TERME DI CHIANCIANO
DOCUMENTO ATTUATIVO DEL REGOLAMENTO COMUNITARIO PER LA PROTEZIONE DEI DATI PERSONALI (EU 2016/679)

***

1) LA NORMATIVA COMUNITARIA
CONCETTI GENERALI

Il Regolamento generale per la protezione dei dati personali n. 2016/679 (General Data Protection Regulation o GDPR) è la normativa europea in materia di protezione dei dati. Pubblicato nella Gazzetta Ufficiale europea il 4 maggio 2016. Trattandosi di un regolamento, non necessita di recepimento da parte degli Stati dell'Unione e quindi è attuato allo stesso modo in tutti gli Stati dell'Unione senza margini di libertà nell'adattamento. Il suo scopo è la definitiva armonizzazione della regolamentazione in materia di protezione dei dati personali all'interno dell'Unione europea. Il regolamento proclama tutela del diritto alla protezione dei dati personali inteso come diritto fondamentale delle persone fisiche:

Art. 1. *Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.*

In quest'ottica il principio cardine del nuovo regolamento è costituito dall'autodeterminazione informativa.

Approccio *risk based* e responsabilizzazione

Il regolamento sposta il fulcro della normativa dalla tutela dell'interessato alla responsabilità del titolare e dei responsabili del trattamento (“accountability” vuol dire "dover rendere conto del proprio operato") che si concretizza nell'adozione di comportamenti proattivi a dimostrazione della concreta adozione del regolamento. In particolare si evidenzia la necessità di attuare misure di tutela e garanzia dei dati trattati, con un approccio del tutto nuovo che demanda ai titolari il compito di decidere autonomamente le modalità e i limiti del trattamento dei dati alla luce dei

criteri specifici indicati nel Regolamento:

- principio "*privacy by design*", in base al quale i prodotti e i servizi dovranno essere progettati fin dall'inizio in modo da tutelare la privacy degli utenti.
- rischio del trattamento, inteso come valutazione dell'impatto negativo sulle libertà e i diritti degli interessati.

L'approccio è centrato sulla protezione dei dati. Si tratta di un approccio basato sulla valutazione del rischio (*risk based*), con il quale si determina la misura di responsabilità del titolare o del responsabile del trattamento, tenendo conto della natura, della portata, del contesto e delle finalità del trattamento, nonché della probabilità e della gravità dei rischi per i diritti e le libertà degli utenti.

Le nuove norme prevedono inoltre:

- per i cittadini un più facile accesso alle informazioni riguardanti i loro dati;
- un diritto alla portabilità dei dati che consentirà di trasferire i dati personali tra i vari servizi *on line*;

- l'istituzionalizzazione del diritto all'oblio, che consente di chiedere ed ottenere la rimozione dei dati quando viene meno l'interesse pubblico alla notizia;
- l'obbligo di notifica da parte delle aziende delle gravi violazioni dei dati dei cittadini;
- le aziende dovranno rispondere alla sola autorità di vigilanza dello Stato di appartenenza;

- sanzioni amministrative in caso di violazioni delle norme.

Base giuridica del trattamento

Il nuovo regolamento pone l'accento sul principio della trasparenza, in un'ottica di rispetto della finalità.

Trasparenza e conformità al regolamento

Il regolamento europeo prevede una serie di obblighi proattivi ed in tale ottica la predisposizione e l'aggiornamento della documentazione è essenziale, in quanto indice di corretta implementazione delle norme.

Ambito di applicabilità materiale e territoriale

Il Regolamento generale si applica ad ogni "t*rattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali*

contenuti in un archivio o destinati a figurarvi".

Per quanto riguarda l'ambito territoriale, il regolamento si applica ad ogni trattamento che ha ad oggetto dati personali e a tutti i titolari (*controller*) e responsabili (*processor*) del trattamento stabiliti nel territorio dell'Unione.

2) APPROCCIO METODOLOGICO

La redazione del documento è stata preceduta da una fase di acquisizione dati e/o documentazione e sono state assunte informazioni dal DPO e dal personale amministrativo di Terme

Sono state effettuate, attraverso checklist, approfondite valutazioni in merito alla necessità di:

a) redazione di un documento di attuazione "ampio";

b) necessità di adozione del registro dei trattamenti;

c) necessità della c.d valutazione di impatto del trattamento (D.P.I.A., cioè *Data Protection Impact Assessment*);

Mentre le prime due valutazioni hanno avuto esito positivo ci si è orientati sulla non necessità della c.d. Valutazione d'impatto per le ragioni che seguono.

L'articolo 35 del regolamento europeo regolamenta la valutazione di impatto. A differenza delle valutazioni di sicurezza, la valutazione di impatto va sviluppata solo per particolari trattamenti, e cioè quando il trattamento prevede l'uso di nuove tecnologie e può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

In particolare l'articolo 35 evidenzia la necessità della valutazione di impatto nei seguenti casi: il trattamento determina 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; il trattamento riguarda dati sensibili o giudiziari su larga scala; sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Partendo dal presupposto che Terme provvede al trattamento di dati sensibili, l'analisi si è concentrata sul concetto di "larga scala". Nel silenzio normativo l'unico supporto ci proviene dalle linee guida rilasciate dal WP 29 che indica che il concetto deve essere legato a fattori quali: Il territorio geografico – quanto ampio è il territorio

all’interno del quale effettuo il trattamento; l volume e la tipologia dei dati trattati; la percentuale di interessati sul totale di una popolazione di riferimento; la durata del trattamento.

Su tali presupposti si ritiene che stante la tipologia dei dati trattati (sensibili ma comunque limitati non a tutto lo spettro sanitario ma mirati a determinate specifiche situazioni patologiche a fini preventivi) la percentuale di interessati (limitata rispetto alla popolazione di riferimento) e la durata del trattamento (anch'essa limitata) la valutazione d'impatto non sia necessaria anche il ragione dei potenziali rischi che il trattamento comporta trattandosi di procedure, di fatto, standardizzate con intervento limitato degli operatori e con dati che non si “trasferiscono” per altri scopi a d altri soggetti.

Terme, invece, ha deciso di dotarsi di un c.d. Codice Deontologico finalizzato a stabilire i principi generali ai quali il comportamento di tutti i soggetti, l*atu sensu* interessati alla vigenza delle norme del Regolamento, si devono attenere.

3) MODELLO ORGANIZZATIVO SULLA PROTEZIONE DATI PERSONALI

Alla base del nuovo regolamento è il principio di responsabilità (Accountability) che informa tutta la struttura della normativa europea.

Terme si è dotata di un modello organizzativo, tecnologico e di processo che soddisfa quanto richiesto dal GDPR. Sulla base di tali sistemi di gestione Terme ha messo in atto controlli, procedure, informative, meccanismi di miglioramento continui atti a rendere i trattamenti dei dati personali effettuati da essa e da eventuali Responsabili dei Trattamenti e/o Incaricati che, in suo nome e per suo conto, dovessero eseguirli, in linea con quanto previsto dal regolamento europeo.

Terme promuove il rispetto, da parte dei propri dipendenti e collaboratori, di alti valori morali e di integrità di condotta, imponendo il corretto utilizzo delle informazioni personali di cui entrano in possesso nello svolgimento della propria attività lavorativa.

Terme è società attiva nel campo sanitario e del benessere e svolge la propria attività nel rispetto dei principi di eguaglianza, imparzialità, continuità, partecipazione, efficienza, efficacia ed economicità.

Si impegna inoltre ad ascoltare le esigenze di istituzioni, aziende e cittadini, a confrontarsi con loro e a fornire informazioni aggiornate sui servizi.

