

RAPPORTO AUDIT

**MODELLO DI GESTIONE PRIVACY PER LA PROTEZIONE DEI
DATI PERSONALI AI SENSI DEL GDPR N. 2016-679
VALUTAZIONE DI IMPATTO: ANALISI E GESTIONE DEL
RISCHIO**

Thesis Group S.r.l.

Indice

PREMESSA

PARTE I

Sistema Privacy: nuovo Regolamento europeo n. 2016-679. Tipologia di dati personali trattati da Thesis Group S.r.l.

Figure Privacy – Atti di nomina

a) Titolare del trattamento dei dati

b) Responsabile del trattamento dei dati: dott.ssa Stefania Meroni

c) Responsabile della Protezione dei dati personali: Avv. Andrea Cantoni

d) Incaricato del trattamento dei dati personali

Informativa e acquisizione del consenso al trattamento dei dati personali

Esercizio dei diritti di cui all'art. 15 Reg. Eu n. 679-2016

4. Privacy Policy del sito web

- tipologia dei dati personali trattati sul sito web e finalità del trattamento

- Facoltatività del conferimento dei dati

- Luogo di trattamento dei dati

- Titolare del trattamento

Dati personali trattati tramite sistema di videosorveglianza

PARTE II

Analisi del rischio e misure di sicurezza

Misure a tutela dell'integrità e disponibilità dei dati personali

La protezione di aree e locali

Custodia, archiviazione dei dati e analisi del rischio informatico

Accesso ai dati e istruzioni

Protezione di strumenti e dati

Supporti rimovibili

Criteri di ripristino dei dati

Controllo generale sullo stato della sicurezza

Interventi formativi

Esito rapporto AUDIT

Thesis Group S.r.l.

Premessa

La tutela per la protezione dei dati personali (*Data Protection*) ha trovato la sua piena realizzazione in un nuovo quadro normativo: il 04 maggio 2016 è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il Regolamento UE n. 2016-679 (indicato con acronico GDPR) del Parlamento Europeo e del Consiglio, relativo alla tutela e protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Il Regolamento europeo nasce dalla consapevolezza, ormai, che l'evoluzione tecnologica, gli strumenti impiegati e la globalizzazione comportano nuove sfide per la protezione dei dati personali; il possesso di strumenti tecnologici potenti e sofisticati, ma anche facili da utilizzare da chiunque (si pensi ad es. all'utilizzo di uno smartphone con accesso ai social network) consentono di gestire quantità di dati personali in misura elevata, ma vi è necessità che chiunque ne faccia utilizzo abbia una chiara e precisa consapevolezza sui rischi ad essi connessi.

Il Regolamento Europeo, a cui imprese private, Enti, Pubblica Amministrazione e studi professionali dovranno conformarsi entro la data del 25 maggio 2018, introduce da un lato nuove figure professionali con specifica preparazione in materia di tutele dei dati personali (es. Amministratore di sistema, il D.P.O. *Data Protection Officer*; peraltro figura non obbligatoria per soggetti privati), impone nuove analisi sui rischi (il cd *data protection impact assessment*), dall'altro predispone un sistema normativo improntato ad aumentare il senso di responsabilità di chi tratta i dati personali (viene introdotto il **principio di accountability**¹ all'art. 5, comma 2 del Regolamento).

La *ratio legis* della tutela dei dati personali delle persone fisiche (familiarmente conosciuto come tutela della privacy) risiede nel fatto che il trattamento dei dati è un diritto fondamentale della persona in quanto intrinsecamente connesso al diritto della riservatezza e della propria identità personale².

1 In virtù di questo principio il Regolamento dispone che il Titolare del trattamento dei dati adotti politiche interne e adotti misure adeguate per garantire ed essere in grado di dimostrare che il trattamento dei dati personali effettuato sia conforme allo stesso Regolamento. Il termine anglosassone – tradotto con espressione “responsabilità” - fa riferimento alla necessità in capo al titolare del trattamento di introdurre meccanismi di responsabilizzazione interna, mediante l'elaborazione di un idoneo sistema documentale di gestione della privacy, attraverso l'adozione di specifici modelli organizzativi, analoghi a quelli utilizzati nell'applicazione della disciplina di cui al D. Lgs. n. 231-2001.

2 Stefano Rodotà, già Presidente dell'Autorità, ha scritto *“la tutela della privacy si è sempre più strutturata come diritto di ogni persona al mantenimento del controllo sui propri dati”*.

Thesis Group S.r.l.

Rispetto alla disciplina contenuta nella Direttiva n. 95/46/CE, oggi non più vigente in quanto abrogata, il Regolamento (UE) n. 679/2016 presenta un capovolgimento di prospettiva destinando la parte più significativa della disciplina a tutela della riservatezza non più ai diritti dei *data subjects* (gli interessati), ma ai doveri dei Titolari e dei Responsabili del trattamento e alle misure di sicurezza adottabili o da adottare alla luce del nuovo approccio. Approccio che fin da subito si impone nel riservare alle misure un livello adeguato di sicurezza (per definizione più elevato del livello minimo assicurato dalle misure di sicurezza del Codice). L'art. 32, comma 1, del Regolamento prevede al riguardo che “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”. **Il legislatore europeo sembra aver fatto già le sue prime valutazioni quando dispone per un nucleo minimo di misure che rispondono a criteri di sicurezza predefiniti e che puntano sicuramente a bilanciare in maniera adeguata il rischio a contrasto del quale vengono chiamate.** Tra esse comprende:

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

Al di là di ciò, l'art. 32 del Regolamento fin dal suo esordio chiarisce il ruolo del Titolare del trattamento (e per esso del Responsabile) chiamato a mettere in pratica le misure di sicurezza valutandone, in via preventiva, ma anche successiva, all'instaurazione del trattamento, l'adeguatezza in ragione di parametri dinamici per definizione, rispettando comunque i livelli predefiniti dal legislatore.

ovunque essi si trovino, così riflettendo la nuova situazione nella quale ogni persona cede continuamente, e nelle forme più diverse, dati che la riguardano” Il mondo della rete. Quali diritti, quali vincoli, Laterza, Roma 2014.

Thesis Group S.r.l.

