POLICY IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

FORTNES S.P.A.
PIAZZA UMBERTO I, 1 - 84121 - SALERNO
TEL +39 089 273683 - +39 089 2576093
FAX +39 089 2022201

SOMMARIO

PREMESSA

La presente policy (di seguito "Policy") è redatta in ottemperanza all'art. 24, comma 2, del Regolamento (UE) 2016/679 (di seguito "GDPR" o "Regolamento") che abroga la precedente Direttiva 95/46/CE e disciplina gli aspetti relativi alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione degli stessi.
La Politica definisce:

- i principi generali applicabili a FORTNES S.p.a. (in seguito anche detta "FORTNES" o "La Società"), in qualità di titolare del trattamento di dati personali e i presidi generali adottati per ottemperare a tali principi;
- le responsabilità e i compiti degli organi sociali e delle strutture aziendali di FORTNES S.p.a.

Il Responsabile Affari Legali, provvede, con cadenza almeno annuale, a rivedere la Politica e a valutare eventuali modifiche da apportare. Ogni modifica sostanziale del documento deve essere approvata dal Consiglio di Amministrazione.
Eventuali modifiche derivanti da *i)* cambiamenti organizzativi, *ii)* emanazione o modifica della normativa di secondo livello (es. Provvedimenti del Garante Privacy) sono apportate, su proposta del Responsabile Affari Legali, della Direzione, con informativa al Consiglio di Amministrazione.
La Politica entra in vigore il 25 maggio 2018 e sarà diffusa a tutte le Unità Organizzative della Società.

1 PRINCIPI E PRESIDI GENERALI SUL TRATTAMENTO DEI DATI PERSONALI

La Politica identifica i principali presìdi individuati da FORTNES S.p.a. per assicurare il rispetto dei principi generali contenuti nel GDPR, con particolare riguardo a:

- liceità del trattamento;
- diritti degli interessati;
- registro dei trattamenti e valutazione d'impatto sulla protezione dei dati;
- sicurezza dei trattamenti;
- gestione degli eventi di *data breach*.

Al riguardo FORTNES:

i. adotta processi, strumenti e controlli idonei, che consentano il pieno rispetto dei principi generali sul trattamento dei dati personali;
ii. garantisce adeguati flussi informativi da e verso gli organi sociali, le strutture di controllo e operative;
iii. assicura lo svolgimento delle attività di formazione del personale in materia di protezione dei dati personali, al fine di garantire il rispetto della normativa applicabile da parte di chiunque ponga in essere attività di trattamento dei dati personali all'interno della struttura aziendale sotto l'autorità del titolare.

I trattamenti di dati personali delle diverse categorie di soggetti interessati (es. clienti, dipendenti, visitatori, fornitori) svolti dalla Società si fondano sui seguenti principi:

- **liceità, correttezza e trasparenza**: i dati personali sono raccolti e trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- **limitazione della finalità**: i dati personali sono raccolti e trattati per finalità determinate, esplicite e legittime;
- **minimizzazione dei dati**: i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- **esattezza**: i dati personali sono mantenuti esatti ed aggiornati e sono adottate misure ragionevoli per cancellare o rettificare, tempestivamente, i dati inesatti o superati;
- **limitazione della conservazione (c.d. *data retention*)**: i dati personali sono conservati per un arco temporale non superiore al conseguimento delle finalità per cui sono stati raccolti;
- **integrità e riservatezza**: i dati personali sono trattati in modo da garantirne un'adeguata sicurezza, attraverso l'adozione di misure tecniche ed organizzative adeguate;
- ***privacy by design* e *privacy by default***: gli aspetti in materia di protezione dei dati personali devono essere considerati fin dalle fasi di progettazione, implementazione e configurazione di tutte le tecnologie utilizzate per le operazioni di trattamento. FORTNES deve trattare, di default, solamente quei dati che siano necessari al perseguimento delle finalità del trattamento;
- **responsabilizzazione (c.d. *accountability*)**: i trattamenti dei dati personali sono svolti secondo i principi che precedono e il loro rispetto è adeguatamente documentato.

1.1 Liceità del trattamento

I trattamenti di dati personali all'interno della Società possono essere condotti esclusivamente sulla base di una o più delle seguenti condizioni:

i. contratto di cui l'interessato è parte;
ii. obbligo legale cui è soggetta la Società;
iii. esplicito consenso dell'interessato;
iv. perseguimento di un legittimo interesse della Società.