Il Modello

Il modello organizzativo di Terme si articola su tre livelli:

• Governo: i ruoli coinvolti in questa attività determinano il sistema di Governance applicabile ai trattamenti effettuati dall'azienda e definiscono le decisioni strategiche e le linee guida in materia di Data Protection

• Sorveglianza: il DPO è deputato alla verifica della conformità del sistema di gestione dei dati alla normativa.

• Attuazione e Gestione: le figure coinvolte in queste attività danno attuazione alle decisioni aziendali e hanno cura di effettuare i trattamenti nel rispetto delle linee guida elaborate e dettagliate dal titolare e dai ruoli deputati alla Governance.

Flussi informativi del Modello Organizzativo

In tema di flussi informativi il DPO è il fulcro dei medesimi e si rivolge e rapporta in maniera diretta al titolare del trattamento attraverso sia l'organo amministrativo sia a quello di controllo.

Il DPO svolge inoltre azione diretta sia nei confronti dell'autorità di controllo che degli interessati che nei confronti dei responsabili del trattamento ed, ove eventualmente nominati, degli incaricati.

Il DPO riferisce almeno una volta all'anno all'Organo Amministrativo e agli Organi di Controllo in merito al livello di conformità al Regolamento, all'osservanza della normativa e delle politiche aziendali in materia di *data protection,* all'attuazione del Modello Organizzativo *Data Protection*, agli esiti dell'attività di vigilanza svolta e formula suggerimenti per il miglioramento del modello. In particolare, il DPO riporta in maniera continuativa al Consiglio di Amministrazione e agli Organi di Controllo, in ogni circostanza in cui lo ritenga necessario e/o opportuno per l'attuazione degli obblighi previsti dal Regolamento, fornendo ogni informazione rilevante e/o utile per il corretto adempimento delle prescrizioni del Regolamento attraverso una relazione scritta al Consiglio di Amministrazione con periodicità almeno annuale, sulle attività svolte, sulle richieste degli interessati, sulle richieste dell'autorità di controllo, sui suggerimenti in merito agli interventi correttivi da adottare per rimuovere eventuali

disallineamenti riscontrati.

Il titolare del trattamento dati ha invece rapporto diretto sia con i responsabili del trattamento dati che con gli eventuali incaricati.

Pubblicazione

Terme, al fine di portare a conoscenza di tutti i soggetti interessati ed in maniera organica la sua politica di privacy aziendale, pubblica il suo modello organizzativo sul proprio sito internet, nel settore appositamente dedicato alla "privacy", secondo il modello reperibile nella parte "Modulistica" del presente documento

4) CODICE DENTOLOGICO

La *ratio* della sua adozione

Al fine di meglio precisare e conformare i comportamenti tenuti da Terme (intesi in senso oggettivo e di comportamento soggettivo) quest'ultima ha inteso necessario precisare principi di ordine generale da tenere da parte di tutti i soggetti "interni ed interni" ma che comunque sono da intendersi interessati al tema della privacy.

Il Codice

"Terme di Chianciano (in avanti anche "Terme") adotta sulla base della normativa comunitaria in tema di protezione dei dati personali (di seguito denominata anche"normativa"), un codice deontologico e ciò sulla base delle seguenti premesse:

- *le disposizioni del presente codice di deontologia e di buona condotta sono volte ad assicurare l'equilibrio tra i diritti e le libertà fondamentali della persona, in particolare il diritto alla protezione dei dati personali e il diritto alla riservatezza, con le esigenze del trattamento dei dati personali e la salute del soggetto che entra in contatto con Terme per fini sanitari e del benessere;*
- *Terme, ed ogni altro soggetto che direttamente od indirettamente tratta dati di carattere sanitario, conformano al presente codice ogni fase dei trattamenti di dati personali effettuati a fini sanitari indipendentemente dalla sottoscrizione del codice stesso da parte dei rispettivi enti/soggetti/persone ai quali appartengono;*
- *nell'applicazione del presente codice, i soggetti che ne sono destinatari osservano i princìpi contenuti nel Regolamento Comunitario nonché nelle altre disposizioni normative nazionali, comunitarie ed internazionali relative al trattamento dei dati personali. Essi operano nel rispetto dei princìpi di pertinenza e di non eccedenza, intesa come non ridondanza del trattamento progettato rispetto agli scopi perseguiti, avuto riguardo ai dati disponibili ed*

ai trattamenti già effettuati dallo stesso titolare.

Art 1. Ambito di applicazione

Il presente codice si applica all´insieme dei trattamenti effettuati per scopi sanitari e terapeutici e del benessere in genere conformemente agli standard metodologici del pertinente settore disciplinare e devono essere rispettate nel trattamento di dati personali da parte di tutti i soggetti che operando direttamente od indirettamente per Terme entrano in contatti con i c.d. "interessati" secondo la definizione datane dal Regolamento Europeo sulla privacy.

Art. 2 Modalità di trattamento

Terme organizza il trattamento anche non automatizzato dei dati personali secondo le modalità che risultino più adeguate a favorire in concreto l´effettivo rispetto dei diritti, delle libertà e della dignità degli interessati, applicando i princìpi di finalità, necessità, proporzionalità e non eccedenza sulla base di un attenta valutazione sostanziale e non formalistica delle garanzie previste, nonché di un´analisi della quantità e qualità delle informazioni che utilizza e dei possibili rischi.
Specifica attenzione è prestata all´adozione di idonee cautele per prevenire l'ingiustificata raccolta, utilizzazione o conoscenza di dati in caso di:

a) acquisizione anche informale di notizie, dati e documenti connotati da un alto grado di confidenzialità o che possono comportare, comunque, rischi specifici per gli interessati;
b) scambio di corrispondenza, specie per via telematica;
d) utilizzo di dati di cui è dubbio l´impiego lecito, anche per effetto del ricorso a tecniche invasive;
e) utilizzo e distruzione di dati riportati su particolari dispositivi o supporti, specie elettronici (ivi comprese registrazioni audio/video), o documenti
f) custodia di materiale documentato
h) conservazione di atti

Art. 3 Informativa

Nella raccolta di dati è chiaramente rappresentata all´interessato la finalità del trattamento lo scopo e le sue caratteristiche con espressa indicazione dei diritti dell'interessato secondo quanto previsto dal Regolamento Europeo.

Art. 4 Consenso

Il trattamento dati non può essere effettuato da TERME senza il consenso dell´interessato salvo che si evidenzi in dettaglio e specificamente le ragioni per le quali il conferimento è facoltativo.

Art.5 Comunicazione e diffusione dei dati

È consentito diffondere dati soltanto in forma aggregata ovvero secondo modalità che non rendano identificabili gli interessati neppure tramite dati identificativi indiretti.

Quando il trattamento comporta il trasferimento anche temporaneo dei dati personali

in un Paese, non appartenente all´Unione europea, il cui ordinamento non assicura un livello di tutela delle persone adeguato, il trasferimento è consentito sulla base di garanzie per i diritti dell'interessato comparabili a quelle del presente codice e della normativa comunitaria in materia.

Art 6 Trattamento dati sensibili

I dati sensibili devono essere trattati, di regola, in forma anonima.
Quando i dati sensibili non possono essere raggiunti senza la identificazione anche temporanea degli interessati, il titolare adotta specifiche misure per mantenere separati i dati identificativi già al momento della raccolta, salvo ciò risulti impossibile in ragione delle particolari caratteristiche del trattamento o richieda un impiego di mezzi manifestamente sproporzionato

Art. 7 Dati sanitari particolari: i dati genetici.

