Allegato 1 al decreto del Direttore n. 97 del 7 settembre 2018

"Indicazioni operative per il Registro delle attività di trattamento"

Versione del documento	1.0
Data emissione	23/05/2018
Stato del documento	Definitivo
Nome del file	*"Indicazioni operative per il registro delle attività di trattamento.docx"*

Sommario

1 Contesto di riferimento2

2 PREMESSA5

2.1 Oggetto del documento5

2.2 Ambito di applicazione del documento5

2.3 Validità e Aggiornamento del documento5

2.3.1 Soggetti Approvatori5

2.3.2 Soggetto verificatore6

2.3.3 Versione del documento6

3 QUADRO NORMATIVO7

3.1 Definizioni normative di riferimento7

3.2 Adempimenti prescritti dalla normativa10

3.2.1 Legenda attributi registro14

4 Stato dell'arte del sistema di gestione del registro dei trattamenti16

4.1 Interventi da porre in essere e definizione dell'indice dei Trattamenti17

5 Modalità di intervento/aggiornamento e compilazione del registro trattamenti18

5.1 Definizione di attributi di gestione del software18

5.2 Accesso, compilazione e tempistiche di intervento sul registro trattamenti18

5.3 Tenuta del registro da parte dei soggetti nominati Responsabili20

6 Controlli22

6.1 DPO22

6.2 Soggetti attivi23

7 Aspetti sanzionatori24

7.1 Violazioni24

7.2 Sanzioni24

1 Contesto di riferimento

La presente introduzione è necessaria al fine di inquadrare sotto un profilo contestuale il Regolamento Europeo nr. 679/2016 (General Data Protection Regulation meglio noto come GDPR), entrato in vigore il 24 maggio 2016 ma pienamente applicabile a partire dal 25 maggio 2018, che andrà ad uniformare ed armonizzare le legislazioni dei Paesi Europei con riguardo alla materia di protezione dei dati personali.

L'esigenza di una rivisitazione della normativa in materia di protezione dei dati personali si apprezza in relazione al mutato contesto politico, economico e sociale di riferimento del tutto differente rispetto a quello degli anni 90, periodo nel quale l'impatto e la cultura del dato non era così centrale come invece è oggi; ciò è dato dallo sviluppo repentino delle moderne tecnologie (in primis mobile devices, smartphone, tablet, social network, ecc.; in seconda battuta strumenti IOT (Internet of things), sistemi di Data Analytics e Big Data, Business Intelligence, ecc.) nemmeno immaginabile negli anni che chiudevano il secolo scorso, grazie alle quali è pensabile e apprezzabile anche il valore economico del dato.

Accanto a questa constatazione di tipo "sociologica" va da sé che il programma di integrazione europeo che vede come base di partenza la creazione di un mercato unico europeo, da realizzarsi inizialmente attraverso la libera circolazione di persone, servizi e merci, non possa non tenere in considerazione anche della libera circolazione del "dato personale" così come puntualmente sottolineato dai "considerando" del Regolamento fino anche alla maggiore rilevanza di questa libertà rispetto alla tutela del dato in sé come diritto soggettivo (considerando nr. 4).

A seguito di questa breve introduzione storica/sociologica ed avviando la riflessione sul terreno giuridico, in prima battuta preme precisare che la scelta di tipologia di intervento del legislatore Europeo risulta alquanto significativa nella misura in cui, con la scelta di un Regolamento, non viene lasciata agli Stati membri alcuna possibilità di intervento (se non in termini di adozione di provvedimenti volti ad armonizzare la normativa nazionale) stante la piena applicabilità del Regolamento a dispetto della presenza, come successo invece in passato in materia di protezione di dati personali, di direttiva europea (95/46) che necessitava di un atto di recepimento (Dlgs. 196/2003, meglio noto come codice della privacy).

In riferimento invece ai contenuti della presente legge si sottolinea come l'approccio che propone il Regolamento sia del tutto differente rispetto a quello proposto dal codice privacy nazionale.

Principio fondamentale che impernia l'intera normativa è infatti quello di **accountability** (la capacità di rendere conto delle azioni) il quale illustra, di fatto, una responsabilizzazione dei soggetti coinvolti in materia di protezione di dati personali; questi infatti secondo il dettato normativo non dovranno più

ragionare in termini di mero adempimento alla norma di riferimento, come invece accaduto fino ad oggi con riferimento ai dettami del codice della privacy.