1.2 Richiesta del consenso

Laddove il trattamento di dati personali si fondi sul consenso dell'interessato, la raccolta del consenso è effettuata tramite dichiarazione scritta ovvero, in casi particolari caratterizzati da minore rischiosità, in forma orale e documentata per iscritto.
Qualora nel modulo utilizzato per la raccolta del consenso si trattino altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio chiaro e semplice in modo tale che la volontà dell'interessato sia liberamente espressa. Il consenso è revocabile in qualsiasi momento e la sua revoca non pregiudica la liceità del trattamento effettuato fino a quel momento.

1.3 Legittimo interesse

In alcuni casi, le procedure interne devono prevedere che il trattamento di dati personali possa essere effettuato al fine di perseguire un legittimo interesse di FORTNES.
In ottemperanza al principio di accountability, in tali casi, le procedure devono prevedere che la valutazione circa il corretto bilanciamento tra gli interessi di FORTNES e i diritti dell'interessato sia adeguatamente documentata.

1.4 Trasferimento di dati all'estero

Il trasferimento di dati personali verso un paese terzo (non appartenente all'Unione) o un'organizzazione internazionale può avere luogo senza autorizzazioni specifiche solo se la Commissione Europea ha deciso che il paese terzo o l'organizzazione internazionale garantisce un livello di protezione adeguato, sulla base di una serie di elementi (tra cui il rispetto dei diritti umani e delle libertà fondamentali, l'esistenza e l'effettivo funzionamento delle Autorità di controllo).
In mancanza di una decisione di adeguatezza, la Società può trasferire i dati personali solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi.

1.5 Diritti degli interessati

1.5.1 Informativa sul trattamento

In conformità ai principi di trasparenza, correttezza, limitazione delle finalità e *data retention*, le procedure devono prevedere che ai soggetti interessati, all'atto della raccolta dei dati personali, vengano fornite chiare informazioni (**Informativa**) circa:

- l'identità di FORTNES S.p.a. e del Responsabile della Protezione dei Dati ("DPO – Data Protection Officer");
- le caratteristiche del trattamento (es. le finalità e la base giuridica dello stesso, il periodo di conservazione dei dati);
- i diritti del soggetto interessato.

Qualora i dati non siano stati ottenuti presso l'interessato, l'informativa indica anche la fonte da cui hanno origine i dati personali e se si tratta di dati provenienti da fonti accessibili al pubblico.

1.5.2 Diritti d'accesso, rettifica, cancellazione, probabilità e opposizione

Le procedure devono assicurare il rispetto del principio di esattezza e di *data retention*, prevedendo che ogni interessato abbia il diritto di ottenere:

i. la conferma che siano o meno in corso attività di trattamento di suoi dati personali e informazioni sulle caratteristiche del trattamento (es. finalità, categorie di dati personali, destinatari della comunicazione dei dati, diritti dell'interessato);
ii. la rettifica di dati personali inesatti che lo riguardano, nonché la loro integrazione qualora siano incompleti;

iii. la cancellazione, se sussistono alcune fattispecie, ad esempio se i dati non sono più necessari rispetto alle finalità per le quali sono stati raccolti, se l'interessato ha revocato il consenso o ha esercitato il diritto di opposizione al trattamento, oppure se i dati personali sono stati trattati illecitamente;
iv. la portabilità dei dati oggetto del trattamento, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, qualora il trattamento si basi su un consenso legittimo e sia effettuato con mezzi automatizzati;
v. la cessazione del trattamento dei dati nel caso di trattamento effettuato sulla base del consenso dell'interessato.

Le procedure devono prevedere che, a seguito di ciascuna richiesta, si debbano fornire agli interessati le informazioni necessarie in forma concisa, accessibile ed usando un linguaggio semplice e chiaro, entro un mese (estendibile fino a due mesi, in casi di particolare complessità), anche in caso di diniego.