Il trattamento di dati genetici è consentito nei soli casi e modi previsti da apposita autorizzazione del Garante

Art. 8 Raccolta dei dati

Nella raccolta dati Terme di Chianciano pone specifica attenzione nella selezione del personale incaricato della raccolta e nella definizione dell´organizzazione e delle modalità di rilevazione, in modo da garantire il rispetto del presente codice e la tutela dei diritti degli interessati.
2. Il personale incaricato della raccolta si attiene alle disposizioni contenute nel presente codice e alle istruzioni ricevute. In particolare:

a) rende nota la propria identità, la propria funzione e le finalità della raccolta del dato anche attraverso apposita modulistica applicativa e comunicando all'interessato la esistenza del sito internet ufficiale dove si trovano, in apposito settore, tutte le informazioni utili.

b) fornisce le informazioni utli nonché ogni altro chiarimento che consenta all´interessato di rispondere in modo adeguato e consapevole, evitando comportamenti che possano configurarsi come artifici ed indebite pressioni;
c) provvede tempestivamente alla correzione degli errori e delle inesattezze delle informazioni acquisite;
e) assicura una particolare diligenza nella raccolta dati;

Art. 9 Conservazione dati

Terme tratterà i dati personali esclusivamente per le finalità connesse alle attività aziendali per il tempo strettamente necessario a conseguire gli scopi per cui sono stati raccolti. Terme adotta specifiche misure di sicurezza per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati ed archivierà i dati personali per un periodo di tempo non superiore a quello strettamente necessario agli scopi per i quali sono stati raccolti o successivamente trattati, conformemente a

quanto previsto dagli obblighi di legge.

Art. 10. Misure di sicurezza

Terme adotta le misure di sicurezza dei dati e dei sistemi di cui agli artt. del Regolamento Comunitario e di massima prende in considerazione (ma non in forma vincolante non essendo più obbligatorio) quanto indicato nel disciplinare tecnico contenuto nell' allegato B) del Codice.

Art. 11. Esercizio dei diritti dell´interessato

In caso di esercizio dei diritti l´interessato può accedere agli archivi che lo riguardano per chiederne l´aggiornamento, la rettifica o integrazione od il c.d. Diritto all'oblio sempre che tale operazione non risulti impossibile per la natura o lo stato del trattamento o comporti un impiego di mezzi manifestamente sproporzionato.

Art. 12. Regole di condotta

Terme assicura che i responsabili e gli incaricati del trattamento e comunque ogni soggetto che, per motivi di lavoro, abbia legittimo accesso ai dati personali trattati, conformano il proprio comportamento anche alle seguenti disposizioni:

a) i dati personali possono essere utilizzati soltanto per gli scopi ad essi propri;
b) i dati personali devono essere conservati in modo da evitarne la dispersione, la sottrazione e ogni altro uso non conforme alla legge e alle istruzioni ricevute;
c) i dati personali di cui si venga a conoscenza in occasione dello svolgimento dell´attività lavorativa non possono essere diffusi, né altrimenti utilizzati per interessi privati, propri o altrui;
d) le conoscenze professionali in materia di protezione dei dati personali sono adeguate costantemente all´evoluzione delle metodologie e delle tecniche;
personali;
e) i comportamenti non conformi alle regole di condotta dettate dal presente codice sono immediatamente segnalati al responsabile del trattamento al DPO o al titolare del trattamento.

Art. 13. Adeguamento

La corrispondenza delle disposizioni del codice alla normativa, anche di carattere internazionale, introdotta in materia di protezione dei dati personali trattati è verificata nel tempo anche su segnalazione dei soggetti interni e/o esterni a Terme; ciò ai fini dell´introduzione nel codice medesimo delle modifiche necessarie al fine del coordinamento con dette fonti, ovvero, qualora tali modifiche incidano in maniera apprezzabile sulla disciplina del presente codice.

Modulistica

Il Codice si trova trascritto nella sua completezza nella parte relativa alla

"Modulistica" del presente documento

5) IL REGISTRO DEI TRATTAMENTI DEI DATI PERSONALI

Informazioni Generali

Il registro dei trattamenti è il primo adempimento imposto dal GPDR a chiunque effettui un trattamento di dati che possa presentare un rischio per i diritti e le libertà degli interessati che non sia occasionale o che includa dati sensibili, genetici, biometrici e giudiziari.

Esplicitazione del principio di "*accoutability*" (responsabilizzazione), precisa e definisce la procedura sul trattamento dei dati prevista dall'abrogato Codice Privacy (che prevedeva solo l'obbligo di notifica preventiva al Garante della Privacy in caso di trattamento di dati a rischio), risultando in tal modo uno strumento fondamentale - oltre che per eventuali controlli di legittimità da parte del Garante - per disporre di un quadro sempre aggiornato dei trattamenti in essere all'interno di un'azienda, ma soprattutto risulta indispensabile per poter procedere a qualsiasi valutazione e analisi di eventuali rischi, costituendo, dunque, non un mero "*adempimento formale bensì parte integrante di un sistema di corretta gestione dei dati personali"* (Guida all'applicazione del Regolamento Europeo in materia di protezione dati personali)

L'art. 30 c. 1 del Reg. UE 679/2016 prevede che esso deve contenere una serie di informazioni sulle attività riguardanti il trattamento dei dati personali, quali:

- il nome e i dati di contatto del titolare (ed eventualmente del contitolare) del trattamento, del rappresentante del titolare e del responsabile della protezione dei dati;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali trattati;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi eventualmente i destinatari di paesi terzi non appartenenti all'Unione Europea od organizzazioni internazionali;
- nel caso in cui sia previsto, l'indicazione del fatto che i dati personali saranno trasferiti verso un paese terzo o un'organizzazione internazionale, indicando

anche di quale paese od organizzazione internazionale si tratta e, inoltre, la documentazione delle garanzie previste;

- i termini ultimi stabiliti per la cancellazione delle diverse categorie di dati;
- una descrizione generale delle misure di sicurezza tecniche e organizzative individuate al fine di garantire un livello di sicurezza dei dati personali adeguato al rischio cui gli stessi sono esposti**.**

Da un punto di vista strettamente formale, il GDPR non detta delle regole generali né individua le concrete modalità attraverso cui il registro delle attività di trattamento dovrà essere formato.

L'art. 30 si limita infatti a precisare che il registro delle attività di trattamento dei dati dovrà essere tenuto in forma scritta, su supporto tangibile oppure, e preferibilmente, in formato elettronico, ad esempio utilizzando un file excel (per le organizzazioni più semplici) oppure un software apposito che consenta di raccogliere, organizzare, individuare facilmente tutte le informazioni che un registro deve contenere ai sensi dell'art 30 del GPDR. In tal modo sarà più agevole aggiungere, cancellare e/o modificare informazioni quando necessario, tenere traccia delle operazioni effettuate sui registri delle attività, e metterlo a disposizione su richiesta dell'autorità di controllo : il Garante per la protezione dei dati personali).

Si tenga presente che ogni specifico trattamento deve avere una sezione dedicata e le informazioni devono essere strutturate e collegate in maniera logica tra di esse, in quanto ad esempio una tipologia di trattamento può avere periodi di conservazione diversi rispetto ad un'altra, oppure una specifica tipologia di trattamento può prevedere che i dati siano condivisi con alcuni soggetti che un'altra non prevede o ancora un trattamento può riguardare una specifica categoria di dati diversa rispetto ad un altro. Un elenco generico di dati senza alcuna organizzazione, logica o collegamento tra le informazioni contenute non ha alcun senso.

Quindi, un titolare del trattamento potrebbe suddividere i trattamenti partendo dalle aree aziendali che se ne occupano e sulla base di ciascuna area, individuare ogni specifico trattamento che la coinvolge, per ciascun trattamento definire le finalità, le specifiche modalità, le categorie di interessati, le categorie di dati trattati, i soggetti con cui i dati si condividono, allegando i relativi contratti di designazione e quanto altro richiesto dall'art. 30.