In tal senso il principio di accountability deve essere letto sotto un duplice profilo: esso non solo è il principio che ispira l'adeguamento/l'adempimento degli enti alla normativa europea, ma è anche il punto di partenza per **dimostrare** la compliance (il rispetto, l'aderenza) dell'ente/organizzazione alla norma europea.

Ciò significa che un ente/organizzazione può disattendere una prescrizione del Regolamento, avendo tuttavia cura di indicare in apposito documento le ragioni in forza delle quali si ritiene di non dover seguire il dettato normativo.

Oltre quindi a lasciare uno spazio di intervento ai soggetti Titolari del trattamento in ordine alla scelta di adozione delle novità introdotte dal GDPR, obbligandoli comunque ad una seria riflessione in ordine alle politiche da adottare per essere conformi al Regolamento, si segnalano a titolo esemplificativo alcuni istituti del tutto lontani dalla logica "burocratica" del Codice Privacy.

Si richiama inevitabilmente quindi al processo di istituzione e conservazione del **registro di trattamenti** in capo ai titolari e responsabili del trattamento che consente quindi di avere una chiara panoramica dei trattamenti di dati personali che vengono effettuati all'interno dell'organizzazione che fa per l'appunto capo al titolare o al responsabile; a ciò si aggiunga l'organizzazione del processo che porta il titolare o responsabile del trattamento in contatto con l'autorità garante e con i soggetti interessati in caso di "violazione di dati" nota anche come ***Data Breach***, che come sarà meglio trattato nell'apposito documento non si limita al solo furto di dati.

Ancora, la previsione di una conduzione di **Valutazione di impatto** per quei trattamenti che presentino un rischio elevato per i diritti e le libertà degli interessati.

Sotto il profilo dei soggetti attivi e protagonisti, in questo nuovo quadro, viene introdotta la figura del ***Data Protection Officer – DPO*** (obbligatorio per tutti gli enti pubblici) il quale si andrà a configurare da un lato come consulente per i Titolari e i Responsabili dei trattamenti, attraverso una continua verifica della *compliance* dell'organizzazione/ente rispetto ai dettami del GDPR, ma anche come punto di riferimento per i soggetti interessati rappresentando per questi ultimi il referente dell'organizzazione con il quale interfacciarsi in materia di protezione dei dati personali.

In conclusione, come già emerso dalla disamina condotta, a mutare è l'atteggiamento della normativa rispetto alla tematica della protezione dei dati personali, esso infatti impone una riflessione preventiva rispetto alla materia *de qua*, che porta quindi ad adattare la propria organizzazione in base alle opportunità

che si intendono cogliere, lasciando non solo ampi spazi di autonomia ai soggetti Titolari/Responsabili ma anche abbandonando quell'approccio di mero adempimento richiesto dalla normativa. In sintesi, non è sufficiente avere "le carte a posto".

2 PREMESSA

1.1 Oggetto del documento

L’oggetto del presente documento consiste nella redazione di indicazioni operative che consentono di aver un quadro di insieme per consentire la corretta gestione e conservazione del registro delle attività di trattamento così come richiesto dal GDPR.

I contenuti del registro, come si vedrà meglio in seguito, sono contenuti all’art. 30 del GDPR.

1.2 Ambito di applicazione del documento

Le presenti indicazioni sono destinate alla corretta gestione del registro delle attività di trattamento della Regione Toscana nonché agli enti di diritto pubblico e privato partecipati dalla Regione.

L'onere della tenuta del Registro è a carico del titolare o suo delegato e, se nominato, del responsabile del trattamento. La tenuta del registro è utile per una completa ricognizione e valutazione dei trattamenti svolti e quindi finalizzata anche all'analisi del rischio di tali trattamenti e a una corretta pianificazione degli stessi.

Il registro deve essere tenuto in forma scritta, anche in formato elettronico, e va esibito all'autorità di controllo in caso di verifiche.