La valutazione del rischio, pertanto, diventa un passaggio fondamentale nella gestione e nell'organizzazione delle risorse associate ai trattamenti posti in essere. Tanto che il Regolamento si spinge a proceduralizzarne l'obbligo soprattutto nei casi in cui i trattamenti medesimi si presentino particolarmente pericolosi per i diritti e le libertà degli interessati o il rischio che ne derivi sia particolarmente elevato (cfr. artt. 35 e 36 del Regolamento)³. **L'analisi dei rischi e la valutazione di impatto per la sicurezza dei dati personali è destinata a diventare, in sostanza, una buona prassi che il Titolare del trattamento deve adottare sia all'atto in cui essa viene posta in essere, sia nel suo svolgimento che, addirittura, alla sua cessazione;** e questi deve essere in grado di dimostrare (*in primis* all'Autorità di controllo) che le misure organizzative adottate siano conformi alle prescrizioni del Regolamento così come le misure di sicurezza, che devono rimanere efficaci e adeguate per tutta la durata del trattamento. La necessità di assicurare trasparenza nelle operazioni del trattamento dei dati personali, soprattutto quelli di tipo sanitario (ossia trattamento effettuato per finalità di prevenzione, diagnosi, cura e riabilitazione del paziente) e adeguata protezione degli stessi impone al titolare del trattamento (e per esso il Responsabile del Trattamento) precise valutazioni di impatto privacy.

A tal fine la valutazione del rischio deve prevedere:

- a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento;
- b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità ;
- c) una valutazione dei rischi per i diritti e le libertà degli interessati;
- d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento europeo, tenuto conto dei diritti e degli interessi legittimi degli interessati.

I rischi relativi ad una organizzazione aziendale si possono raggruppare in queste tipologie base:

3 L'analisi del rischio deve rientrare come processo preventivo al trattamento dei dati personali di una azienda: la valutazione di impatto del trattamento sulla protezione dei dati è a carico del Titolare del trattamento e deve essere effettuata quando un tipo di trattamento, allorchè prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche (cfr. paragrafo n. 35 del Reg. UE n.679-2016).

Thesis Group S.r.l.

1) rischi strategici, 2) rischi operativi, 3) rischio di mancata compliance, 4) rischio privacy.

I rischi di mancata compliance impattano direttamente sull'organizzazione aziendale che tratta i dati, mentre quelli privacy riguardano la persona interessata dei cui dati si tratta; nella realtà queste due tipologie di rischio non si presentano così nettamente separate ma fortemente intrecciate.

Il rischio di mancata compliance è quella che deriva dalla non ottemperanza alle leggi o a norme prescrittive: gli eventi che portano a tali rischi possono derivare dalla mancata conoscenza della norma o dalla consapevole omissione. L'inosservanza può avere la conseguenza di incorrere in sanzioni giudiziarie o amministrative, perdite finanziarie, danni di reputazione, ecc. ecc..

Nel caso di non conformità alla normativa in ambito privacy in senso stretto, il rischio sarà quello delle conseguenze di un reclamo, una segnalazione o un ricorso alla Authority da parte del soggetto interessato che lamenta una violazione di propri dati personali, oppure, ancora, il Garante sulla base di un'ispezione potrà stabilire che i dati sono trattati in violazione di legge con conseguente divieto o restrizione dei trattamenti.

Il rischio di trattamento illecito dei dati personali di un soggetto interessato può avvenire a seguito dei seguenti eventi, che il presente rapporto di AUDIT intende prevedere e prevenire con le misure tecniche ed organizzative in adozione presso la Thesis Group S.r.l.:

- distruzione o perdita, anche accidentale, dei dati;
- indisponibilità dei dati per un periodo significativo;
- accesso non autorizzato ai sistemi informatici in essere presso i locali aziendali o ad aree contenenti archivi;
- trattamento di dati non lecito o non conforme alle finalità indicate;
- modifica dei dati personali in conseguenza di interventi non autorizzati o non conformi alle regole.

Dunque, l'analisi preliminare dell'impatto privacy impone di valutare gli aspetti relativi alla protezione dei dati, di adottare misure appropriate per minimizzare i rischi e adottare ogni altra misura organizzativa tecnica e giuridica.

Thesis Group S.r.l.

Solo attraverso una corretta e precisa valutazione dell'impatto privacy permette di adottare un efficace modello di gestione del sistema privacy.

PARTE I

Tipologia di dati trattati (dati comuni e dati sanitari dei pazienti).

La società Thesis Group S.r.l., P. IVA 09702130965, con sede legale in Milano Via Mac Mahon n. 2, in persona del legale rappresentante *pro tempore* nonché Amministratore Unico dott.ssa Roberta Cossutta, nata a Milano il 17 luglio 1967, C.F. CSSRRT67L57F205U, è Titolare del trattamento dei dati personali.

La Thesis Group S.r.l. svolge, come meglio descritto nell'atto costitutivo della società, attività di prevenzione, cura, accoglienza, sostegno psicologico, riabilitazione attraverso tutte le azioni terapeutiche individuali e di gruppo rivolte al singolo, alla famiglia e a gruppi sociali sia lavorativi sia di altra natura; ogni attività che compie viene svolta attraverso la gestione di servizi riabilitativi e di accoglienza, assistenza qualificata anche a domicilio o presso strutture residenziali, semi-residenziali, in case protette, in caso di degenza in ospedale o in caso di cura, di assistenza infermieristica, nonché in comunità alloggio e terapeutiche, in comunità di convivenza e centri di aggregazione; procede al compimento di operazioni necessarie per l'erogazione dei servizi stessi a favore di anziani, disabili, soggetti con handicap o socialmente svantaggiati, ospiti di centri socio educativi o centri di assistenza polivalenti.

Nell'ambito della propria attività, la Thesis Group S.r.l., tratta numerosi dati personali, non solo quelli cd comuni, bensì anche quelli particolarmente sensibili, ossia i dati sanitari dei propri pazienti.

Da Thesis Group S.r.l. vengono raccolti ed elaborati dati che concernono:

- a) dati personali (c.d comuni) dei propri pazienti (es. nome, cognome, cod. fiscale, data nascita, residenza, numeri recapiti telefonici);
- b) dati sanitari dei propri pazienti (contenuti nelle relative cartelle cliniche);
- c) dati personali dei fornitori;
- d) dati personali (cd. comuni) dei soci cooperatori (es. nome, cognome, cod. fiscale, data nascita, residenza, numeri recapiti telefonici);

Thesis Group S.r.l.