Ad ogni modo, è bene rilevare che un registro delle attività di trattamento consente di identificare velocemente le operazioni svolte sui dati trattati, sapere quali dati personali si detengono perché si conservano e per quanto tempo e aiuta a riconoscere i dati non più necessari; operazioni, queste, che consentono di affrontare proattivamente tutte le questioni che dovessero sorgere in relazione al trattamento dei dati personali ed aiutano a rendere i processi aziendali più snelli ed efficaci.

Per quanto concerne i soggetti obbligati alla tenuta del registro dei trattamenti, come risulta dall'art. 30, paragrafi 2 e 3 ("*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*"**)** essi sono tanto il titolare quanto il responsabile del trattamento o, se presenti, i loro rappresentanti. Su entrambi incombe pertanto uno specifico dovere in tal senso, tenendo però conto che, dal punto di vista del contenuto, nel caso in cui il registro sia tenuto direttamente dal titolare del trattamento, o dal suo rappresentante, avrà una portata più estesa, invece qualora esso sia tenuto dal responsabile del trattamento, o dal suo rappresentante, dovrà indicare obbligatoriamente (ma ogni ulteriore informazione sarà sempre utile, nell'ottica del GDPR) solo:

- i contatti del titolare, del responsabile del trattamento e dei loro rappresentanti, se presenti, nonché del responsabile della protezione dei dati;
- le categorie di trattamenti effettuati per ciascun titolare del trattamento;
- il trasferimento dei dati ad un paese terzo (extra-europeo) o ad

un’organizzazione internazionale, specificando di quale paese o organizzazione si tratta ed evidenziando le adeguate garanzie previste per il trasferimento stesso;

- se possibile, la descrizione delle misure di sicurezza tecniche ed organizzative adeguate ai rischi preventivati.

Per completezza nell’esposizione, occorre precisare che il responsabile del trattamento (nel nuovo regolamento europeo data processor) è identificato nella persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento (art. 4, par. 1, n. 8 GDPR). E’ un soggetto, distinto dal titolare, che deve essere in grado di fornire garanzie al fine di assicurare il pieno rispetto delle disposizioni in materia di trattamento dei dati personali, nonché di garantire la tutela dei diritti dell'interessato. Ha una competenza qualificata dovendo garantire una conoscenza specialistica della materia, e l'attuazione delle misure tecniche e organizzative in grado di soddisfare i requisiti stabiliti dal regolamento europeo. Inoltre è necessario che garantisca una particolare affidabilità, un requisito fondato su aspetti etici e deontologici (ad esempio, l'assenza di condanne penali). Tratta i dati attenendosi alle istruzioni del titolare, assume responsabilità proprie e ne risponde alle autorità di controllo e alla magistratura**.**

Il titolare del trattamento invece rimane, a sua volta, responsabile della gestione effettuata dai responsabili, dovendo garantire che le loro decisioni siano conformi alle leggi, e in particolare il titolare deve ricorrere a responsabili che presentino garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del Regolamento (Considerando 81 GDPR). Compito specifico del titolare è, infatti, quello di valutare il rischio del trattamento che pone in essere tramite i responsabili e deve sempre poter sindacare le decisioni dei responsabili.

Nello specifico, dunque, la responsabilità formale della redazione, dell’aggiornamento e della corretta tenuta del registro resta comunque sempre in capo al titolare del trattamento e del responsabile del trattamento mentre il DPO deve fornire assistenza nella redazione e verificare la corretta tenuta dei registri, ma non ha alcuna responsabilità in merito.

Nessuna norma del GDPR prevede, poi, che un registro delle attività di trattamento sia

sottoscritto o vidimato, anche perché - come già accennato- la tenuta dei registri si basa sul principio dell'accountability.

E' consigliabile però che questo venga firmato dal legale rappresentante o da un responsabile della tenuta del registro (ove nominato) mentre il DPO potrebbe procedere al fianco del legale rappresentante ad un'ultima verifica, fornire supporto e consigli sulla redazione, provvedere ad informare i dipendenti dell'avvio del processo e di come dovranno comportarsi tutti i soggetti a vario titolo coinvolti.

Non viene inoltre fatta alcuna menzione sulla necessità di attribuire data certa ai registri delle attività di trattamento e al momento non ci sono dettami da parte del Garante Privacy, pertanto l'argomento sarà rimesso alla responsabilità dell'organizzazione e dunque la scelta sul modo più opportuno per avere una data certa sulle operazioni effettuate sui registri pertanto spetta a ciascun titolare o responsabile del trattamento; in ogni caso, l' utilizzo di software appositi che prevedono sistemi di accesso solo a persone autorizzate, permette di tenere traccia delle date e degli orari in cui ogni azione viene effettuata sui registri.

Il par. 5 del citato art 30 GPDR prevede, infine, in merito all'obbligo di adozione del registro trattamento dati che questo non competa "*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.*"

Il Working Party Article 29 (ora EDPB) ha pubblicato un parere sull'obbligo di tenuta del registro dei trattamenti nel quale precisa che è sufficiente che occorra una sola delle condizioni previste dall'articolo 30 per far scattare l'obbligo di tenuta del registro; per cui basterebbe trattare dati personali in modo stabile per essere tenuti alla registrazione dei trattamenti.

Terme ha effettuato una attenta analisi del caso ed attraverso una valutazione effettuata con l'ausilio di una checklist ad hoc ha verificato la sussistenza delle condizioni della obbligatorietà della tenuta del registro e lo ha adottato.

Modello.

In relazione a quanto sopra detto in tema di obbligatorietà del registro Terme dopo la

individuazione delle misure minime che lo stesso deve avere adotta il relativo modello/i per come si trova indicato nella parte attinente alla "Modulistica" del presente documento.

6) LE MISURE DI SICUREZZA

I riferimenti normativi

Sul tema il primo riferimento è contenuto nel disposto dell'art. 22 del GDPR, il quale dispone che il titolare del trattamento dei dati personali debba adottare delle misure tecniche e organizzative idonee al fine di assicurare, ed essere poi in grado di dimostrare, che il trattamento dei dati personali è realizzato in modo conforme alla disciplina dettata dal Regolamento stesso.

Questa norma è, in particolare, in linea con il principio della responsabilizzazione (c.d. accountability) che sta alla base del nuovo approccio promosso dal Regolamento europeo. Successivamente l'art. 32 del GDPR si occupa nello specifico della sicurezza del trattamento dei dati personali: "*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 per garantire un livello di sicurezza adeguato al rischio*"

In sostanza il titolare e il responsabile del trattamento dei dati personali dovranno predisporre ed attuare delle misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio. Come precisato poi dalle linee guida del Garante della Privacy in materia non sussistono più obblighi generalizzati di adozione di misure minime di sicurezza, come previsto dall'art. 33 del Codice in materia di protezione dei dati personali. Quindi l'indicazione fatta dal GDPR deve essere necessariamente considerata esemplificativa e non esaustiva e, in questo senso, aperta all'individuazione di altre diverse possibili misure ideate in base al contesto concreto in cui vengono poste in essere. Per fare questo essi dovranno tenere debitamente conto dell'attuale stato dell'arte (della tecnologica disponibile, dei sistemi informatici, ecc), dei costi di attuazione, della natura dei dati e dei meccanismi adottati, del campo di applicazione, del contesto e delle finalità del trattamento dei dati, oltre che del rischio

per i diritti e le libertà delle persone fisiche che può essere più o meno probabile e più o meno alto a seconda di ciascun diverso contesto.

