno degli adempimenti cogenti previsti dal GDPR e deve essere tenuto in forma scritta o anche in formato elettronico e messo a disposizione dell'autorità di controllo qualora richiesto.

Il Registro dei Trattamenti, corretto ed aggiornato nel tempo, costituisce una significativa evidenza della responsabilizzazione del Titolare, e costituisce l'elemento basilare per un approccio razionale ed esaustivo alla gestione della privacy, in quanto fornisce un quadro sinottico dei trattamenti posti in essere dall'organizzazione, da utilizzare come fonte di riferimento per ogni attività di valutazione degli impatti e dei rischi privacy.

Di seguito si riporta una descrizione sulle modalità di compilazione dei campi presenti nella seconda sezione, nella quale vengono esplicitate le informazioni relative a ciascun trattamento:

- Unità organizzativa
- Trattamento
- Finalità del trattamento
- Descrizione Workflow processo
- Base giuridica del trattamento
- Categorie di Interessati
- Categoria di Dati personali
- Descrizione categoria di dati
- Tipologia di dati: Personali, Particolari, Ultra-sensibili, Giudiziari
- Modalità di raccolta dati
- Modalità di gestione dati
- Modalità di archiviazione dati
- Destinatari
- Paese terzo
- Termini di cancellazione
- Misure di sicurezza organizzative
- Misure di sicurezza tecnica
- DB/applicativo e sua allocazione
- Sistema Backup e Restore e allocazione
- Consenso
- Modalità di raccolta Consenso
- Contitolare del trattamento
- Rappresentante del titolare
- Ente terzo/ Responsabile al trattamento
- Necessità DPIA
- Note

2.2.1 Unità organizzativa

In questo campo deve essere inserita l'Unità Organizzativa dell'azienda, il servizio o il Presidio in cui viene svolto il Trattamento. Il campo è a compilazione libera.

2.2.2 Trattamento

Si definisce Trattamento (art. 4) "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".
In questo campo deve essere riportato l'identificativo del Trattamento. Il campo è a compilazione libera e può contenere un identificativo numerico di riferimento piuttosto che un nome che individui in maniera univoca il trattamento stesso.

2.2.3 Finalità del trattamento

In questo campo deve essere inserita una breve descrizione delle finalità del trattamento. Il campo è a compilazione libera ma è possibile far riferimento ad alcuni esempi non esaustivi di finalità riportati in Figura 1Figura 2:

Esempi Finalità
Rilascio esenzione
Assistenza sanitaria
Gestione del personale
Gestione di assicurazione sani

Figura 2 -Esempi di finalità

2.2.4 Descrizione Workflow processo

In questo campo deve essere inserita una breve descrizione del trattamento ed in particolare del processo con cui questo viene gestito. Il campo è a compilazione libera.

2.2.5 Base giuridica del trattamento

In questo campo devono essere riportati i principi di liceità del trattamento come previsto dall'Art. 6 par. 1 del GDPR. Il campo deve essere compilato attraverso la scelta di una voce dal menu a tendina riportato in Figura 3:

Figura 3 - Base giuridica del trattamento

2.2.6 Categorie di Interessati

In questo campo deve essere riportata la categoria di interessati del trattamento. L'interessato è una persona fisica identificata o identificabile, direttamente o indirettamente, con delle informazioni quali il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o con uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. Il campo deve essere compilato attraverso la scelta di una voce dal menu a tendina riportato in Figura 4:

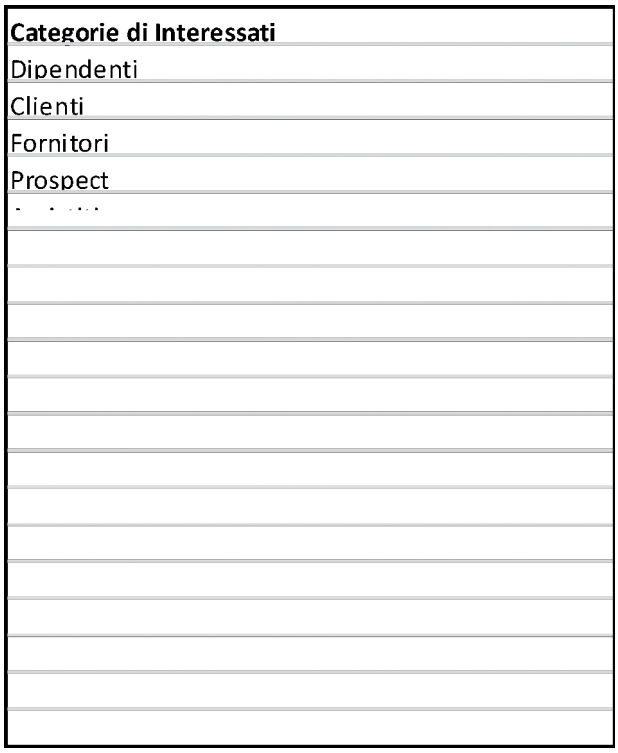

Figura 4 - Categoria di interessati

2.2.7 Categoria di Dati personali

In questo campo deve essere riportata la categoria di dati utilizzata nel trattamento (es. anagrafica, dati sanitari, dati finanziari). Il campo è a compilazione libera.