- e) dati personali sensibili dei soci cooperatori (es. iscrizione a rappresentanze sindacali, iscrizione a Sindacati o partiti politici, n°matricola, dati relativi a infortuni e/o malattia professionale, ecc.);
- f) dati personali dei tirocinanti delle scuole secondarie o universitarie
- g) dati personali degli stagisti,

tutti richiesti per le diverse finalità correlate alla erogazione dei servizi relativi all'attività svolta dalla Onlus (indicata nell'oggetto sociale di cui all'atto costitutivo) e per l'adempimento degli obblighi di legge e che la società tratta nell'ambito delle attività ai fini dell'inserimento, accesso, elaborazioni, modifica con strumenti sia elettronici (personal computer) sia non elettronici⁴.

Thesis Group S.r.l. con il presente documento pone in essere un rapporto di AUDIT interno per conformarsi alla normativa del Regolamento Europeo n. 2016-679 al fine di assicurare la corretta progettazione ed implementazione di un modello di gestione privacy, con l'adozione di misure tecniche ed organizzative in grado di ridurre sensibilmente i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta dei dati stessi.

Coadiuvata dal professionista di fiducia incaricato, Avv. Andrea Cantoni, di predisporre e redigere l'AUDIT, Thesis Group S.r.l.:

- **ha censito accuratamente i dati personali trattati,**
- **ha definito ed indicato le cd. figure privacy ed i rispettivi profili di responsabilità,**
- **ha predisposto idonee informative privacy complete per raccogliere il consenso informato dei soggetti interessati;**
- **ha altresì valutato l'impatto del *risk assessment* delle tecnologie adottate e preso idonee misure di sicurezza per la i sistemi informatici utilizzati;**
- **ha predisposto un registro trattamento dei dati ex art. 30 del GDPR, in formato elettronico Excel.**

L'attività di *impact privacy assessment* viene richiesta dall'art. 35 del Regolamento UE 2016-679 che prevede: *"1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le*

⁴ Per le banche dati trattate mediante supporti elettronici vengono utilizzati personal computer e server con accesso tramite dispositivo elettronico di sicurezza e dotato di programma anti-intrusione e antivirus.

Thesis Group S.r.l.

finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

2. Il titolare del trattamento, allorché svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.

3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti: a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche; b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

4. L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.

5. L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato. 6. Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione.

7. La valutazione contiene almeno: a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento; b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e d) le misure previste

Thesis Group S.r.l.

per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

8. Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.

9. Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.

10. Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.

11. Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.”

Il sistema Privacy implementato da Thesis Group S.r.l. vuole raggiungere e sviluppare standard di sicurezza elevati nel pieno rispetto dei seguenti principi di cui all'art. 5 del Regolamento UE 2016-679:

- riconoscimento dei dati personali come diritto fondamentali delle persone e ne accorda tutela a tutti;
- principio della finalità e proporzionalità, in base ai quali i dati vengono trattati solo se indispensabili e per finalità specifiche indicate nelle specifiche informative necessario per la raccolta del consenso;

Thesis Group S.r.l.

- i dati sono trattati in modo lecito, trasparente e corretto, conformemente alle disposizioni di legge vigenti, in maniera esatta da consentirne il necessario aggiornamento;
- i dati sono trattati in modo da assicurarne la adeguata sicurezza contro i rischi di accessi non autorizzati o contro il rischio di perdita dei dati stessi

Thesis Group S.r.l. adotta il presente Sistema Privacy per assicurare a terzi un modello di gestione affidabile e coerente con le finalità dei trattamenti dei dati raccolti e per garantire all'interno della propria organizzazione procedure atte a responsabilizzare il Titolare dei trattamenti (c.d principio di *accountability*).

Figure Privacy⁵

a) Titolare del trattamento dati: Thesis Group S.r.l..

E' riconosciuto a livello normativo del GDPR n. 679-2016 che una *condicio sine qua non* per un corretto trattamento dei dati personali sia in primo luogo l'individuazione di determinate specifiche figure, a cui ricollegare certe responsabilità e certi attribuzioni.

Il Titolare del trattamento dei dati è la società Thesis Group S.r.l., P. IVA 09702130965, con sede legale in Milano Via Mac Mahon n. 2, in persona del legale rappresentante *pro tempore* nonché Amministratore Unico dott.ssa Roberta Cossutta, nata a Milano il 17 luglio 1967, C.F. CSSRRT67L57F205U.

Il trattamento dei dati personali è affidato solo al Titolare del trattamento attraverso il suo legale rappresentante *pro tempore*.

I dati vengono elaborati per le finalità lavorative dai soci cooperatori della struttura della società che ha una sede: quella legale in cui è altresì sede operativa sita in Milano via Mac Mahon n. 2.

Non sono affidati incarichi a soggetti terzi per il trattamento dei dati.

⁵ Giova evidenziare che il Regolamento UE n. 679-2016 introduce la figura del Data Protection Officer (art. 37, 38, 39). Occorre precisare che la nomina del Data Protection Officer è obbligatoria per i soggetti pubblici, mentre è facoltativa per i soggetti privati, ad eccezione di alcuni trattamenti particolarmente a rischio e salva diversa disposizione della legislazione nazionale (ad es. per quei soggetti privati la cui attività principale consiste nel trattamento su larga scala di categorie particolari di dati personali e di dati relativi alle condanne penali e ai reati).

Thesis Group S.r.l.

Il Titolare del Trattamento ha l'obbligo di implementare le misure idonee affinché il trattamento dei dati personali sia effettuato in conformità alle leggi vigenti. Ciò deve per appunto essere dimostrato in modo documentato (il c.d. principio di *accountability*⁶).

Il presente AUDIT è una delle procedure di ispezione e di controllo per il sistema di verifica di conformità legislativa alle misure tecniche ed organizzative adottate o di cui dotarsi, qualora non vi siano.

Il Titolare deve mettere in atto misure organizzative e tecniche per garantire che siano trattati solo i dati personali necessari per ogni specifica finalità del trattamento: tale obbligo vale per la quantità di dati raccolti, archiviati, per il periodo di loro conservazione fino alla cancellazione.

Si evidenzia, dunque, che quanto alle persone giuridiche, il Titolare del trattamento è l'ente stesso, a prescindere dell'organo o dalle persone fisiche che ne esprimono la volontà: su questo punto merita quanto espresso dal Garante Privacy con la Circolare n.291/S del 13 novembre doc. 39785, con la quale si è chiarito che *“qualora il trattamento sia effettuato nell'ambito di una persona giuridica, di una pubblica amministrazione o di un altro organismo, “il titolare” è l'entità nel suo complesso (quindi la srl, l'associazione, la cooperativa onlus, ecc ecc), anziché taluna delle persone fisiche che operano nella relativa struttura e che concorrono, in concreto, ad esprimerne la volontà o che sono legittimati a manifestarla all'esterno”*.

c) Data Protection Officer (Responsabile per la Protezione dei dati personali)

Thesis Group S.r.l., in persona del legale rappresentante *pro tempore*, indica e designa l'Avv. Andrea Cantoni del Foro di Pavia, nato a Pavia il 24 dicembre 1978, c.f. CNTNDR78T24G388D, con studio in Pavia Viale della Libertà n. 23 quale **Data Protection Officer** della società stessa.