1.3 Validità e Aggiornamento del documento

1.1.1 Soggetti Approvatori

Approvatore	Referente e Ruolo	Data

1.1.2 Soggetto verificatore

Verificatore	Referente e Ruolo	Data

1.1.3 Versione del documento

Stato	Versione	Autore	Descrizione	Data

3 QUADRO NORMATIVO

- REGOLAMENTO 2016/679/UE: Articolo 30
- Considerando: C. 82

1.4 Definizioni normative di riferimento

Anonimizzazione: tecnica di trattamento dei dati personali tramite la quale i dati personali non possano più essere attribuiti a un interessato specifico, nemmeno attraverso l'utilizzo di informazioni aggiuntive.

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

Autorità di controllo: è l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51.

Cifratura: tecnica di trattamento dei dati personali tramite la quale i dati personali vengono resi non intellegibili a soggetti non autorizzati ad accedervi.

Consenso dell'interessato: 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;

Contitolare: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, insieme ad altri determina le finalità e i mezzi di trattamento dei dati personali;

Data Breach: è un incidente di sicurezza in cui i dati personali vengono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato o persi accidentalmente.

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;

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;

Dato personale: 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;

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;

DPIA: acronimo di Data Protection Impact Assessment (valutazione di impatto sulla protezione dei dati).

Interessato: persona fisica identificata o identificabile. 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.

Limitazione di trattamento: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

Misure di sicurezza: misure tecniche ed organizzative adeguate per garantire un livello di sicurezza dei dati trattati adeguato al rischio.

Nuovo trattamento: trattamento di dati personali che comporta l'utilizzo di nuove tecnologie o è di nuovo tipo e in relazione al quale il titolare del trattamento non ha ancora effettuato una valutazione d'impatto sulla protezione dei dati, o la valutazione d'impatto sulla protezione dei dati si riveli necessaria alla luce del tempo trascorso dal trattamento iniziale.

Privacy by-design / by-default: l'incorporazione della privacy a partire dalla progettazione di un processo aziendale, con le relative applicazioni informatiche di supporto. La prima introduce la protezione dei dati fin dalla progettazione per caso specifico, la seconda per impostazione predefinita di una pluralità di casi tra loro omogenei.

Profilazione: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

Pseudonimizzazione: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

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 regolamento;

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
Responsabile della Conservazione documentale: si tratta della figura preposta alla gestione e supervisione del processo di conservazione dei documenti (digitali o cartacei).

Security Manager: è la figura preposta alla gestione e supervisione del processo di Security Incident Management.

Sub responsabile: persona fisica o giuridica designata dal responsabile del trattamento previa autorizzazione scritta del titolare del trattamento;

Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il Titolare o suo delegato del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

Titolare del trattamento o suo delegato: 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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

Trattamento: 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;

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

1.5 Adempimenti prescritti dalla normativa

Ai sensi dell'art 30 del GDPR "Registro delle attività di trattamento":

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

a) 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;

b) le finalità del trattamento;

c) una descrizione delle categorie di interessati e delle categorie di dati personali;

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

e) 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;

f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

2. Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:

a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;

b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;

c) 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;

d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

3. I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.

4. Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.

5. Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

Ad ulteriore precisazione della norma si riporta il **considerando 82** del Regolamento.

"Per dimostrare che si conforma al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe tenere un registro delle attività di trattamento effettuate sotto la sua responsabilità. Sarebbe necessario obbligare tutti i titolari del trattamento e i responsabili del trattamento a cooperare con l'autorità di controllo e a mettere, su richiesta, detti registri a sua disposizione affinché possano servire per monitorare detti trattamenti".

Come si evince dalle premesse normative, la tenuta dei registri di trattamento si configura come base necessaria al fine di dimostrare la conformità dei trattamenti ai principi enucleati dal GDPR.

Preme sottolineare come oltre al titolare la norma richiede che anche il responsabile del trattamento sia tenuto alla redazione di un registro dei trattamenti.

Per come si va quindi a configurare, tale strumento di lavoro potrà essere visto sotto un duplice punto di vista: sia come strumento operativo di mappatura dei trattamenti effettuati sia come strumento probatorio che dimostra il pieno adempimento alla normativa.

La norma prevede tuttavia deroghe alla tenuta della documentazione in esame; nel caso in cui l'organizzazione del titolare o del responsabile si sostanziano in realtà con meno di 250 dipendenti non sarà necessaria l'adozione del registro, tuttavia nel caso in cui l'organizzazione al di sotto di tale soglia dimensionale effettui trattamenti che presentino un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale oppure includa il trattamento di dati sensibili o giudiziari, in tal caso è obbligatoria la tenuta dei registri di trattamenti.