1.5.3 Registro trattamenti, analisi rischi, valutazione impatto e consultazione preventiva

FORTNES, pur non essendo sottoposta e preciso obbligo di legge, ha la possibilità di predispone e manutenere un "Registro delle attività di trattamento" che identifica le attività svolte in qualità di titolare o di responsabile del trattamento.
Il Registro costituisce la mappatura di tutti i trattamenti effettuati e viene aggiornato periodicamente. Il Registro deve essere reso disponibile su richiesta all'Autorità di Controllo. Il Registro rappresenta la base per assicurare il rispetto dei principi generali sanciti dal GDPR.
Al fine di assicurare l'integrità e la riservatezza dei dati personali, per ciascuna attività di trattamento identificata nel Registro, viene effettuata un'analisi del rischio. Ove da tale analisi emerga che il trattamento possa comportare un livello di rischio elevato per i diritti e le libertà degli interessati, le procedure devono prevedere lo svolgimento di una valutazione di impatto sulla protezione dei dati (*Data Protection Impact Assessment*, di seguito "DPIA").
In particolare, le procedure devono prevedere che, nel valutare la necessità di effettuare una DPIA su un determinato trattamento, si tenga conto: *(i)* del livello di rischio per i diritti e le libertà degli interessati, *(ii)* dell'esistenza di un trattamento automatizzato (inclusa la profilazione); *(iii)* del fatto che il trattamento sia effettuato su larga scala o *(iv)* possa comportare la sorveglianza sistematica su larga scala di una zona accessibile al pubblico Cfr. par 4).

1.5.4 Sicurezza del trattamento

Per garantire un livello di sicurezza del trattamento dei dati adeguato al rischio, le procedure devono definire misure tecniche e organizzative, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi del trattamento e alla natura dei dati personali, in accordo ai principi di "*privacy by design*" e "*privacy by default*".
Queste misure possono comprendere:

- la pseudonimizzazione e la cifratura dei dati personali;
- la riservatezza e l'integrità dei sistemi e dei servizi di trattamento assicurate su base permanente;
- meccanismi di verifica e valutazione della loro efficacia.

Tenendo conto dei rischi presentati dal trattamento che derivano, in particolare, dalla distruzione, dalla perdita o dalla modifica non autorizzata di dati personali, le procedure devono definire le misure di sicurezza che possono garantire un adeguato livello di protezione dei dati personali di default e in via preventiva rispetto allo stesso trattamento dei dati personali.

1.5.5 Gestione degli eventi di data breach

Sempre al fine di assicurare il rispetto dei principi di integrità e riservatezza dei dati personali, laddove sia identificata una violazione di sicurezza, accidentale o illecita, che comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata dei dati compromettendone la riservatezza, la disponibilità o l'integrità, le procedure devono assicurare, che la notifica all'Autorità di Controllo avvenga entro 72 ore dal momento in cui sia stata ravvisata la violazione.
Tale notifica contiene:

- la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati;
- i dati di contatto del Titolare del trattamento e del DPO se nominato;
- le probabili conseguenze della violazione;
- le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e attenuarne i possibili effetti negativi.

Qualora la notifica non sia effettuata entro 72 ore, devono essere indicati i motivi del ritardo. Nei casi in cui la violazione possa comportare elevati rischi per i diritti e le libertà dei soggetti interessati, le procedure devono prevedere che sia fornita agli interessati informativa sulla violazione senza ingiustificato ritardo. Tale comunicazione non è necessaria se

comporterebbe uno sforzo sproporzionato oppure se sono state adottate misure tecniche ed organizzative adeguate alla tutela dei dati (es. cifratura).
Le procedure devono stabilire che: *(i)* la scelta della modalità di comunicazione dovrà tenere in considerazione l'accessibilità dei soggetti interessati a formati diversi, e, ove necessario, le diversità linguistiche dei destinatari; e *(ii)* ciascuna violazione dei dati personali, sospetta o accertata, deve essere adeguatamente censita e documentata nel registro delle violazioni al fine di garantire il rispetto del principio di accountability.

2 IL MODELLO ORGANIZZATIVO DI FORTES SPA

2.1 Distribuzione dei compiti e delle responsabilità

2.1.1 Il Titolare del trattamento

Il Titolare del trattamento (o *data controller*) è colui che "*da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali*" (direttiva 95/46, art. 2 lett. d), e decide quali categorie di dati personali devono essere registrate (Convenzione 08, art. 2 lett. d).O anche, è "*la persona fisica, giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali ed agli strumenti utilizzati, ivi compreso il profilo della sicurezza*".
Coerentemente a quanto previsto dall'art. 24 del Reg. UE 2016/679, Il Titolare del Trattamento, "*Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario*".
FORTNES S.p.a., in qualità di Titolare del Trattamento ha pertanto il compito di:

- mettere in atto misure tecniche e organizzative adeguate, coerentemente ai costi di attuazione, alla natura, tipologia e finalità del trattamento al fine di garantire:
  - sia al momento di determinare i mezzi del trattamento, sia all'atto del trattamento stesso, l'attuazione di presidi, (quali ad esempio la pseudonimizzazione), volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati (cfr. art. 25, comma 1 Reg. 2016/679)
  - il trattamento, per impostazione predefinita, solo dei dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica (cfr. art. 25, comma 2 Reg. 2016/679).
- assicurare che i dati personali oggetto di trattamento siano custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- definire i principi cui devono attenersi, nello svolgimento della propria attività tutti coloro che sono autorizzati a trattare i dati personali, siano essi responsabili o incaricati del trattamento.

È, infine, onere, non delegabile, del Titolare del trattamento vigilare, anche tramite verifiche periodiche, sulla puntuale osservanza delle disposizioni vigenti in materia di sicurezza dei dati personali e sul rispetto da parte dei Responsabili di cui nel seguito delle proprie istruzioni.
La società FORTNES S.p.a., nella sua qualità di Titolare del trattamento si avvale anche di aziende esterne: in particolare il sistema informativo aziendale è gestito in *outsourcing* da una Società esterna che ha assunto la qualifica di "soggetto terzo Responsabile del Trattamento.
È disponibile al pubblico sul sito e presso il *front office* dalla Società l'elenco di soggetti o categorie di soggetti a cui possono essere comunicati i dati personali raccolti dalla Azienda.

2.1.2 Responsabile del trattamento

Qualora un trattamento debba essere effettuato per conto del Titolare del trattamento, quest'ultimo ricorre unicamente

a **Responsabili del trattamento** che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.
Il Responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del Titolare del trattamento. Nel caso di autorizzazione scritta generale, il Responsabile del trattamento informa il Titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri Responsabili del trattamento, dando così al Titolare del trattamento l'opportunità di opporsi a tali modifiche.
I trattamenti da parte di un Responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il Responsabile del trattamento al Titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento (cfr. art. 28, Reg. 2016/679)
Il Responsabile ha **obblighi di trasparenza**. In tal senso occorre contrattualizzare il rapporto tra Titolare e Responsabile, specificando gli obblighi e i limiti del trattamento dati. Il Responsabile riceverà, tramite l'atto giuridico (cioè per iscritto), tutte le istruzioni in merito ai trattamenti operati per conto del Titolare, alle quali dovrà attenersi. Inoltre il Responsabile del trattamento dovrà mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi che gli impone l'articolo 28 del Regolamento[1]).
Il Responsabile ha, altresì, obblighi di **garanzia della sicurezza dei dati**, adottando tutte le misure di sicurezza adeguate al rischio (art. 32 regolamento); dovrà inoltre **garantire la riservatezza dei dati, vincolando i dipendenti**, dovrà informare il Titolare delle violazioni avvenute, e dovrà occuparsi della cancellazione dei dati alla fine del trattamento.
Sia il Titolare che il Responsabile del trattamento, sono tenuti ad attuare le **misure tecniche ed organizzative** tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, 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.
Inoltre, il Responsabile ha l'obbligo di **avvisare, assistere e consigliare il Titolare**. Dovrà, quindi, consentire e contribuire alle attività di revisione, comprese le ispezioni (o audit), realizzate dal Titolare del trattamento, dovrà avvisare il Titolare se ritiene che un'istruzione ricevuta viola qualche norma in materia, dovrà prestare assistenza al Titolare per l'evasione delle richieste degli interessati, dovrà avvisare il Titolare in caso di violazioni dei dati, e assisterlo nella conduzione di una valutazione di impatto (DPIA).
La Società per lo svolgimento di talune attività ricorre ad *outsourcer* che si configurano come Responsabili dei trattamenti di dati personali svolti per conto della Società presso la loro sede.