Il D.P.O. designato è un consulente esterno della società Titolare del trattamento dei dati e come previsto per legge dal GDPR n. 679-2016 il D.P.O. ha il compito di:

⁶ L'art 32 del Regolamento specifica che sono a capo del Titolare del trattamento l'adozione di misure tecniche ed organizzative la cui finalità è quella di garantire il livello di sicurezza adeguato al rischio; una di queste misure è quella di testare e verificare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. E' evidente che una delle misure necessaria è quella della previsione di un audit interno da parte del D.P.O. che osservi e valuti le misure in essere e quelle da adottare al fine di ridurre il rischio di perdita dei dati personali trattati all'interno della organizzazione aziendale.

Thesis Group S.r.l.

1) informare e fornire al Titolare del trattamento, nonché ai soci cooperatori che eseguono il trattamento in ragione dell'attività commerciale compiuta dalla Thesis Group S.r.l. in merito agli obblighi derivanti dal Regolamento europeo n. 679-2016;

2) sorvegliare l'osservanza delle norme di cui Regolamento europeo;

3) fornire un parere in merito alla valutazione di impatto sulla protezione dei dati personali e sorvegliarne lo svolgimento ai sensi dell'art. 35 Reg. europeo;

4) cooperare con l'Autorità di controllo (Garante per la protezione dei dati personali) e fungere da punto di contatto per l'Autorità di controllo per questioni connesse al trattamento dei dati;

5) controllare che le violazioni dei dati personali siano documentate, notificate e comunicate al Garante della Privacy.

Al D.P.O. è stato inoltre previsto il compito di redigere il presente rapporto di AUDIT per il Sistema Privacy in essere presso la Thesis Group, al fine di verificare che le procedure interne della società siano conformi agli adempimenti richiesti dal Regolamento Europeo e per effettuare la valutazione del rischio (cfr. pag. seguenti).

d) Incaricati del trattamento

Le operazioni di trattamento dei dati personali di cui al paragrafo precedente (*"Tipologia dati trattati"*, pag. 7) possono essere effettuate solo da incaricati che operano sotto la diretta autorità del Titolare dei dati, e per esso dal legale rappresentante, attenendosi alle istruzioni impartite.

I soggetti che trattano dati personali sono incaricati con lettera personalizzata del legale rappresentante della società, che riepiloga istruzioni particolareggiate a cui conformarsi per il rispetto della normativa vigente.

Al momento risultano incaricati del trattamento di dati personali tutti i dipendenti e/o collaboratori, a cui si rinvia ai singoli allegati per ciò che concerne le rispettive lettere di incarico.

La designazione è effettuata per iscritto come da lettera di nomina allegata.

Il trattamento dei dati avviene sia nelle sede legale poc'anzi indicata, sia in ogni sede operativa di Thesis Group S.r.l..

Le chiavi di tutti i locali sono conservate presso la sede legale sia presso la sede operativa della società e sono in possesso del legale rappresentante e dei soci cooperatori.

Thesis Group S.r.l.

Informativa dei dati personali e relativo consenso (cfr. allegati)

L'informativa del trattamento dei dati personali è direttamente collegata alla tutela della riservatezza della persona interessata al trattamento dei propri personali; il Titolare del trattamento deve imporre ai propri incaricati di sottoporre sempre agli interessati che raccolgono e trattano dati personali di persone fisiche le informative (*ad hoc* predisposte) con finalità dettagliate e specifiche con riguardo ai dati personali trattati e raccolti dalla società Thesis Group Srl, poiché è necessario che l'informativa venga resa sempre prima di ogni operazione di trattamento e prima che l'interessato manifesti il proprio consenso.

Si rende necessario che il nominato D.P.O. ponga in essere procedure interne di costante monitoraggio ed eventuale revisione dei requisiti legali delle informative utilizzate per acquisire un corretto consenso da parte dell'interessato. Ogni incaricato del trattamento ha l'obbligo di rendere l'informativa dei dati personali di cui al trattamento specifico, indicandone le specifiche finalità ed la relativa modalità di trattamento, verificando che i consensi espressi siano liberi e specifici per le finalità indicate, enunciando altresì singoli diritti previsti dall'art. 15 del Regolamento Europeo n. 679-2016.

Esercizio dei diritti di cui all'art 15 Reg. Europeo n. 679-2016

Il diritto alla protezione dei dati personali è un diritto fondamentale dell'individuo tutelato dal Codice Privacy (D. Lgs n. 196-2003 e dal Reg. UE 679-20016); l'interessato pertanto non può sempre impedire il trattamento dei propri dati⁷, ma può sempre esercitare il proprio potere di controllo nel rispetto dei diritti riconosciuti dalla legge.

In *primis* è bene ricordare che ai sensi dell'art. 4, comma 1, lett i) del D. Lgs n. 196-2003 il soggetto interessato dalla tutela del trattamento dei dati personali è la sola persona fisica: l'attuale formulazione è stata infatti modificata dal cd "Decreto salva Italia" (D.L. 06 dicembre 2011 n. 201, conv. con modificazioni dalla Legge 22 dicembre 2011 n. 214) che ha introdotto la tutela dei diritti e delle libertà fondamentali alle sole persone fisiche, riallineando la normativa italiana a quella europea. Sono

⁷ Si pensi ai casi di esenzione del consenso di cui all'art. 24 del D. Lgs n. 196-2003

Thesis Group S.r.l.

quindi escluse dall'applicazione del Codice della Privacy e dal Regolamento UE n.2016-679 il trattamento dei dati relativi a persone giuridiche, enti, associazioni⁸.

Alla luce di tali principi, la Thesis Group S.r.l. ha predisposto un modello, in realtà inserito nelle singole informative al trattamento dei dati, attraverso il quale l'interessato al trattamento dei suoi dati personali può chiedere l'esercizio dei diritti in base al Reg. Eu n. 679-2016, ossia al fine di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.