Le misure

Su tali presupposti Terme provvede ad adottare misure che permettano:

- la pseudonimizzazione e la cifratura dei dati personali (ove ciò sia consentito dalla peculiarità dei dati trattati da Terme) nella parte in cui gli stessi attengono a dati di natura sanitaria;

- la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
- la verifica dell'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Pur non essendo più cogenti le misure ed gli strumenti operativi previsti nell'allegato B al Codice della Privacy, Terme ritiene che la indicazioni in essa contenute possano comunque essere un importante punto di riferimento operativo specialmente sotto gli aspetti che seguono da considerarsi esemplificativi e non esaustivi:

1) Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti

2. Le credenziali di autenticazione consistono in un codice per l´identificazione associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo , eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica, eventualmente associata a una parola chiave

3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione

4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la

diligente custodia dei dispositivi in possesso ed uso esclusivo dell´incaricato.
5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all´incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili la parola chiave è modificata almeno ogni tre mesi.
6. Il codice per l´identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati.

7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all´incaricato l´accesso ai dati personali.
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
10. Quando l´accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l´autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell´incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l´incaricato dell'intervento effettuato.

11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.
13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all´inizio del trattamento, in

modo da limitare l´accesso ai soli dati necessari per effettuare le operazioni di trattamento.

14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

15. Nell´ambito dell´aggiornamento periodico con cadenza almeno annuale dell'individuazione dell´ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

16. I dati personali sono protetti contro il rischio di intrusione e dell´azione di programmi di cui all´art. 615-*quinquies* del codice penale, mediante l´attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

19. I dati sensibili sono protetti contro l´accesso abusivo, di cui all´art. 615-*ter* del codice penale, mediante l´utilizzo di idonei strumenti elettronici.

20. Sono impartite istruzioni organizzative e tecniche per la custodia e l´uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

21. I supporti rimovibili contenenti dati sensibili se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

22. Sono adottate idonee misure per garantire il ripristino dell´accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

23. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il

trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all´articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all´identità genetica sono trattati esclusivamente all´interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all´esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

24. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l´intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell´ambito dell'aggiornamento periodico con cadenza almeno annuale dell´individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

25. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

26. L´accesso agli archivi contenenti dati sensibili è controllato. Le persone ammesse, a qualunque titolo, dopo l´orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

7) LA VIOLAZIONE DEI DATI . IL C.D. *DATA BREACH*

Indicazioni operative

La presente indicazione operativa ha lo scopo di descrivere il processo adottato dall'azienda Terme di Chianciano per la gestione degli eventi di violazione dei dati personali.

Essa pertanto si applica a tutti gli archivi/documenti cartacei e a tutti i sistemi sui cui

sono conservati i dati personali degli interessati (Utenti, dipendenti, fornitori, soggetti terzi ecc.) che l'azienda tratta, anche attraverso il supporto del / dei Responsabili del Trattamento e definisce le principali responsabilità ed attività relative agli obblighi di notifica verso gli Organismi di Controllo degli incidenti di Sicurezza delle Informazioni che abbiano come conseguenza la violazione di dati personali o che possano compromettere le libertà e i diritti dei soggetti interessati.
Ai sensi dell'art. 4 par. 12 del GDPR per *data breach,* (violazione dei dati personali) si intende "*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*".

Notifica del data breach

Secondo il GDPR, la notifica di eventuali violazioni di dati dovrà avvenire possibilmente senza ingiustificato ritardo e, ove possibile, entro 72 ore, dal momento in cui si è venuto a conoscenza della violazione, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. L'eventuale ritardo dovrà essere motivato.
A tale proposito, è stato introdotto dall'articolo 33, l'obbligo generalizzato, in capo al titolare del trattamento di notifica di *data breach* all'autorità di controllo (DPO) competente a norma dell'art. 55 GDPR e ss., ovvero l'Autorità di controllo. Le informazioni minime da inserire nella notifica sono incluse nell'art. 33.
Tale documentazione consente all'Autorità di controllo di verificare il rispetto delle prescrizioni.
La notifica deve:

- descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni
- descrivere le probabili conseguenze delle violazioni dei dati personali
- descrivere le misure adottate o di cui si propone l'adozione da parte del titolare

del trattamento per porre rimedio alla violazione dei dati personali e anche, per attenuarne i possibili effetti negativi.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Quando la violazione dei dati personali presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo. La comunicazione all'interessato descrive con un linguaggio semplice e chiaro la natura della violazione. Tale comunicazione non è richiesta all'interessato se:

- il titolare del trattamento ha messo in atto le misure tecniche ed organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- Il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

Detta ultima comunicazione richiederebbe tuttavia sforzi sproporzionati. In tale caso, si procede invece a una comunicazione pubblica o a una misura simile. Quindi la notifica all'Autorità è obbligatoria quando vi è un rischio probabile per i diritti e le libertà delle persone fisiche.

Nel caso in cui la notifica all'autorità di controllo non sia effettuata entro 72 ore dal momento in cui ne è venuto a conoscenza è possibile effettuarla in ritardo corredandola con i motivi del ritardo.

Se la notifica effettuata nelle 72 ore non sia completa è possibile integrarla in una o più fasi successive (ad es. nel caso di violazioni complesse per le quali occorrono indagini approfondite) corredandola con i motivi (analogamente come in caso di notifica in ritardo).

Nello specifico della notifica al Garante, dall' avvenuta conoscenza dell'evento, si dovrà recare, attraverso un modulo o comunicazione ad hoc, almeno, le seguenti informazioni:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie (clienti, dipendenti, categorie vulnerabili, minori, ecc.) e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni tipologie di record es numeri di passaporto, numeri di carte di credito, ecc.) dei dati personali in questione;
b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento o suo delegato per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
Inoltre, nel caso in cui la scoperta della violazione non sia contestuale al verificarsi dell'evento che l'ha generata, devono essere indicate nella comunicazione le motivazioni che non hanno consentito l'immediata rilevazione dell'evento stesso e le misure adottate o che si intende adottare affinché ciò non si ripeta in futuro.
Vi è inoltre l'obbligo di comunicazione senza ingiustificato ritardo all'interessato (cittadino, dipendente, soggetto terzo ecc.), quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.
La comunicazione a tali soggetti deve avvenire senza ingiustificato ritardo, il prima possibile.
Il Garante Privacy può autorizzare il differimento di tale comunicazione qualora quest'ultima rischi di compromettere gli accertamenti relativi al Data Breach.
La predetta comunicazione, infine, non è dovuta:
a) se si dimostra al Garante di aver applicato ai dati oggetto della violazione misure tecnologiche di protezione che li hanno resi inintelligibili a chiunque non sia autorizzato ad accedervi quali la cifratura;
b) il Titolare del trattamento o suo delegato ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati (ad esempio sono state immediatamente intraprese azioni contro colui che ha avuto acceso ai dati oggetto della violazione);
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli

interessati sono informati con analoga efficacia (ad es. in caso di perdita di documenti conservati solo in formato cartaceo potrebbero essere predisposte procedure o soluzioni tecniche che rendano le informazioni fruibili su richiesta degli stessi).

La gestione del data breach

Per poter valutare o meno la necessità di notificare la violazione dei dati al Garante e agli interessati qualora il rischio fosse elevato, è necessario, innanzitutto, procedere ad un'analisi dei rischi.

La probabilità e la gravità del rischio, per i diritti e le libertà dell'interessato, dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento.

Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato.

I criteri per valutare il rischio elevato, ai fini della comunicazione all'utente finale, dovranno basarsi su:

• il grado di pregiudizio che la violazione può comportare (danno alla reputazione, furto di identità ecc.);

• l'attualità dei dati (i dati più recenti potrebbero essere considerati più interessanti);

- la qualità dei dati coinvolti (dati sanitari, dati finanziari, dati giudiziari, credenziali di autenticazione);
- la quantità dei dati coinvolti;
- la tipologia di violazione (accesso non autorizzato, distruzione dei dati, perdita,furto);
- la capacità di identificare le persone coinvolte nella violazione.