2.1.3 Incaricati del trattamento

Tutti coloro che, nello svolgimento delle proprie mansioni, effettuano operazioni di trattamento di dati personali di cui la FORTNES S.p.a. è titolare, sono nominati, con forma scritta, tramite atto nel quale sono indicati i nominativi e i compiti, compreso gli obblighi inerenti alle misure di sicurezza.
La nomina pertanto è effettuata con specifiche lettere di incarico attraverso le quali a ciascun incaricato sono impartite idonee istruzioni in merito alle misure minime di sicurezza ed alle procedure che devono applicare per un corretto, lecito

[1] Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:
a. tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
b. garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
c. adotti tutte le misure richieste ai sensi dell'articolo 32;
d. rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;
e. tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;
f. assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
g. su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;
h. metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato. Con riguardo alla lettera h) del primo comma, il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

e sicuro trattamento dei dati personali effettuati.
Le suddette istruzioni sono integrate da incontri formativi che il Titolare ovvero Responsabile del trattamento dei dati ha cura di organizzare periodicamente secondo quanto indicato nel paragrafo 5 del presente documento.
Gli Incaricati del trattamento sono autorizzati a trattare i soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati; gli stessi operano nel pieno rispetto delle norme di legge, attenendosi alle istruzioni ricevute
Per ogni incaricato, in relazione alle funzioni previste dal regolamento della struttura organizzativa della Società ed al trattamento dei dati effettuati, è definito un profilo di accesso al sistema informativo in modo che ciascuno possa svolgere unicamente le operazioni definite.
A ciascun Incaricato sono, in particolare, impartite istruzioni relative:

- all'elaborazione della componente riservata della credenziale di autenticazione necessaria per accedere agli elaboratori elettronici e ai dati in essi contenuti; è prescritta l'adozione delle necessarie cautele per assicurarne la segretezza;
- all'uso e custodia dei supporti rimovibili su cui sono memorizzati i dati, al fine di evitare accessi non autorizzati e trattamenti non consentiti;
- al controllo, alla custodia ed archiviazione degli atti e dei documenti contenenti dati personali, affinché adottino specifiche procedure atte a salvaguardare la riservatezza dei dati contenuti.

La lettera di incarico è completata con la consegna di apposite istruzioni, aventi ad oggetto:

- Disposizioni per gli incaricati e linee guida per il trattamento dei dati personali;
- Disposizioni operative;
- Disposizioni su archiviazione materiale cartaceo;
- Disposizioni relative all'adozione delle necessarie cautele per assicurare la segretezza della componente riservata della credenziale di autenticazione e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'Incaricato.

Sono inoltre espressamente designati quali Incaricati del trattamento gli eventuali promotori finanziari e/o collaboratori esterni di cui la società si avvale e che abbiano accesso a dati personali.
Le lettere di incarico, controfirmate da ciascun Incaricato per accettazione, sono trasmesse dal Titolare o dal Responsabile del trattamento dei dati al Responsabile Affari Legali che ha cura di conservarle.
L'elenco degli Incaricati autorizzati a compiere le operazioni di trattamento dei dati nell'ambito della qualifica attribuita a ciascuno di essi è disponibile presso gli uffici del Responsabile Affari Legali.

2.1.4 Il Data Protection Officer (DPO)

Il Responsabile della Protezione dei Dati, ha il compito di informare e consigliare il Titolare o il Responsabile del trattamento da lui preposto, nonché i dipendenti, in merito agli obblighi derivanti dal Regolamento Europeo e dalle altre disposizioni dell'UE o delle normative locali degli Stati membri relative alla protezione dei dati. Deve poi verificare che la normativa vigente e le *policy* interne del Titolare siano correttamente attuate ed applicate, incluse le attribuzioni delle responsabilità, la sensibilizzazione e la formazione del personale, ed i relativi *audit*.
Su richiesta, deve fornire pareri in merito alla valutazione d'impatto sulla protezione dei dati, sorvegliandone poi i relativi adempimenti. Il Responsabile della Protezione dei Dati funge inoltre da punto di contatto sia con il Garante della *Privacy* che con gli interessati, che possono rivolgersi a lui anche per l'esercizio dei loro diritti. E' consentito assegnare al DPO ulteriori compiti e funzioni, a condizione che non diano adito a un conflitto di interessi e che questi gli consentano di avere a disposizione il tempo sufficiente per l'espletamento dei compiti attribuiti dall'art. 39 del Regolamento Europeo.
L'art. 37 del Regolamento Europeo Privacy (GDPR - Regolamento Privacy UE/2016/679) obbliga i Titolari del trattamento e i Responsabili del trattamento a designare un Data Protection Officer (DPO) nei seguenti casi:

- *quando il trattamento (indipendentemente dal tipo di dati trattati) è effettuato da un soggetto appartenente alla pubblica amministrazione (eccetto i soggetti che esercitano funzioni giurisdizionali).*
- *quando le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala* [2].