Non solo, ma il Titolare del trattamento dei dati deve consentire che l'interessato abbia il diritto di ottenere, da coloro che sono incaricati di effettuare il trattamento, l'indicazione dell'origine dei dati personali, ossia degli atti o dei soggetti dai quali i dati provengono prima di essere trattati; l'indicazione delle finalità e modalità (e ciò infatti dovrà risultare nelle idonee informative da sottoporre) e degli estremi identificativi del titolare e del D.P.O..

Infine, l'interessato ha il diritto di ottenere l'aggiornamento, la rettificazione ovvero quando vi ha interesse la integrazione dei dati, la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione della legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati.

Privacy Policy del sito web

Per quanto riguarda il sito web della società il sistema Privacy si prefigge lo scopo di descrivere le modalità di gestione del proprio sito, in riferimento al trattamento dei dati personali degli utenti che lo consultano.

Si tratta di un'informativa che è resa conformemente al Regolamento UE n. 2016-679 - Codice in materia di protezione dei dati personali – a coloro che si collegano al sito web della società Thesis Group S.r.l. e usufruiscono dei relativi servizi web.

L'informativa è resa soltanto per il sito sopra menzionato e non anche per altri siti web eventualmente consultati dall'utente tramite appositi link.

⁸ La *ratio* della riforma legislativa del Decreto Salva Italia – così si legge nella relazione al Decreto legge – è quella di ridurre gli oneri derivanti dal trattamento di dati nell'ambito di rapporti di natura meramente amministrativa o economica tra imprese e tra queste ed enti pubblici, senza alterare in alcun modo i livelli di tutela garantiti dal codice alla persone fisiche.

Thesis Group S.r.l.

Il sito è di proprietà e gestione della società, che garantisce il rispetto della normativa in materia di protezione dei dati personali. Gli utenti/visitatori hanno l'obbligo di leggere attentamente la presente Privacy Policy che è pubblicata sul sito prima di inoltrare qualsiasi tipo di informazione personale e/o compilare qualunque eventuale modulistica elettronica che in futuro potrebbe essere presente sul sito stesso.

Tipologia di dati trattati sul sito web e finalità del trattamento.

1) Dati di navigazione.

I sistemi informatici e le procedure software preposte al funzionamento di questo sito acquisiscono, nel normale esercizio, alcuni dati personali che vengono poi trasmessi implicitamente nell'uso dei protocolli di comunicazione Internet.

Si tratta di informazioni che non sono raccolte per essere associate a interessati identificati, ma che per loro stessa natura potrebbero, attraverso elaborazioni ed associazioni con dati detenuti da terzi, permettere di identificare gli utenti. In questa categoria di dati rientrano gli indirizzi IP o i nomi a dominio dei computer utilizzati dagli utenti che si connettono al sito, gli indirizzi in notazione URI (Uniform Resource Identifier) delle risorse richieste, l'orario della richiesta, il metodo utilizzato nel sottoporre la richiesta al server, la dimensione del file ottenuto in risposta, il codice numerico indicante lo stato della risposta data dal server (buon fine, errore, ecc.) ed altri parametri relativi al sistema operativo e all'ambiente informatico dell'utente. Questi dati vengono utilizzati al solo fine di ricavare informazioni statistiche anonime sull'uso del sito e per controllarne il corretto funzionamento e vengono cancellati immediatamente dopo l'elaborazione. I dati potrebbero essere utilizzati per l'accertamento di responsabilità in caso di ipotetici reati informatici ai danni del sito: salva questa eventualità, i dati sui contatti web non persistono per più di sette giorni.

2) Dati forniti volontariamente dagli utenti/visitatori.

Qualora gli utenti/visitatori, collegandosi a questo sito, inviino propri dati personali per accedere a determinati servizi, ovvero per effettuare richieste in posta elettronica, ciò comporta l'acquisizione da parte della società dell'indirizzo del mittente e/o di altri eventuali dati personali che verranno trattati esclusivamente per rispondere alla richiesta, ovvero per la fornitura del servizio. I dati personali forniti dagli

Thesis Group S.r.l.

utenti/visitatori verranno comunicati a terzi solo nel caso in cui la comunicazione sia necessaria per ottemperare alle richieste degli utenti/visitatori medesimi.

3) Cookies

Per i cookies si rimanda alla relativa privacy cookies disponibile sul sito web della società.

Modalità del trattamento dei dati personali trattati attraverso il sito web.

I dati personali sono trattati con strumenti automatizzati per il tempo strettamente necessario a conseguire gli scopi per cui sono stati raccolti. Specifiche misure di sicurezza sono osservate per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati.

Facoltatività del conferimento dei dati.

A parte quanto specificato per i dati di navigazione, gli utenti/visitatori sono liberi di fornire i propri dati personali. Il loro mancato conferimento può comportare unicamente l'impossibilità di ottenere quanto richiesto.

Titolare del trattamento dei dati personali acquisiti attraverso il sito web

Il titolare del trattamento dei dati personali per il sistema web è sempre la società Thesis Group S.r.l..

Dati personali trattati con sistemi di videosorveglianza.

Thesis Group S.r.l. ha in dotazione sistemi di videosorveglianza presso la sede operativa sita in Via Mac Mahon n. 2, Milano.

La raccolta, la registrazione, la conservazione e in generale l'utilizzo di immagini configura un trattamento di dati personali (cfr. art. 4, comma 1, lett. b) D.lgs n. 196-2003), perché – come noto – è considerato dato personale qualunque informazione

Thesis Group S.r.l.

relativa a persona fisica identificata o identificabile, anche indirettamente mediante riferimento a qualsiasi altra informazione.

L'installazione di sistemi di rilevazione delle immagini deve avvenire nel rispetto di determinati e precisi principi generali: quello della liceità e finalità. I sistemi installati da Thesis Group S.r.l. devono rispondere ad esigenze di protezione e incolumità dei dipendenti, di eventuali soggetti terzi, di protezione della proprietà e del patrimonio dell'azienda.

Nelle zone in cui vi sono sistemi di videosorveglianza l'Amministratore Unico deve assicurare che le zone siano segnalate con idonea cartellonistica, affinché ogni interessato sia sempre informato che sta per accedere ad una zona video sorvegliata⁹.

L'informativa che deve essere conforme a quanto stabilito dall'art. 13 del D. Lgs n. 196-2003 può essere resa in forma "minima" (semplificata), indicando il titolare del trattamento e la finalità perseguita.