La norma indica altresì le informazioni che dovranno confluire nel registro delle attività di trattamento: oltre ai dati di contatto contenuti nella lett. a) art. 30 (titolare, contitolare, rappresentante del titolare e DPO) i dati relativi alle finalità del trattamento, alla descrizione delle categorie di interessati, di dati

personali, di destinatari cui i dati saranno comunicati, tra cui rientrano quelli di paesi terzi od organizzazioni internazionali.

Nonostante i punti b), c) e d) non siano richiamati con riferimento alle indicazioni contenutistiche cui il responsabile è tenuto, è ragionevole pensare che tali informazioni rientrino nelle "categorie dei trattamenti effettuati per conto del titolare del trattamento".

Non può infatti la definizione di trattamento ignorare l'esatto inquadramento delle finalità del trattamento, categorie di interessati, di dati personali e di destinatari cui i dati saranno comunicati.

In ogni caso al responsabile del trattamento non sarà difficile reperire le informazioni di cui alle citate lettere b), c) e d) che saranno invece individuate nell'atto di nomina a responsabile per l'appunto.

Una riflessione analoga si può proporre con riguardo alla lett. f) art. 30 in riferimento ai termini previsti per la cancellazione dei dati, essendo anche questa previsione contenuta nell'atto di nomina a responsabile.

Di medesimo contenuto invece la previsione dell'individuazione dei soggetti di cui alle lettere a), così come di cui all'art. 30 par. 1 lett. e) e paragrafo 2 lett. c).

In entrambe le descrizioni dei registri emerge la presenza della "*descrizione generale delle misure di sicurezza tecniche ed organizzative di cui all'art. 32 paragrafo 1*"; se da un lato all'atto di designazione di responsabile è obbligatorio indicare che il responsabile "*adotti tutte le misure richieste ai sensi dell'art. 32*" è altrettanto vero notare come queste non vengano puntualmente definite nella nomina, con la conseguenza di un margine di operatività in capo al responsabile del trattamento dei dati personali in ordine alle misure da adottare; va da sé in altri termini che essendo in potenza difformi tali misure di sicurezza dovranno necessariamente essere presenti nel registro sia del titolare che del responsabile.

Sulla scorta di quanto affermato in apertura di commento alla norma secondo cui il registro trattamenti, in un'ottica di *accountability*, attesta l'adempimento alla normativa va da sé che la possibilità da parte dell'autorità garante di controllo di richiedere che il registro le venga messo a disposizione conferma quanto appena ribadito; su tale direttrice si muove altresì la tenuta in forma scritta dei registri dei trattamenti, ancora una volta infatti la forma scritta consente di adempiere all'onere della prova nel caso in cui si debba eventualmente accertare una forma qualsiasi di responsabilità in capo a titolare oppure al responsabile.

1.5.1 Legenda attributi registro

La seguente sezione intende fornire una guida per definire le voci presenti nel registro trattamenti che sarà adottato da Regione Toscana nonché dagli enti da questa controllata

INFORMAZIONI GENERALI

Dati generali del trattamento: insieme di informazioni che identificano il trattamento (codice, denominazione, stato, descrizione)

Soggetti: persone fisiche o giuridiche idonee ad individuare i soggetti attivi del trattamento ed i loro dati di riferimento/identificativi (Titolare o suo delegato/riferimento titolare, contitolare/riferimento contitolare)

Struttura del dirigente titolare del trattamento: dati identificativi (nome proponente) della struttura dirigenziale quale punto di riferimento delegato dal titolare (ufficio/settore cui afferisce, direzione generale, direttore generale, numero decreto nomina, data decreto nomina)

Responsabile esterno del trattamento: dati identificativi del soggetto nominato responsabile esterno ex art. 28 GDRP.