[2] In particolare il WP29 (Article 29 Data Protection Working Party) ha chiarito che i titolari del trattamento e i responsabili del trattamento (non appartenenti alla pubblica amministrazione) sono soggetti alla nomina del Data Protection Officer (DPO) quando le operazioni chiave necessarie per raggiungere i propri obiettivi istituzionali comportano:

- *il trattamento su larga scala di dati sensibili, genetici, giudiziari e biometrici*

- *quando le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono nel trattamento, su larga scala, di dati sensibili, genetici, giudiziari e biometrici.*

In merito alla obbligatorietà della figura del DPO, il Garante fornisce utili precisazioni, individuando dei casi esemplificativi in cui la nomina del DPO deve considerarsi doverosa. Si tratta ad esempio dei trattamenti di dati personali svolti da:

- istituti di credito;
- imprese assicurative;
- sistemi di informazione creditizia;
- società finanziarie;
- società di informazioni commerciali;
- società di revisione contabile;
- società di recupero crediti;
- istituti di vigilanza;
- partiti e movimenti politici;
- sindacati; CAF e patronati;
- società operanti nel settore delle telecomunicazioni, della distribuzione di energia elettrica o gas e simili;
- imprese di somministrazione di lavoro e ricerca del personale;
- imprese operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione; società di call center; imprese che forniscono servizi informatici;
- società che erogano servizi televisivi a pagamento;
- agenti, rappresentanti, mediatori che operano su larga scala

2.1.5 Funzioni esternalizzate

AMMINISTRATORE DI SISTEMA E CUSTODE DELLE PASSWORD

Il soggetto preposto a sovrintendere alle risorse del sistema operativo e di consentirne l'utilizzazione, l'attribuzione, la gestione dei codici identificativi personali e la custodia delle password è individuato nella società Brain Computing S.r.l.
Per tale Ragione il Titolare del Trattamento ha nominato Brain Computing S.r.l., Responsabile esterno del Trattamento.

GESTORE DEL PROCESSO DI PAYROLL

FORTNES ha affidato ad uno studio esterno il l trattamento dei dati relativi ai dipendenti della Società per quanto concerne il rapporto con gli Istituti (INAIL, INPS, Provincia, Agenzia Entrate, ecc.) e la gestione delle paghe e dei contributi.
Per tale Ragione il Titolare del Trattamento ha nominato tale studio, Responsabile esterno del Trattamento.

2.2 Elenco dei trattamenti dei dati personali effettuati

La società, per lo svolgimento della propria attività, in qualità di Titolare del trattamento, acquisisce e tratta dati personali, relativi alla propria clientela, al personale dipendente, nonché ai soci, amministratori e quanti altri soggetti siano ad essa legati per rapporti di varia natura direttamente, per mezzo della propria struttura, o attraverso collaborazioni esterne.
La società, inoltre, potrebbe anche ricevere la nomina di responsabile ove per attività specifiche, vada a raccogliere e

- *il monitoraggio regolare e sistematico del comportamento di interessati su larga scala (es: tracciamento su internet, geolocalizzazione e profilazione per finalità di pubblicità comportamentale)*

Per valutare se un trattamento possa essere considerato su larga scala è necessario fare un'accurata analisi privacy dei processi aziendali tenendo in considerazione i seguenti parametri:

- *numero di interessati coinvolti*
- *volume e tipologia di dati trattati*
- *durata del trattamento*
- *estensione geografica del trattamento*

Per valutare se un'attività di monitoraggio possa essere considerata regolare e sistematica è, invece, necessario fare un'analisi privacy tenendo in considerazione i seguenti parametri:

- *durata, periodicità e ricorrenza*
- *sistematicità e pianificazione*
- *metodologia organizzativa*
- *strategia aziendale*

trattare dati di titolarità di terzi.
La raccolta ed il trattamento di tali dati, viene effettuato previo rilascio dell'Informativa ai soggetti interessati ed acquisizione del necessario Consenso dagli stessi.