Le finalità del sistema di video sorveglianza devono bilanciarsi con il diritto alla riservatezza e alla dignità delle persone, con particolare riguardo ai dipendenti della società e alla luce dei principi contenuti nello Statuto dei lavoratori (Legge n. 300-1970).

Questa non è la sede opportuna per analizzare i profili relativi alla disciplina dello Statuto dei lavoratori, ma occorre evidenziare seppur brevemente che per poter installare correttamente un sistema di videosorveglianza (audiovisivo) si devono tenere in considerazione sia la disciplina privacy sia quella prevista in tema di controlli a distanza prevista dalla Statuto dei lavoratori, modificata dal recente intervento legislativo D lgs n. 151 del 14.09.2015 (cd *Jobs act*).

In tale sede si vuole richiamare che il novellato art. 4 dello Statuto dei lavoratori ammette l'installazione di un impianto di videosorveglianza in un luogo di lavoro, purché vi siano esigenze organizzative, produttive, di sicurezza del lavoro o di tutela del patrimonio aziendale e a condizione che venga raggiunto un previo accordo con le rappresentanze sindacali o si ottenga una autorizzazione dalla competente Direzione Territoriale del Lavoro.

⁹ Giova infatti menzionare orientamento della giurisprudenza della Corte di Cassazione secondo cui *"l'installazione di un impianto di videosorveglianza, costituendo trattamento di dati personali, deve formare oggetto di previa informativa ex art. 13 D. lgs n. 196-2003, resa ai soggetti interessati prima che facciano accesso nell'area videosorvegliata, mediante supporto da collocare perciò fuori del raggio di azione delle telecamere che consentono la raccolta delle immagini delle persone e danno così inizio al trattamento stesso"* (Cass. Sez II 05.07.2016 n. 13663).

Thesis Group S.r.l.

Pertanto Thesis Group Srl è ben consapevole della necessità di avere un accordo sindacale o di essere autorizzata dalla D.T.L. per poter procedere alla legittima installazione dell'impianto di videosorveglianza. Si suggerisce alla società di presentare istanza alla Direzione Territoriale del Lavoro, mediante il modello unificato, adottato dal Ministero del Lavoro che si allega.

La disciplina relativa alla privacy (art. 11, comma 1, lett. e) del D. Lgs n. 196-2003) Conservazione immagini stabilisce che la conservazione delle informazioni, in una forma che consenta l'identificazione dell'interessato, non superi il periodo di tempo necessario agli scopi per i quali sono state raccolte o successivamente trattate.

Il Provvedimento generale dell'08 aprile 2010 dell'Autorità ha stabilito che “*nei casi in cui sia stato scelto un sistema che preveda la conservazione delle immagini, in applicazione del principio di proporzionalità, anche l'eventuale conservazione temporanea dei dati deve essere commisurata al tempo necessario e predeterminato a raggiungere la finalità perseguita*”; con riguardo alla definizione delle tempistiche di conservazione, ciò è rimessa alla prudente valutazione del titolare del trattamento; con nota del 20 agosto 2013 l'Autorità Garante ha chiarito che “*la concreta valutazione dei tempi – comunque infrasettimanale – reputati necessari per la conservazione delle immagini è direttamente rimessa al titolare del trattamento che, al riguardo, assume ogni responsabilità; ciò ovviamente tranne che nell'ipotesi in cui dall'installazione degli impianti audiovisivi all'interno [della società Thesis Group nel nostro caso] possa derivare, seppur in via indiretta, un controllo a distanza sull'attività lavorativa: nel qual caso si rende necessario espletare la procedura di cui all'art. 4 dello Statuto dei Lavoratori. Pertanto in assenza di un accordo con le rappresentanze sindacali aziendali, i tempi di conservazione delle immagini debbono essere fissati – anche oltre le 24 ore, purché non oltre 48 ore – dalle direzioni del lavoro territorialmente competenti, anche alla luce dei principi stabiliti dal codice della Privacy*”.

Si evidenzia che i dati personali trattati tramite un impianto di videosorveglianza devono essere protetti con idonee misure di sicurezza, capaci di ridurre i rischi di distruzione, di perdita anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alla finalità della raccolta.

Pertanto si impone al Titolare del trattamento di designare gli incaricati che possono accedere ai locali dove sono situate le postazioni di controllo attraverso credenziali di autenticazione per poter visionare le immagini; inoltre per i soli soggetti abilitati deve essere limitata la possibilità di visionare le immagini, non necessariamente in sincronia

Thesis Group S.r.l.

con la ripresa, ma anche in tempo differito, e di poter effettuare operazioni di cancellazione: il sistema di videosorveglianza va infatti configurato in modo tale da poter procedere con la cancellazione delle immagini al termine del periodo di conservazione previsto.

PARTE II

Analisi del rischio e misure di sicurezza adottate

Il Titolare del Trattamento Thesis Group S.r.l., coadiuvata dal suo Data Protection Officer, ha condotto in modo completo un'analisi con l'obiettivo di identificare i rischi per la sicurezza e la custodia dei dati personali trattati dalla società cooperativa e per individuare le aree in cui vi è il pericolo di distruzione o perdita, anche accidentale dei dati.

Il Regolamento Europeo 2016-679 impone che i dati personali, a maggior ragione quelli qualificati come sensibili, debbano essere trattati in maniera da garantirne un'adeguata sicurezza e protezione, mediante l'adozione di misure tecniche ed organizzative, per ovviare a trattamenti non autorizzati, illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

Deve essere cura del Titolare del trattamento, coadiuvato dal D.P.O., svolgere preventive valutazioni di impatto privacy in ordine alle misure di sicurezza adottate o di cui dotarsi se ancora non esistenti

Per lo svolgimento dell'analisi di rischio, il sottoscritto D.P.O. ha fatto riferimento a queste particolari categorie di rischio:

- distruzione o perdita anche accidentale dei dati (il rischio va letto in correlazione al principio secondo cui i dati devono essere completi e disponibili. Un modo per garantire la disponibilità e la integrità dei dati è quello di proteggere fisicamente gli strumenti informatici che li contengono);
- accesso non autorizzato (il rischio fa riferimento sia all'accesso fisico ad ambienti dove sono custoditi dati personali, sia a banche dati elettroniche. In questo ultimo caso si configurerebbe la fattispecie di reato ex art. 615-ter cod. pen., in materia di accesso abusivo ad un sistema informativo o telematico);
- trattamento non consentito (il rischio fa riferimento a qualunque operazione che renda il trattamento illecito o non corretto, ad es. assenza di informativa della privacy, assenza dell'acquisizione del consenso);
- trattamento non conforme alle finalità della raccolta (il rischio fa riferimento ad un trattamento inizialmente lecito e corretto, ma che con il tempo si è discostato dal principio di finalità).