Sarà ulteriormente necessario tenere presente le tre macro-categorie di *data breach* delineate dal WP29:

"Confidentiality Breach", in caso di accesso accidentale/abusivo ai dati personali;

"Availibility Breach", se vi è una perdita/distruzione accidentale o non autorizzata di dati personali;

"Integrity Breach", se siamo in presenza di alterazioni accidentali o non autorizzate dei dati personali.

Le comunicazioni interne fra le varie funzioni coinvolte nel processo di gestione delle violazioni dovranno essere inviate tramite i normali canali di comunicazione aziendale.

Il processo di gestione delle violazioni si articola nelle fasi di seguito descritte:

1) Segnalazione degli eventi di violazione dei dati personali

In questa fase si acquisisce la notizia di una possibile violazione di dati personali.

La segnalazione di un possibile *Data Breach* può provenire dall'esterno (cittadini, fornitori esterni, enti istituzionali ecc.) o dall'interno, da parte delle varie funzioni di settore durante il normale svolgimento dell'attività lavorativa anche se naturalmente è più frequentemente tali eventi vengono evidenziati da funzioni che svolgono attività di verifica e /o di controllo.

La segnalazione dovrà essere inviata al Responsabile del Trattamento e/o al DPO che si attiverà per acquisire elementi necessari per l'effettiva rilevazione del *Data Breach.*

2) Rilevazione degli eventi di violazione dei dati personali

In questa fase si acquisiscono gli elementi necessari per condurre la fase successiva di valutazione al fine di escludere o confermare la sussistenza del *Data Breach.*

Nella pratica, rilevazione e valutazione dell'evento sono interconnesse; ma è solo al termine della fase di valutazione che si considera accertata o meno la violazione dei dati personali. Da questo momento decorrono le tempistiche per la comunicazione al Garante.

Resta inteso che la fase di rilevazione deve avvenire in tempi brevi.

Se dalla prima analisi emergono elementi tali da escludere la possibile violazione dei dati personali, l'anomalia viene gestita secondo i processi aziendali standard. Se invece dalla prima analisi emergono gli estremi per una probabile violazione dei dati personali avviene una ulteriore fase istruttoria.

3) Valutazione degli eventi di violazione ai dati personali.

Scopo di questa fase è quello di confermare o meno l'avvenuta violazione, di circostanziare in modo completo l'evento e fornire una valutazione del possibile pregiudizio per i clienti.

Viene effettuata una analisi di dettaglio, si raccoglie informazioni aggiuntive e si valuta il livello di rischio dell'evento e il livello di pregiudizio per gli eventuali clienti impattati dalla violazione.

Ove dall'analisi non si ravvisi l'esistenza di una violazione, l'evento anomalo viene

gestito secondo le procedure aziendali vigenti.

Nel caso in cui, invece, dall'analisi, si accerti che l'evento costituisce una violazione dei dati personali, da questo momento decorrono le tempistiche previste dalla normativa (dal momento della conoscenza – 72 h) in tema di comunicazioni al Garante ed in questa fase si procede all'invio formale delle informazioni inerenti il *Data Breach* al Garante Privacy e, ove previsto, ai soggetti interessati dalla violazione.

Prima di procedere alla notifica della violazione ai soggetti interessati il testo della comunicazione, la modalità di notifica e le evidenze che attestano il reale livello di pregiudizio, dovranno essere validate dal Titolare del Trattamento o suo delegato.

La comunicazione dovrà descrivere con un linguaggio semplice e chiaro la natura della violazione.

Ad avvenuta segnalazione, si eseguirà in collaborazione con il DPO la procedura di valutazione del *data breach* e se ne analizzerà i risultati, in funzione del rischio e delle possibilità di mitigazione e rimedi perseguibili dall'azienda o dagli interessati. In particolare, si dovrà prontamente porre in essere le misure di mitigazione dei rischi già previste in fase di preparazione all'evento del *data breach.*

Terme ha effettuato, inoltre, una approfondita Analisi dei rischi per determinare i criteri per valutare il rischio elevato, ai fini della comunicazione all'utente finale, ed ha individuato i seguenti criteri cui attenersi:

- il grado di pregiudizio che la violazione può comportare (danno alla reputazione, furto di identità ecc.);
- l'attualità dei dati (i dati più recenti potrebbero essere considerati più interessanti);
- la qualità dei dati coinvolti (dati sanitari, dati finanziari, dati giudiziari, credenziali di autenticazione);
- la quantità dei dati coinvolti;
- la tipologia di violazione (accesso non autorizzato, distruzione dei dati, perdita, furto);
- la capacità di identificare le persone coinvolte nella violazione.

Su tali presupposti in caso di violazione il DPO provvederà alla valutazione del singolo caso e determinerà la sussistenza o meno del c.d. rischio elevato e provvederà a comunicare al titolare del trattamento la sua valutazione per permettere al titolare medesimo ogni consequenziale provvedimento

Il registro delle violazioni

Il processo di *data breach* si conclude con la tenuta del registro delle violazioni.

Ai sensi del dell'art 33 par. 5 "*Il titolare del trattamento documenta qualsiasi violazione dei dati personali comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.*

Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo".

L'azienda è pertanto tenuta ad adottare un registro / inventario aggiornato delle violazioni contenente tutte le informazioni necessarie a chiarire le circostanze nelle quali si sono verificate, le conseguenze che le stesse hanno avuto e i provvedimenti adottati per porvi rimedio, la tenuta di tale inventario consente al Garante di verificare il rispetto delle disposizioni di legge. E' comunque opportuno che l'inventario tenga traccia anche delle varie fasi di gestione dell'evento, dalla rilevazione, all'analisi e alla sua risoluzione e conclusione. L'inventario dovrà essere dotato di idonee misure di sicurezza atte a garantire l'integrità e l'immodificabilità dei dati in esso registrati.

Nel registro saranno annotate tutte le informazioni richieste dalla normativa vigente, quali, ad es.: (a) le circostanze relative alla violazione; (b) le conseguenze; (c) i provvedimenti adottati per contrastarla e limitarne gli effetti; (d) i dati personali coinvolti, etc.

Tipologie di violazioni dei dati.

Le violazioni dei dati personali si considerano tali se hanno un reale impatto sulla confidenzialità, integrità o disponibilità dei dati personali degli interessati (cittadini, dipendenti, soggetti terzi ecc.)

Di seguito una breve descrizione delle varie tipologie di violazione dei dati personali:

a) Distruzione: Indisponibilità definitiva di dati personali dei clienti con impossibilità di ripristino degli stessi entro sette giorni. La violazione può essere determinata da una eliminazione logica (es. cancellazione dei dati) oppure fisica (es. rottura dei supporti di memorizzazione) non autorizzata e relativa impossibilità di ripristinare i dati entro i sette giorni.

b) Perdita: Perdita del supporto fisico di memorizzazione dei dati (dischi esterni, pendrive ecc.) in termini di privazione, sottrazione, smarrimento dei dispositivi

contenenti i dati degli interessati oppure dei documenti cartacei. La perdita può essere anche temporanea ma superiore a sette giorni. Può riguardare le copie o gli originali dei supporti contenenti i dati personali dei soggetti interessati.

c) Modifica: Modifiche improprie dei dati degli interessati non autorizzate, effettuate al di fuori dei processi operativi di trattamento dei dati svolti dagli incaricati autorizzati, oppure modifiche con finalità fraudolente eseguite dagli incaricati autorizzati all'accesso.

d) Rivelazione: Distribuzione non autorizzata o impropria dei dati personali degli interessati verso terze parti (persone fisiche, persone giuridiche, gruppi di soggetti, pubblico) anche non precisamente identificabili.

e) Accesso: Accesso non autorizzato o improprio ai dati degli interessati. Accessi ai dati (anche in sola visualizzazione, sia in caso di accessi logici ai sistemi informatici sia agli archivi cartacei) effettivamente avvenuti al di fuori dei processi operativi di trattamento dei dati previsti e autorizzati.