Tabella 1 • ELENCO DEI TRATTAMENTI: ESTRATTO DEL REGISTRO (INFORMAZIONI ESSENZIALI)

Descrizione sintetica del trattamento		Natura dei dati trattati*			Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
Finalità perseguita o attività svolta	Categorie di interessati	P	G	S			
Gestione Forniture	Fornitori	X			Dipendenti Segreteria	Server in cloud	Elenco Fornitori su archivio informatico profilato
Gestione Contratti	Clienti	X	X		Dipendenti Segreteria	Brain Computing	Elenco Fornitori su archivio informatico profilato
Gestione contatti Clienti	Clienti	X	X		Risorse interne Potenziali Clienti	Brain Computing	Sistema Informatico interno con accessi tracciabili e profilati – Brochure, Sito Web e Presentazioni personali – Autorizzazione del Cliente
Gestione del personale	Dipendenti e Collaboratori	X			Clienti e Debitori	Studio dr. Giuseppe Inno	Offerte tecnico-economiche
Recupero Crediti per conto Clienti	Debitori ceduti in gestione	X			Clienti Dipendenti Interni	Brain Computing	Sistema interno Informatico con accessi tracciabili e profilati – Accesso al data base profilato – Firewall ultima generazione – Beckup su server esterni gestiti da Respionsabile estermo (Brain Compunting)
Consulenza legale stragiudiziale e recupero giudiziale	Debitori ceduti in Gestione - Clienti	X		X	Clienti Debitori Avvocati domiciliatari	Brain Computing	Sistemi informativi in uso dal Cliente con accessi profilati – Archivio fisico sotto chiave

***P**: Personali; **G**: Giudiziari, **S**: Sensibili*

2.3 Modalità di trattamento dei dati

Relativamente ai dati per i quali la società effettua il trattamento, si specifica quanto segue:

Dati oggetto del trattamento

- *Dati giudiziari;*
- *Dati relativi a comportamenti illeciti o fraudolenti;*
- *Dati relativi ad altri provvedimenti o procedimenti giudiziari;*
- *Dati relativi ad altri provvedimenti o procedimenti sanzionatori, disciplinari, amministrativi o contabili;*
- *Dati relativi al comportamento debitorio;*
- *Dati relativi alla solvibilità economica;*
- *Dati relativi all'adempimento di obbligazioni;*
- *Dati relativi allo svolgimento di attività economiche e altre informazioni commerciali (es. fatturato, bilanci, aspetti economici, finanziari, organizzativi, produttivi, industriali, commerciali, imprenditoriali).*

Si evidenzia che oggetto di trattamento possono essere anche dati sensibili; questi in particolar modo riguardano i trattamenti conseguenti alla gestione del personale, all'accertamento dell'onorabilità degli amministratori, nonché quelli conseguenti alle ricerche effettuate per conto delle pubbliche autorità (ad esempio Magistratura e Guardia di Finanza), mentre solo occasionalmente ed incidentalmente possono riguardare trattamenti relativi a dati forniti dalla clientela, come ad esempio, in occasione dell'indicazione di una causale di bonifico, che evidenzi dati relativi alla salute ovvero l'adesione ad un partito politico.

Modalità di trattamento dei dati

I dati possono essere trattati con strumenti elettronici ovvero senza l'ausilio di strumenti elettronici. In particolare, le modalità di trattamento sono:

- *Associazione o raffronto di dati anche provenienti da diverse banche dati pubbliche o private;*
- *Definizione di profili dell'interessato;*

- *Organizzazione in banche dati sia in forma automatizzata che non automatizzata;*
- *Raccolta di dati in luoghi pubblici o aperti al pubblico;*
- *Raccolta di dati per via informatica o telematica;*
- *Raccolta di dati presso l'interessato;*
- *Raccolta di dati presso registri, elenchi atti o documenti pubblici;*
- *Raccolta di dati presso terzi;*
- *Raccolta di dati tramite schede, coupon e questionari;*

2.4 Modalità dei trattamenti con strumenti elettronici

La società utilizza il sistema informativo fornito in *outsourcing* dalla Società *Brain Computing* ed un sistema di *storage* e gestione documentale *in cloud*.
Si evidenzia che, non sono ammessi collegamenti, anche temporanei, che, al di fuori della struttura sopra descritta, realizzino connessioni tra elaboratori collegati alla rete della società ed il mondo esterno.
Inoltre, non sono ammessi collegamenti, anche temporanei, che, al di fuori della struttura sopra descritta, realizzino connessioni tra elaboratori della società contenenti dati personali ai sensi del Regolamento.