2.2.8 Descrizione categoria di dati

In questo campo deve essere descritta con maggiore dettaglio la categoria inserita nel campo precedente, indicando i dati personali che la compongono (es. nome, cognome, indirizzo, diagnosi clinica, numero conto corrente). Il campo è a compilazione libera.

2.2.9 Tipologia di dati

I dati personali sono classificati nelle seguenti tipologie:

- **Dati personali**: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, 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 (vedi Art.4 par.1).

- **Dati particolari (o sensibili)**: 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 ultrasensibili**: Dati relativi ad atti di violenza sessuale o di pedofilia, all'infezioni da HIV o all' uso di sostanze stupefacenti, di sostanze psicotrope e di alcool, alle prestazioni erogate alle donne che si sottopongono ad interventi di interruzione volontaria della gravidanza o che decidono di partorire in anonimato e ai servizi offerti dai consultori familiari.

- **Dati giudiziari**: quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato.

Per indicare la tipologia di dati trattati dallo specifico trattamento è necessario apporre una "x" ad uno o più di questi campi.

2.2.10 Modalità di raccolta dati

In questo campo deve essere riportato il formato con il quale vengono raccolti i dati del trattamento, attraverso la scelta di una voce dal menu a tendina riportato in Figura 5:

Modalità di raccolta dati
N/A
Cartaceo
Digitale
Cartaceo e digitale

Figura 5 - Modalità di raccolta dati

2.2.11 Modalità di gestione dati

In questo campo deve essere riportata la modalità con la quale vengono gestiti i dati del trattamento, attraverso la scelta di una voce dal menu a tendina riportato in Figura 6:

Modalità di gestione dati
N/A
Automatizzata
Non automatizzata
Semiautomatizzata

Figura 6 - Modalità di gestione dati

2.2.12 Modalità di archiviazione dati

In questo campo deve essere riportato il formato con il quale vengono archiviati i dati del trattamento, attraverso la scelta di una voce dal menu a tendina riportato in Figura 7:

Modalità di conservazione dat
N/A
Cartaceo
Digitale
Cartaceo e digitale

Figura 7 - Modalità di conservazione dati

2.2.13 Destinatari

Si definisce 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".
In questo campo deve essere riportata la categoria di destinatari a cui i dati personali sono stati o saranno comunicati. Il campo è a compilazione libera ma è possibile far riferimento ad alcuni esempi non esaustivi di finalità riportati in Figura 8:

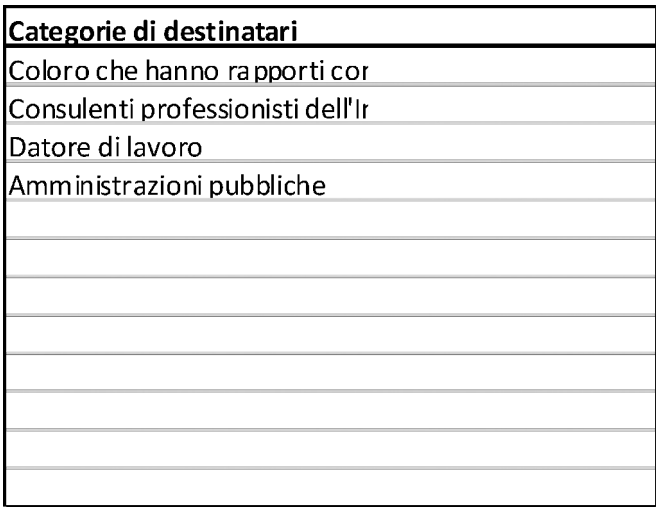

Figura 8 - Esempi di Categorie di destinatari

2.2.14 Paese terzo

In questo campo deve essere dichiarato l'eventuale trasferimento dei dati ad un paese terzo o ad una organizzazione internazionale, attraverso la scelta di una voce dal menu a tendina riportante SI o NO.

2.2.15 Termini di cancellazione

In questo campo devono essere riportati i termini ultimi previsti per la cancellazione dei dati personali trattati. Il periodo di conservazione dei dati deve essere strettamente correlato allo scopo perseguito con il trattamento ovvero deve rispettare i termini di legge qualora esistenti. Il campo è a compilazione libera.