Thesis Group S.r.l.

Nella tabella A segue la *check-list* dell'**analisi dei rischi**:

Tabella A – Check-list analisi del rischio

EVENTO RISCHIO		GRAVITÀ STIMATA	MISURE D'AZIONE	STATO DELLA MISURA DI SICUREZZA
Comportamento dei soci, operatori ed incaricati del trattamento	Sottrazione di credenziali di autenticazione	Bassa	Accesso al sistema informativo e di posta elettronica sono consentiti solo attraverso credenziali di autenticazione assegnati agli incaricati	In essere
	Carenza di consapevolezza e informazione; disattenzione	bassa	Formazione-informazione, istruzioni e modalità operative,	In essere
	Comportamenti sleali o fraudolenti	Bassa	Formazione, informazione, istruzioni operative	In essere
	Errore umano materiale nella gestione della sicurezza	bassa	Sono adottati sistema antivirus, firewall e gruppi di continuità	In essere
Eventi relativi agli strumenti	Malfunzionamento guasti tecnici di hardware, software, supporti o degrado degli strumenti	bassa	Interventi di manutenzione da consulente qualificato, eventuale sostituzione strumenti.	In essere
	Accessi esterni non autorizzati	Media	Accesso all'ufficio controllato; esistono sistemi di videosorveglianza presso ogni sede e magazzino.	In essere
	Azione di virus informatici o di programmi suscettibili di recare danno; intercettazione di informazioni in rete; spamming o altre tecniche di sabotaggio	media	Sistema firewall	In essere

Thesis Group S.r.l.

	Accessi non autorizzati a locali ad accesso ristretto Accesso Sala Server	Media	Locali custoditi, schedari/archivi chiusi a chiave Tutti i dati personali sono salvati su un proprio server di cui la Thesis Group è proprietaria ed il Server è in loco presso i locali aziendali di Via Mc Mahon n. 2, Milano.	Accesso al server non è controllato con sistema di video sorveglianza. Il locale è chiuso con chiavi in dotazione presso il solo personale della società
Eventi relativi al contesto fisico-ambientale	Ingressi non autorizzati a locali ed aree di accesso ristretto/ furto di strumenti contenenti dati	medio-alta	Locali custoditi con porte blindate.	In essere
	Eventi distruttivi naturali o artificiali, dolosi, accidentali o dovuti ad incuria; guasto ai sistemi	Media	Dispositivi antincendio previsti dalla normativa vigente.	In essere
	Errori umani nella gestione della sicurezza fisica	Bassa	Formazione-informazione	In essere
	Guasto dei sistemi complementari (Impianto elettrico)	Bassa	Stabilizzatore di tensione e gruppo di continuità dell'alimentazione elettrica	In essere

Misure a tutela dell'integrità e disponibilità dei dati personali

Alla luce dei fattori di rischio e delle aree individuate vengono di seguito descritte le misure atte a garantire:

- la protezione delle aree e dei locali ove si svolge il trattamento dei dati personali e sensibili;
- la corretta archiviazione e custodia di atti, documenti e supporti contenenti dati personali e sensibili;
- la sicurezza logica, nell'ambito degli strumenti elettronici;
- attività di verifica e controllo periodici dell'efficacia delle misure adottate.

Thesis Group S.r.l.

La protezione di aree e locali

Per quanto concerne il rischio che i dati vengano danneggiati o perduti a seguito di eventi distruttivi, tutti i locali aziendali ove si svolge il trattamento dei dati sono protetti da dispositivi antincendio previsti dalla normativa vigente.

Sono adottate le seguenti misure per impedire accessi non autorizzati:

- Presenza costante di personale di servizio nelle ore d'ufficio;
- Locali custoditi e accessi controllati;
- Locali e schedari chiusi a chiave.

Custodia, archiviazione dei dati e analisi del rischio informativo

La gestione, la custodia e l'archiviazione dei documenti e dei supporti elettronici è attuata con il programma di Microsoft 365 di nuova generazione tali da garantire il corretto sistema di salvataggio dei dati con sistema di backup.

Il titolare del trattamento ha predisposto idonea *check-list* che si allega al presente documento.

Il rischio informatico è un evento principalmente capace di determinare la perdita o l'alterazione dei dati personali trattati.

A tal fine il Titolare del trattamento dei dati ed il D.P.O. devono costantemente curare e affrontare la gestione del rischio attraverso l'adozione e la verifica delle misure di sicurezza finalizzate a identificare, analizzare e risolvere situazioni di pericolo di perdita e/o alterazione dei dati trattati.

Pertanto deve essere cura del Titolare del trattamento, attraverso ausilio e coordinamento con il D.P.O., assicurare che all'interno della società vi siano sistemi informatici dotati di codici di accesso al fine di:

- limitarne l'uso alle persone autorizzate ai PC e connessione al server;
- autorizzare e definire le tipologie di dati ai quali gli incaricati possano accedere e utilizzare al fine delle proprie mansioni lavorative;
- proteggere strumenti e dati da malfunzionamenti e attacchi informatici (attraverso adozione di *antivirus* e *antispam* e *firewall*);
- prescrivere le opportune cautele per la custodia e l'utilizzo dei supporti rimovibili, contenenti dati personali (ad es. si consiglia agli incaricati del trattamento di non installare autonomamente programmi software provenienti dall'esterno, salva previa esplicita autorizzazione dell'Amministratore di Sistema, perché sussiste il grave

Thesis Group S.r.l.

pericolo di portare virus informatici e di alterare la stabilità delle applicazioni del pc in dotazione).

Accesso ai dati e istruzioni

Gli incaricati al trattamento dei dati dovranno osservare le seguenti istruzioni per l'utilizzo degli strumenti informatici:

- obbligo di custodire i dispositivi di accesso agli strumenti informatici (*username* e *password*) e di modificarli periodicamente, comunicandolo all'Amministratore di Sistema;
- obbligo di non lasciare incustodito e accessibile lo strumento elettronico assegnato durante una sessione di trattamento;
- obbligo di assoluta riservatezza;
- divieto di divulgazione delle password di accesso al sistema.