DETTAGLIO TRATTAMENTO

Date significative: individuazione delle date rilevanti ai fini della gestione del trattamento (data compilazione, data validazione, data di inizio validità, data di fine validità)

Fonti normative: indicazione delle fonti normative che individuano/supportano il trattamento

Finalità: individuazione delle finalità di rilevante interesse pubblico perseguite relativamente all'attività istituzionale a cui è collegato il trattamento

Categoria di soggetti associabili: macro categoria di soggetti interessati i cui dati rientrano in un'attività di trattamento del soggetto titolare/responsabile

Modalità di trattamento: indicazione dell'ambito nel quale il trattamento viene posto in essere nonché indicazione del carattere automatizzato o meno del trattamento.

Altre informazioni: informazioni aggiuntive volte in particolare a rivelare se il trattamento può essere definito su "larga scala" o meno.

INFORMAZIONI SUI DATI

Natura dei dati personali: indicazione della tipologia di dati oggetto di trattamento

Operazioni sui dati di cui si compone il trattamento: indicazione delle operazioni svolte sui dati; le operazioni possono essere di carattere standard oppure particolari

Regolamento dei dati sensibili e giudiziari: annotare e citare eventuali codici di condotta o codici deontologici

Consenso e trattamento di dati: indicazioni relative al consenso prestato al trattamento dei dati, all'informativa, al trasferimento ed all'eventuale comunicazione a terzi

ASSET

Strumenti utilizzati: banche dati, tecnologie cloud, strumenti IoT, ecc.

RISCHIO

Dati relativi al rischio: indicazioni volte a quantificare il rischio (sotto un profilo di probabilità di verificazione ed impatto) a seguito di trattamento per i diritti e le libertà per l'interessato; successivamente a tale valutazione si decide se procedere a DPIA.

4 Stato dell'arte del sistema di gestione del registro dei trattamenti

L'accesso al sistema che gestisce il software deve avvenire mediante Smart-card o SPID; la gestione di tali chiavi di accesso è demandata alla Funzione di Abilitazioni che assegna i profili corretti.

Il sistema, come già affermato in aperura del presente documento, è pensato affinché lo strumento non sia pensato solo per la Regione Toscana ma anche per altri enti collegati ad essa, per fare in modo che questi possano censirsi come titolare del trattamento o di suo delegato.

Ad analoga indicazione si giunge con riguardo ai responsabili esterni che devono essere messi in condizione di potersi censire come tali.

Il sistema distingue due tipologie di trattamenti: quelli trasversali per i quali intervengono più profili per la gestione del trattamento e quelli verticali per i quali interviene un'unica organizzazione.

Tanto le schede per i trattamenti trasversali quanto quelle per quelli verticali contengono informazioni generali:

1. Soggetti: Titolare del Trattamento (nella persona di: nome e cognome del delegato), Contitolare del trattamento: nome/cognome; nella persona di Struttura del dirigente delegato dal titolare del trattamento (settore, direzione, nome/cognome del direttore, numero decreto di nomina, data del decreto di nomina).
2. Date significative: (data di compilazione, data ultima modifica del trattamento, data validazione, data inizio validità, data fine validità, nome/cognome del compilatore).
3. Dettaglio del Trattamento: (codice trattamento, stato del trattamento, denominazione trattamento, descrizione trattamento, procedimento, ambito di attività, fonti normative del procedimento, altre fonti normative, Finalità, finalità old, categorie di soggetti associabili al trattamento, trattamento effettuato su larga scala, criterio del trattamento effettuato su larga scala, natura dei dati (categoria, tipo, termine ultimo di cancellazione), modalità trattamento (automatizzato o meno), tipologia delle operazioni, ASSET/strumenti utilizzati, regolamento dei dati sensibili e giudiziari, eventuale responsabile esterno (CF/ P. IVA, ragione sociale/nome cognome, data atto autorizzativo, data inizio/ data fine (entrambi obbligatori), consenso (necessario, non necessario, non raccolto) specificare in che forma viene raccolto, informativa, livello di impatto del rischio (da graduare in basso, medio, alto), probabilità di verificazione del rischio (da graduare in basso, medio, alto), livello di rischio (calcolato secondo la formula), trasferimento, comunicazione a terzi (se si specificare il soggetto destinatario, fonte normative).