Tassonomia eventi

Terme ha individuato, in maniera esemplificativa e non esaustiva, una tassonomia dei possibili eventi causa delle violazioni dei dati personali.

a) Trattamenti elettronici

- Eventi accidentali -

Eventi anomali determinati da fatti fortuiti che causano la perdita delle caratteristiche di sicurezza dei dati personali dei clienti (confidenzialità, integrità o disponibilità) in caso di trattamenti informatizzati. Rientrano in tali casistiche eventi generati nella gestione dei sistemi gestiti internamente oppure in outsourcing quali:

Esecuzione erronea di comandi e/o procedure per distrazione: ad esempio pubblicazione erronea delle informazioni personali (non di dominio pubblico) su portali web pubblici; erroneo invio di dati; divulgazione accidentale di credenziali di accesso a colleghi o personale non autorizzato ecc.

Rottura delle componenti HW: a titolo di esempio distruzione dei supporti di memorizzazione a causa di sbalzi di temperatura e di elettricità, umidità, corto circuito, caduta accidentale, eventi catastrofici/incendi, ecc.

Malfunzionamenti Software: ad esempio esecuzione di uno script automatico non autorizzato; errori di programmazione che causano output errati, ecc.

Visibilità errata di dati sul sito web: ad esempio visibilità da parte di clienti di dati di altri clienti anche per casi di omonimia.

Fornitura dati a persona diversa dall'interessato: a titolo di esempio comunicazioni di dati di interessati a destinatari errati; gestione di informazioni avanzate da persone diverse dal Titolare o suo delegato;

Guasti alla rete aziendale: a titolo di esempio caduta delle comunicazioni durante il trasferimento di dati e perdita di dati durante la trasmissione, etc.

- Eventi dolosi -

Eventi dolosi causati da personale interno o soggetti esterni realizzati tramite:

- accesso non autorizzato ai dati con lo sfruttamento di vulnerabilità dei sistemi interni e delle reti di comunicazione;

- compromissione o rivelazione abusiva di credenziali di autenticazione; -utilizzo di software malevolo. In tale casistica rientrano gli incidenti di sicurezza che comportano la violazione dei dati personali dei clienti quali:

Furto: furto di supporti di memorizzazione e/o elaborazione contenenti dati personali dei clienti (es: furto laptop, hard disk, chiavette USB, smartphone, tablet ecc)

Truffa informatica esterna: tutti i casi di frodi realizzate da un soggetto esterno all'azienda rivolto a procurare a sé o ad altri un profitto o, comunque, un vantaggio in termini economici, pubblicitari, ideologici/politici, qualora tali frodi causino perdita delle caratteristiche di sicurezza dei dati personali dei soggetti interessati (confidenzialità, integrità o disponibilità)

Truffa informatica interna: tutti i casi di frodi realizzate da personale interno all'azienda che comportano la violazione dei dati personali. Tali eventi possono derivare dall'utilizzo illecito e/o illegittimo delle informazioni a cui un incaricato del trattamento accede anche se autorizzato.

b) Trattamenti Cartacei -

- Eventi accidentali

Eventi anomali causati nell'ambito dei trattamenti non automatizzati effettuati su archivi cartacei dei dati personali dei clienti dell'ente/organizzazione quali:

- Distruzione accidentale di documenti: ad esempio incendio/ allagamento dei locali dove sono presenti archivi cartacei, causati da eventi fortuiti e non dolosi presso le sedi di Terme, dei partners commerciali e dei locali, degli outsourcers , dei partners cessati dai quali si attende la restituzione della documentazione contrattuale;

distruzione per errore di documenti originali, senza eventuale copia, da parte di dipendenti interni, di partners commerciali.

- Smarrimento di documenti: ad esempio perdita di documenti contenenti dati degli interessati;

- Fornitura involontaria di dati a persona diversa dal contraente: ad esempio tramite invio lettera , gestione ed evasione reclami/richieste di informazioni avanzate da persone diverse dal titolare, comunicazione di dati dal subentrato al subentrante e viceversa.

- Eventi dolosi -

Comportamenti dolosi da parte di personale interno o soggetti esterni realizzati, attraverso accessi non autorizzati, nell'ambito di trattamenti effettuati su archivi cartacei di dati personali e/o soggetti collegati/controllati quali:

- Distruzione dolosa dei documenti: ad esempio incendio doloso provocato da personale interno o soggetti esterni che rende indisponibile in modo definitivo i documenti contenenti dati dei clienti; accesso non autorizzato da parte di terzi ad archivi interni della Società e distruzione volontaria di documenti contenenti dati dei clienti.

- Accesso non autorizzato: ad esempio accesso non autorizzato da parte di personale interno o soggetti esterni, con lettura e/o copia dei documenti, ad archivi documentali presso le sedi di Terme, dei partners commerciali. Non si verifica violazione se si ha la ragionevole certezza che non vi è stata lettura o copia dei documenti contenenti dati degli interessati.

- Furto (cartacei): Furto da parte di personale interno o soggetti esterni (o non identificati) di documenti cartacei contenenti dati dei soggetti interessati.

Esempi

Esempi riportati nel documento WP 250 edito dal Gruppo dei Garanti europei ex art.29.

Esempio 1

Viene effettuato un back up di un archivio di dati personali su una chiavetta USB criptata. La chiavetta viene rubata. Notifica della data breach al Garante? NO Notifica della data breach all'interessato?NO

Esempio 2

Gestione di un servizio on line agli utenti. A seguito di un attacco hacker contro tale servizio, i dati degli utenti vengono diffusi. Notifica al Garante? SI, poiché vi è un probabile rischio per i diritti e le libertà degli interessati (gli utenti del servizio i cui dati sono diffusi a seguito dell'attacco). Notifica all'interessato? SI, laddove vi sia un rischio elevato per i diritti e le libertà degli interessati (gli utenti del servizio i cui dati sono diffusi a seguito dell'attacco), in base alla natura dei dati oggetto dell'attacco e alle conseguenze.

Esempio 3

Si subisce un attacco di tipo ransomware che determina il blocco e la crittografia di tutti i suoi dati sui sistemi. Non sono disponibili back-up e i dati non possono dunque essere ripristinati. Dopo le opportune verifiche e investigazioni, risulta che lo scopo del ransomware è esclusivamente quello di crittografare i dati e che nessun malware è presente nei sistemi. Notifica della data breach al Garante? SI, in quanto vi è una data breach rappresentata da una perdita di disponibilità dei dati personali che impatta sugli interessati. Notifica della data breach all'interessato? SI, in quanto vi è una data breach rappresentata da una perdita di disponibilità dei dati personali che impatta sugli interessati.

Esempio 4

Per errore di un addetto del Titolare del trattamento le schede anagrafiche dei partecipanti a un corso di formazione sono trasmesse ad una mailing list errata di più di mille destinatari. Notifica della data breach al Garante? SI. Notifica della data breach all'interessato? SI. Va comunque valutato il livello di gravità la severità delle conseguenze dell'errato invio.

Esempio 5

Una email di direct marketing è inviata in copia palese e non nascosta a molti destinatari, che dunque possono vedere i recapiti di posta elettronica di ciascun destinatario in copia. Notifica della data breach al Garante? SI, ma nel caso in cui sia coinvolto un elevato numero di interessati, vi sia una natura delicata dei dati, o il contenuto del messaggio sia rischioso (es: invio del primo pin o password per accedere a un servizio). Notifica della data breach all'interessato? SI.