Protezione di strumenti e dati

Il sistema di elaborazione dati è protetto da programmi *antivirus*, per il controllo all'accesso, in grado di intercettare tutte le operazioni eseguite dall'incaricato ed effettuare una scansione per l'individuazione di *virus* ogni volta che un *file* viene aperto, copiato, creato o rinominato.

Il sistema di protezione è aggiornato periodicamente.

E' installato anche un *firewall* che impedisca gli accessi non autorizzati.

Supporti rimovibili

Anche se le norme prevedono particolari cautele solo per i supporti rimovibili contenenti dati sensibili e giuridici, la tutela per il trattamento viene estesa ai dati personali come segue:

- custodia dei supporti in locali chiusi a chiave con accesso ai soli autorizzati;
- cancellazione e/o distruzione del supporto una volta cessate le ragioni per la conservazione dei dati;
- obbligo di utilizzo dei supporti rimovibili solo ed esclusivamente in struttura.

Criteri di ripristino dei dati

Per i dati trattati con strumenti elettronici **sono previste procedure di *backup*** attraverso le quali viene periodicamente effettuata una copia di tutti i dati presenti nel

Thesis Group S.r.l.

sistema. Il salvataggio dei dati avviene in modo automatico, programmato un periodo breve entro cui salvare i dati.

Controllo generale sullo stato della sicurezza

Il Titolare del trattamento dei dati mantiene aggiornate le misure di sicurezza al fine di adottare gli strumenti più idonei per la tutela dei dati trattati. Egli verifica, attraverso il D.P.O. l'efficacia delle misure adottate relativamente a:

- accesso fisico a locali dove si svolge il trattamento;
- procedure di archiviazione e custodia dati trattati;
- efficacia e utilizzo misure di sicurezza strumenti elettronici;
- integrità dei dati e delle loro copie di backup;
- distruzione dei supporti magnetici non più riutilizzabili;
- cancellazione dei filmati della videosorveglianza ed utilizzo degli stessi solo per le ragioni di sicurezza e rispetto dei regolamenti;
- livello di informazione degli interessati.

Ogni semestre il D.P.O. deve esporre quanto riscontrato nelle verifiche sull'efficacia delle misure adottate e in tale sede saranno valutate eventuali proposte e piani di miglioramento delle misure di sicurezza.

Interventi formativi

La formazione erogata ha riguardato i seguenti contenuti:

- informazione sulla normativa vigente in materia di protezione dei dati,
- rischi che incombono sui dati,
- misure disponibili per prevenire eventi dannosi,
- profili della disciplina sulla protezione dei dati personali più rilevanti in relazione alla propria attività,
- responsabilità che ne derivano.

La formazione è programmata al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti, rilevanti per il trattamento dei dati personali.

L'intervento formativo viene registrato e documentato attraverso la modulistica del sistema qualità.

Thesis Group S.r.l.

Rapporto finale di AUDIT

L'analisi condotta in base alle *check-list* e alla *best practice* evidenzia all'interno della struttura aziendale della Thesis Group S.r.l. una situazione a livello di Sistema Informatico nel suo complesso discreto, conforme a livello normativo con l'insieme delle misure di sicurezza richieste per il sistema Privacy.

Il Titolare del trattamento ha messo in atto una serie di misure di sicurezza del Sistema Informatico su diversi livelli; ad esempio adottando un sistema *antivirus* aggiornato quotidianamente per la sicurezza del Sistema stesso; unitamente a ciò i sistemi informatici in essere hanno in adozione anche un sistema di salvataggio dati (backup) automatizzato; i dati sono salvati attraverso Google e Microsoft.

Il sottoscritto D.P.O. ha rilevato un non consono uso delle password dei personal computer, come si può evincere dalla check list ad hoc predisposta: dall'analisi delle misure di sicurezza dei pc si rileva che le singole password non sono riferibili a ciascun incaricato e soprattutto non vengono modificate dopo brevi intervalli di tempo; si suggerisce che ogni incaricato abbia proprie password di almeno 8 caratteri alfanumerici e di provvedere alla loro modifica ogni 3 mesi.

L'analisi condotta fotografa un grado di sicurezza del sistema informatico discreto; pertanto si può affermare che l'attuazione del Sistema Gestione Privacy all'interno dell'azienda Thesis Group S.r.l. necessita di essere maggiormente adeguato alla disciplina normativa del Regolamento Europeo n. 679-2016, sia sul piano documentale sia soprattutto su quello applicativo, valutati i rischi indicati nell'impatto esaminato, in considerazione anche di molti dati sensibili, afferenti lo stato di salute dei pazienti. Anche in relazione alla sala del server, si evidenzia che i locali aziendali sono chiusi a chiave, non accessibili da terzi.

L'AUDIT ha dunque avuto ad oggetto interviste al legale rappresentante della società a cui sono state richieste le informazioni di cui alla check-list allegata al presente documento.

La lista di controllo allegata al presente rapporto, di cui fa parte integrante, può essere riutilizzata e adeguata rispetto alle normative vigenti e all'aggiornamento delle tecnologie impiegate di volta in volta.

Nel caso di specie, la Thesis Group S.r.l. è una società che non divulga su larga scala ma, stante il numero elevato di dati sensibili che tratta, ha istituito un proprio

Thesis Group S.r.l.

registro del trattamento dei dati personali conforma quanto previsto dall'art. 30 Regolamento europeo.

Il presente documento è stato completato ed ultimato il giorno 25 luglio 2018 e viene aggiornato in caso di variazione delle procedure.

L'originale del presente documento è custodito presso la sede del Titolare del trattamento dei dati personali, per essere esibito in caso di controllo.

Pavia, 25 luglio 2018

Per previa visione

il legale rappresentante nonché l' Amministratore Unico
dott.ssa Roberta Cossutta

Sono allegati i seguenti documenti:

All. 1 – lettera di nomina Data Protection Officer

All. 2 – lettera nomina incaricato del trattamento dati personali

All. 3- a – Informativa Privacy PAZIENTI

All. 3-b – Informativa Privacy socio cooperatore

All. 3-c – Informativa Privacy stagista/tirocinante

All. 3-d – Informativa Privacy fornitori

All. 4 – Informativa Videosorveglianza

All. 5 – check list misure di sicurezza strumenti informatici ed internet

All. 6 -check list registro trattamento dati

All. 7 – nomina del Responsabile del Trattamento dati

All. 8 – Regolamento UE n. 2016-679

Il presente documento di Gestione Privacy è stato redatto dal Data Protection Officer incaricato, Avv. Andrea Cantoni del foro di Pavia.