1.6 Interventi da porre in essere e definizione dell'indice dei Trattamenti

Al fine di una corretta compilazione ed aggiornamento del registro dei trattamenti è necessario, in fase di redazione del registro, individuare i trattamenti posti in essere dal Titolare indicando le seguenti informazioni: categorie di dati personali trattati; eventuale trattamento di dati personali di minori o di altre categorie di soggetti giuridicamente incapaci; individuazione di categorie particolari di dati personali; base giuridica del trattamento; diverse finalità del trattamento; operazioni eseguite sui dati personali; soggetti coinvolti nelle singoli operazioni di trattamento, qualificazione giuridica (tipologia di soggetto giuridico) e ruolo rivestito nell'organigramma interno relativo alla funzione "privacy/protezione dei dati personali"; eventuale comunicazione di dati personali a soggetti terzi; eventuale diffusione di dati personali; tempi di conservazione dei dati; risorse – anche informatiche – utilizzate per lo svolgimento delle operazioni di trattamento e relative modalità; eventuale trasferimento di dati personali all'estero; esistenza di procedure per assolvere alle richieste dell'interessato con riferimento all'esercizio dei propri diritti; indicazione se trattasi trattamento su larga scala; indicazione se trattasi di monitoraggio dell'interessato; utilizzo dei dati personali per la profilazione; utilizzo dei dati personali nell'ambito di processi decisionali automatizzati.

5 Modalità di intervento/aggiornamento e compilazione del registro trattamenti

1.7 Definizione di attributi di gestione del software

Come già rilevato in sede di analisi della norma, il registro delle attività di trattamento può essere redatto in formato cartaceo oppure elettronico.

Vero è, stante la matrice di diritto pubblico che caratterizza l'ente Regione nonché gli enti di diritto pubblico partecipati dalla stessa o gli enti che formalmente di diritto privato mantengono una partecipazione pubblica, a cui si aggiunge l'elevato numero di trattamenti censiti (come ad es. per la Regione Toscana il numero ad oggi è oltre i 1.300 trattamenti) risulta preferibile l'adozione di un sistema informativo che meglio possa rendere l'aggiornamento e/o l'accesso alle informazioni.

Chiarito l'aspetto del formato che il registro dovrebbe assumere, per quel che concerne la gestione del registro delle attività di trattamenti si ritiene opportuno adottare una serie di accorgimenti tecnici che determinano una corretta gestione dello stesso. Ebbene, a titolo esemplificativo ma non esaustivo si fa riferimento a Log di sistema che consentono di capire quale soggetto ha compiuto determinate azioni, archiviazione su una cartella dedicata di un server, prevedere copie di backup settimanali, ecc.

1.8 Accesso, compilazione e tempistiche di intervento sul registro trattamenti

Il presente paragrafo intende analizzare i livelli di intervento/accesso sui registri di trattamento.

Nello specifico, con riguardo alla gestione del registro delle attività di trattamento sono individuabili una pluralità di profili:

- Titolare del trattamento o di un suo delegato
- Referente interno
- Utente: dipendente di regione che agisce e opera sulle schede a cui è abilitato
- Ufficio del DPO
- DPO
- Garante

Con riguardo alle tempistiche di aggiornamento si deve sin da subito sottolineare che il registro sarà aperto e aggiornato tutte le volte che vengono modificati uno o più degli attributi, sopra citati, a titolo

esemplificativo e non esaustivo le modifiche potrebbero riguardare il cambio responsabile ex art. 28 del GDPR, se cessa un trattamento, se il trattamento muta nelle finalità, se cambia la valutazione della DPIA, ecc.

Il procedimento che porta un determinato trattamento all'interno dell'apposito registro segue un iter classificabile per fasi:

1. **Censimento del trattamento**: scopo dell'attività è quella di capire se vi è una tipologia di trattamento non ancora censita nel registro trattamenti.
2. **Identificazione del trattamento**: scopo dell'attività identificare i soggetti attivi del trattamento, identificandoli secondo le definizioni del Regolamento.
3. **Verifica di conformità**: scopo dell'attività è capire se il trattamento in esame rispetta in primo luogo i principi di cui all'art. 5 del GDPR. ed in seconda battuta le condizioni di liceità di cui all'art. 6.
4. **Valutazione DPIA**: attività che serve ad analizzare una perfetta compliance con il GDPR. Essa si articola in diverse fasi:
   a) Valutazione preliminare: scopo dell'attività è quella di raccogliere tutte le informazioni necessarie a valutare prima di tutto se il trattamento è conforme al regolamento GDPR e in seconda battura comprendere se quel trattamento deve essere sottoposto ad una valutazione DPIA.
   b) Esecuzione DPIA: una volta determinata la necessità di procedere ad una attività di DPIA si rende necessario procedere alla raccolta delle informazioni necessarie allo sviluppo successivo delle attività di analisi dei rischi e produzione del piano dei trattamenti.
   c) Formalizzazione dei risultati: valutare se le misure individuate sono idonee a mitigare i rischi ad un livello accettabile, stimando in tal senso un rischio residuo, nonché documentare i risultati di tutte le attività svolte durante la DPIA ed i razionali che determinano la scelta se procedere o meno alla Consultazione Preventiva
   d) Eventuale Consultazione Preventiva: consultare l'Autorità di Controllo qualora non sia stato possibile ridurre il rischio residuo a un livello accettabile. L'attività include il recepimento dell'eventuale risposta e l'attuazione degli eventuali interventi necessari per aderire al parere fornito dall'Autorità.
   e) Monitoraggio e Riesame: il processo DPIA, una volta terminate le attività relative alla prima valutazione, deve prevedere un monitoraggio dei risultati raggiunti e un conseguente riesame costante al fine di garantire nel tempo la mitigazione dei rischi e la conformità al

Regolamento Europeo anche a fronte di fisiologici cambiamenti a cui sono soggetti tutti i trattamenti.

Per ciò che concerne il dettaglio delle operazione di DPIA si rimanda al documento "Indicazioni operative per redazione di linee guida per la valutazione di impatto del rischio"

NOTA BENE: al termine della valutazione DPIA e prima di passare alla scrittura nel registro dei trattamenti, il DPO deve essere informato e chiamato a valutare il passaggio allo step finale.

5. **Scrittura nel registro trattamenti:** ultima fase del processo è la scrittura del trattamento nell'apposita scheda del registro dei trattamenti mediante allegazione di checklist per l'analisi del rischio.

La scheda può assumere una pluralità di stati:

Bozza: scheda inserita, modificabile e visibile solo dagli utenti del medesimo livello di struttura aziendale

Validabile: scheda inserita, modificabile e visibile agli utenti preposti alla validazione

Validata: la scheda è validata, visibile agli utenti ma non più modificabile dal proponente

Da rivedere: dopo la fase di validazione, possono verificarsi degli eventi, manuali o automatizzati, che determinano il cambiamento di questo stato.

In revisione: la scheda è presa in carico dall'utente gestore della scheda per la sua revisione. A seguito di tale evento la scheda potrà riportare due stati: "Da validare" (per successiva validazione) oppure chiusa (data fine validità)

Chiusa: quando termina il periodo di validità.

1.9 Tenuta del registro da parte dei soggetti nominati Responsabili

Per quello che concerne il rapporto tra Titolare e Responsabili del trattamento (es. Fornitori) occorre infine chiarire quali informazioni condividono in ordine alla tenuta del registro.

In particolare, essendo il Responsabile obbligato dall'art. 30 par. 2 a creare un proprio registro dei trattamenti per i dati che tratta per conto del Titolare esso sarà chiamato in caso di verifica da parte dell'Autorità di Controllo ad esibire il suo registro.

Il registro del responsabile contiene *in primis* come elementi obbligatori seguenti dati: nome dati di contatto del responsabile, nome dati di contatto DPO, stato del registro, data generazione del registro, categorie di trattamento effettuate per ogni titolare.

Nello specifico, altresì, per ogni trattamento verrà indicato: tipologia trattamento, denominazione trattamento, finalità, categorie interessati, categorie dati, categorie destinatari/comunicazione, trasferimento, termini cancellazione, descrizione generale su misure di sicurezza tecniche ed organizzative, contenuto ulteriore, data inizio validità, data validazione, data fine validità, data storicizzazione.

Come in precedenza analizzato le schede dei trattamenti possono differenziarsi in verticali e trasversali; la loro sostanziale differenza si apprezza in ordine al procedimento di approvazione delle schede.

6 Controlli

La presente sezione si riferisce ai controlli che verranno posti in essere sul registro dei trattamenti.

1.10 DPO

Una importante funzione di controllo in ordine alla regolare tenuta nonché aggiornamento del registro delle attività di trattamenti è demandata alla figura del DPO.