Modello di comunicazione al Garante

In relazione alla comunicazione al Garante di cui ai punti che precedono Terme dopo

la individuazione delle misure minime che la comunicazione deve avere adotta il relativo modello per come si trova indicato nella parte attinente alla “Modulistica” del presente documento.

8) SITO INTERNET

Analisi

L'analisi della situazione complessiva di Terme ha preso in considerazioni anche le modifiche / integrazioni che si rendono necessarie al sito internet ufficiale di Terme al fine di utilizzare lo stesso per la funzione di rendere ancora più trasparente la informativa sul tema della privacy in relazione a tutti i soggetti, sia interni che interni, che ne sono interessati sia sotto l'aspetto soggettivo attivo che passivo.

Si ritiene, sotto tale punto di vista, che lo stesso sito deva contenere, in un apposito settore dello stesso, con evidenza pari a quello della altre “pagine” in esso contenute, la indicazione di una voce denominata PRIVACY che, aperta, contenga a sua volta la indicazioni delle seguenti sottovoci con i relativi contenuti/modelli:

Informativa privacy

All'interno di tale voce dovrà essere contenuta luna informativa di carattere generale secondo il modello che si trova allegato nella parte denominata “Modulistica” del presente documento

Regolamento Europeo

Al fine di permettere una facile e veloce consultazione della normativa di riferimento si ritiene necessario che venga riportato per esteso il Regolamento Europeo di riferimento o comunque un link che permetta l'accesso immediato ad una pagina diversa che contenga la detta normativa.

Codice deontologico e di condotta

La esplicazione all'esterno dei principi di comportamento che Terme di è dati è molto importante nei confronti degli interessati. Si dovrà allegare il Codice che si trova, nella sua interezza, nella parte della “Modulistica” del presente documento.

Informativa clienti/fornitori

Vedi modello allegato nella parte “Modulistica”

Informativa videosorveglianza

Vedi modello allegato nella parte “Modulistica”

Modello Organizzativo privacy

Si tratta della indicazione della strutturazione “aziendale” in tema di politica/*governance* sulla privacy.

Vedi modello allegato nella parte “Modulistica”

Modelli per l'esercizio dei diritti degli interessati

Al fine di permettere il corretto esercizio dei diritti degli interessati nei confronti di Terme dovranno essere allegati i modelli (riportati anch'essi nella parte della “Modulistica”) relativi a:

a) Dichiarazione consenso

b) Richiesta di accesso

c) Richiesta revoca

d) Richiesta rettifica

e) Limitazione consenso

Contatti

In tale voce dovranno essere analiticamente indicati i nominativi del DPO, dei Responsabili del Trattamento, degli Incaricati (ove esistenti) gli estremi del Titolare del Trattamento (sede, indirizzo, Cod. Fiscale, partita IVA) e comunque di tutte le figure anche successivamente nominate che hanno funzioni/incarichi in tema di privacy, con il relativo indirizzo di posta elettronica e/o telefono dove essere contattati.

9) GLOSSARIO

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
Raccolta di dati personali organizzati in un insieme ordinato e indicizzato (indipendentemente dal fatto che sia elettronico o manuale).

Autorità di controllo
Una o più autorità pubbliche indipendenti che hanno il compito di assicurarsi il rispetto delle nuove norme sulla privacy, in ogni paese membro.

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;

Dati biometrici
Categorie particolari di dati personali, ottenuti da tecnologie in grado di rilevare in modo automatizzato una o più caratteristiche biologiche e/o comportamentali (biometria) di una persona fisica.

Dati genetici
Tutti quei dati personali relativi alle caratteristiche genetiche (ereditarie o acquisite) che risultino dall'analisi di un campione biologico della persona fisica in questione.

Dati personali
Un dato personale è qualsiasi informazione che identifica (o rende identificabile) direttamente o indirettamente una persona fisica.

Dati personali "sensibili" (Categorie particolari di dati personali)

Sono dati personali per i quali sono richieste particolari cautele. Possono rilevare l'identità della persona attraverso elementi biometrici o genetici, oppure attraverso la sua posizione (dati geolocalizzati) oppure sono legati ad altri aspetti quali: l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Dati relativi alla salute
Tutti 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.

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.

Diritto alla portabilità
L'interessato ha il diritto di richiedere i propri dati personali e poterli trasferire da un titolare all'altro.

Diritto alla rettifica
L'interessato ha la possibilità di richiedere, in qualsiasi momento, la modifica dei propri dati personali qualora questi risultino inesatti.

Diritto alla cancellazione (c.d. all'oblio)
L'interessato ha la possibilità di richiedere la totale cancellazione dei propri dati personali presso un determinato titolare del trattamento.

Diritto di accesso
L'interessato ha il diritto di richiedere e ottenere, al titolare del trattamento, la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano, con una descrizione esatta delle modalità e finalità. L'accesso al dato può avvenire da remoto oppure chiedere una copia.

Diritto di opposizione
L'interessato ha la possibilità di opporsi, in qualsiasi momento e per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano.

GDPR

Regolamento generale per la protezione dei dati personali *n. 2016/679 (General Data Protection Regulation)*

Informativa
La comunicazione che fornisce tutte le informazioni utili che l'interessato deve sapere nel momento in cui decide di dare il suo consenso al trattamento dei dati personali.

Interessato
Persona fisica a cui si riferiscono i dati personali oggetto del trattamento, che può essere identificata o identificabile (cioè può essere identificata anche in modo indiretto) attraverso il trattamento stesso.

Limitazione di trattamento
Sospensione temporanea (che può trasformarsi in permanente) del trattamento dei dati in corso, per i quali è consentita solo la conservazione. I

Profilazione

Raccolta di informazioni su un individuo al fine di effettuarne una valutazione automatizzata, attraverso l'analisi delle sue caratteristiche comportamentali e l'inserimento dello stesso in categorie o gruppi.

Pseudonimizzazione
Detta anche cifratura, consiste nel modificare e mascherare i dati personali e sensibili di una persona fisica per non permetterne l'identificazione diretta, se non utilizzando informazioni aggiuntive. I

Responsabile del trattamento
Qualsiasi soggetto che tratta i dati personali del Titolare del trattamento in suo nome e conto.

Responsabile della protezione dei dati (DPO)
L'RPD o DPO (Data Protection Officer) è una figura (obbligatoriamente prevista solo in alcuni casi) che svolge il ruolo di supervisionare i processi relativi al trattamento dei dati personali.

Terme.
Si tratta della abbreviazione che intende individuare le Terme di Chianciano Spa con sede in Chianciano Terme (Siena) Via delle Rose 12 CF. P. IVA 01152750525

Titolare del trattamento
È il proprietario dei dati personali, ed è colui che ne definisce le modalità di trattamento, decidendo tutte le misure tecniche e organizzative.

Trattamento
Si definisce come trattamento qualunque operazione svolta sui dati personali con o senza l'ausilio di strumenti elettronici, che riguarda la raccolta dei dati, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, il blocco, la modifica, l'utilizzo, l'interconnessione, la comunicazione, la diffusione, la cancellazione, la distruzione, la selezione, l'estrazione, il raffronto dei dati personali degli interessati

Violazione dei dati personali (data breack)
Violazione dei dati personali presenti in un determinato database, perchécopiati, trasmessi, consultati o utilizzati da soggetti non autorizzati a farlo. Si tratta di un evento che può comportare diversi livelli di rischio per gli interessati, in base alla tipologia di dato oggetto della violazione e alle libertà personali che possono essere compromesse. In base alla gravità dell'evento, può essere necessario fare o meno una comunicazione al Garante.