2.2.16 Misure di sicurezza organizzative

In questo campo devono essere riportate, ove possibile, le misure di sicurezza organizzativa adottate a protezione del trattamento. Il campo è a compilazione libera ma possono essere riportati gli identificativi (es. 1a, 1b, 1c) delle misure organizzative presenti nella sezione "Misure di sicurezza", riportate in Figura 9 ovvero far riferimento a piani di sicurezza che le descrivono dettagliatamente:

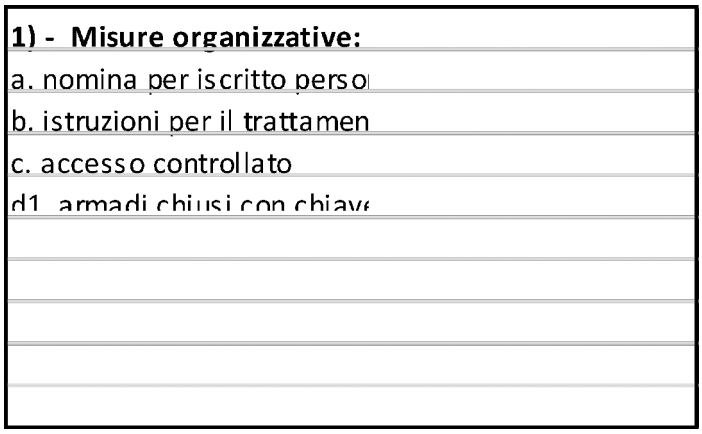

Figura 9 - Misure di sicurezza organizzativa

2.2.17 Misure di sicurezza tecnica

In questo campo devono essere riportate, ove possibile, le misure di sicurezza tecnica adottate a protezione del trattamento. Il campo è a compilazione libera ma possono essere riportati gli identificativi (es. 2a, 2b, 2c) delle misure tecniche presenti nella sezione "Misure di sicurezza", riportate in Figura 10 ovvero far riferimento a piani di sicurezza che le descrivono dettagliatamente:

Figura 10 - Misure di sicurezza tecnica

2.2.18 DB/applicativo e sua allocazione

In questo campo deve essere riportato il nome del data base nel quale i dati relativi al trattamento sono memorizzati, l'applicativo che li elabora e l'allocazione fisica di tali dispositivi. Il campo è a compilazione libera.

2.2.19 Sistema Backup e Restore e allocazione

In questo campo deve essere riportato il nome del supporto di memoria (es. disco, nastro) utilizzato per conservare la copia (backup) dei dati relativi al trattamento, il sistema utilizzato per l'effettuazione del backup e l'allocazione fisica di tali dispositivi. Il campo è a compilazione libera.

2.2.20 Consenso

Si definisce consenso (Art.4): "qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento".
In questo campo devono essere riportate le caratteristiche del consenso, qualora venga raccolto, attraverso la scelta di una voce del menu a tendina riportato in Figura 11:

Consenso
N/A
Comportamentale
Espresso
Per iscritto

Figura 11 - Consenso

2.2.21 Modalità di raccolta Consenso

In questo campo deve essere riportata la modalità di raccolta del consenso (es. all'atto della sottoscrizione di un contratto, all'atto della prima raccolta dei dati) e se disponibile, l'indicazione della data inizio e data fine del consenso stesso. Il campo è a compilazione libera.

2.2.22 Contitolare del trattamento

L'art 26 del GDPR cita: "1. Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, 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 delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti…"

In questo campo devono essere riportati i dati identificativi e di contatto del/i contitolare/i eventualmente presente/i per lo specifico trattamento. Il campo è a compilazione libera.

2.2.23 Rappresentante del titolare

Il GDPR definisce Rappresentante "la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento."
In questo campo devono essere riportati i dati identificativi e di contatto del/i rappresentante/i eventualmente presente/i per lo specifico trattamento. Il campo è a compilazione libera.

2.2.24 Ente terzo/Responsabile al trattamento

Il GDPR definisce Responsabile "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento".
In questo campo devono essere riportati i dati identificativi e di contatto del/i Responsabile/i eventualmente presente/i per lo specifico trattamento o dell'ente terzo, persona fisica o giuridica che tratta dati per contro del titolare del trattamento ma che non viene nominato Responsabile. Il campo è a compilazione libera.

2.2.25 Necessità DPIA

L'Art. 35 cita: "1. Quando un tipo di trattamento, allorché 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. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.
2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.
Qualora si ritenga che il trattamento presenti dei rischi elevati (per esempio perché tratta dati ultra-sensibili), compilare tale campo scegliendo la voce dal menu a tendina riportante SI altrimenti NO.

2.2.26 Note

In questo campo è possibile riportare le eventuali note in riferimento ad uno qualsiasi dei campi precedenti ovvero i riferimenti a documenti che supportano quanto inserito. Il campo è a compilazione libera.

2.3 Misure di sicurezza

L'Art. 32 del GDPR cita: "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 mettono in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio che comprendono, tra le altre, se del caso:

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

In questa sezione è possibile inserire misure di sicurezza organizzative e tecniche che possono essere richiamate attraverso il loro identificativo all'interno della sezione "Registro dei trattamenti del titolare" così come descritto nei par. 2.2.16 e 2.2.17. Nel template sono presenti un set minimo di misure di sicurezza, così come riportato in Figura 12:

Figura 12 – Esempi misure di sicurezza

2.4 Liste

Questa sezione viene utilizzata per l'implementazione dei menu a tendina e per tale ragione può essere nascosta nell'utilizzo corrente del registro dei trattamenti.

3 Allegato 1: Template registro dei trattamenti

Template Registro
dei trattamenti.xlsx