Ai sensi dell'art. 39 che disciplina infatti le prerogative del soggetto *de quo* si evince che tra le altre è tenuto a "*sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché 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*".

All'attribuzione di controllo che gli viene assegnato direttamente dalla legge si aggiunga il già più volte richiamato, nel corso del presente documento, principio di *accountability* che impone in tal caso al DPO di verificare che l'organizzazione per la quale compie attività di verifica sia conforme alla disciplina del Regolamento non solo in termini di adempimento, ma anche di capacità di dimostrazione della compliance normative.

Da ultimo si osservi la possibilità di intervento in ordine al controllo sul registro dei trattamenti, potendo intervenire mediante una pluralità di azioni.

Il DPO e i componenti del suo ufficio possono a titolo esemplificativo, ma non esaustivo: visualizzare tutte le schede, mettere le schede dei trattamenti in stato "da rivedere" qualora fosse ravvisata una qualsiasi irregolarità/anomalia, abilitare il Garante a prendere visione del registro, generare il registro dei trattamenti, agire per tutti gli Enti presenti nel Sistema per i quali sono riconosciuti DPO o come ufficio DPO.

In ogni caso il supporto del DPO non sarà in prima battuta diretto, in quanto qualora dovessero sorgere questioni relative alla tenuta del registro occorrerà fare in primo luogo riferimento al referente d'area cui afferisce la problematica.

1.11 Soggetti attivi

Come visto in precedenza per la figura del DPO, sono previsti compiti di sorveglianza per la corretta applicazione del GDPR, anche in capo ai soggetti autorizzati ex art. 29 del GDPR.

Soggetti che, per la loro normale attività di trattamento dei dati giornaliera, sono tenuti ad operare una verifica puntuale circa la presenza delle condizioni di liceità del trattamento ex art. 6. nonché del pieno rispetto dei principi applicabili al trattamento di dati ex art. 5 del GDPR durante tutte le fasi che portano all'iscrizione del trattamento sull'apposito registro (censimento, identificazione, verifica di conformità, ecc.).

7 Aspetti sanzionatori

1.12 Violazioni

Le indicazioni operative che il Titolare o suo delegato dovrà predisporre per le proprie verifiche periodiche dovrà prevedere quanto meno l'individuazione della casistica delle possibili violazioni con riguardo ai diversi trattamenti e con riferimento agli obblighi giuridici del Titolare del trattamento così come delineati dalla normativa in materia di protezione dei dati personali.

Questo anche al fine di agevolare il controllo della compliance e l'adozione delle misure di contenimento del relativo rischio.

Con il termine violazioni si fa riferimento a quelle irregolarità nella tenuta del registro dei trattamenti che possono essere oggetto di sanzione a seguito di accertamento delle autorità di controllo competenti.

A titolo esemplificativo si può fare riferimento alla mancata conservazione di registro di trattamento in una organizzazione che occupa più di 250 dipendenti; l'assenza di giustificazione in ordine alla mancata redazione del registro dei trattamenti in contrasto quindi con il principio di accountability; la mancata indicazione delle informazioni richieste ex art. 30.

1.13 Sanzioni

In conformità del paragrafo 2 dell'art. 83 GDPR, la violazione da parte del Titolare del trattamento o di suo delegato o del Responsabile del trattamento, con riguardo al registro delle attività di trattamento, è soggetta a sanzioni amministrative pecuniarie fino a 10 000 000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente.

Altresì, secondo il paragrafo 2 dell'articolo 83 GDPR, l'inosservanza di un ordine da parte dell'Autorità di controllo di cui all'articolo 58, paragrafo 2, è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Fatti salvi i poteri correttivi delle Autorità di controllo a norma dell'articolo 58, paragrafo 2, ogni Stato membro può prevedere norme che dispongano se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad Autorità pubbliche e organismi pubblici istituiti in tale Stato membro.

A ciò si deve aggiungere, in via generale, che l'art.82 del GDPR prevede che chiunque subisca un danno materiale o immateriale causato da una violazione del Regolamento ha il diritto di ottenere il risarcimento

del danno dal soggetto al quale l'obbligo (violato) era imposto (salvo che quest'ultimo dimostri che l'evento dannoso non gli è imputabile).