Inoltre, la Società dispone di linee telefoniche ISDN e di una linea telefonica dedicata alle comunicazioni con il centro elaborazione dati e gestite direttamente dall'*outsourcer*.
Nella seguente tabella si riportano a titolo esemplificativo e non esaustivo i presidi adottati per garantire la sicurezza e disponibilità dei dati.

Tabella 2 • ELENCO ESEMPLIFICATIVO DELLE PRINCIPALI MISURE DI SICUREZZA (INFORMAZIONI ESSENZIALI)

Misure di sicurezza	Descrizione dei rischi Contrastati	Trattamenti interessati	Misura in essere
Sistema autenticazione	Accessi non autorizzati	Trattamenti con strumenti elettronici	*Username* + *password* personali + filtro autorizzazione
Antivirus	Rischio di intrusione e dall'azione di programmi	Trattamenti con strumenti elettronici	Antivirus
Firewall	Protezione degli elaboratori in rete dall'accesso abusivo	Trattamenti con strumenti elettronici	
Aggiornamenti patch sicurezza	Prevenzione della vulnerabilità degli strumenti elettronici	Trattamenti con strumenti elettronici	
Gestione supporti rimovibili	Prevenzione trattamenti non autorizzati	Trattamenti con strumenti elettronici	*Backup* dati, *password* e custodia sotto chiave
Backup/Recovery dati personali	Prevenzione perdita e distruzione dati	Trattamenti con strumenti elettronici	*Backup* interno su doppio *hard disk* protetto da *password* e *Backup* su *Server* esterno gestiti in *outsourcing*
Archivio supporto cartaceo	Accesso non autorizzati	Archivio generale e degli addetti	Custodia in ambiente sotto chiave
Incendio e sicurezza ambientale	Danneggiamento supporti	Tutti i trattamenti	Arredo materiale ignifugo - estintori
Gruppo di continuità	Prevenzione perdita e distruzione dati	Trattamenti con strumenti elettronici	Dotazione gruppo continuità per *server*
Sistema di condizionamento	Prevenzione perdita e distruzione dati	Trattamenti con strumenti elettronici	Tenuta *server* in camera condizionata

2.5 Trattamento dei dati senza l'ausilio di strumenti elettronici

Tale trattamento si concretizza nella conservazione della documentazione cartacea fornita dalla clientela e dai fornitori, ovvero da altri soggetti che hanno contatti con la Società (amministratori, sindaci, dipendenti, consulenti e collaboratori). Di seguito si enumerano le regole di condotta da seguire nel trattamento di detto materiale cartaceo.

1. Il materiale cartaceo in parola deve essere custodito con la diligenza del caso.
2. Nel corso delle quotidiane operazioni di lavoro, tale materiale non dovrà risultare visibile a terze persone o comunque a coloro che non risultino formalmente incaricati di tale specifico trattamento.
3. Tali atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione.
4. Al termine delle sessioni di lavoro, la documentazione contenente dati personali sarà riposta negli appositi archivi.
5. La consegna di elenchi, indirizzari o di dati personali, in qualunque forma (cartacea, ottica, magnetica, ecc.) all'esterno, dovrà essere preventivamente autorizzata dal responsabile dell'unità organizzativa.
6. L'invio del materiale cartaceo a macerazione o l'eliminazione di supporti magnetici, se riguardante dati personali, dovrà essere espressamente autorizzato secondo precise disposizioni.

La documentazione relativa al trattamento di dati sensibili e giudiziari è conservata dagli Incaricati del trattamento, per le finalità connesse allo svolgimento dei propri compiti, sulla base delle previsioni contenute nel Codice per la protezione dei dati personali.

1. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato.
2. Le persone ammesse ad entrare nei locali dell'azienda dopo l'orario di chiusura, a qualunque titolo, devono essere identificate.
3. 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.

3 LA VALUTAZIONE DI IMPATTO (DPIA)

La valutazione di impatto del trattamento (D.P.I.A., cioè *Data Protection Impact Assessment*) è un onere posto direttamente a carico del Titolare del trattamento, col quale si assicura trasparenza e protezione nelle operazioni di trattamento dei dati personali, imponendo al Titolare l'onere di una valutazione preventiva delle conseguenze del trattamento dei dati sulle libertà e i diritti degli interessati. Il Responsabile del trattamento deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria.

La valutazione del rischio, da realizzare per ogni singolo trattamento in modalità *self-assessment*, è finalizzata ad identificare se sussistono rischi elevati inerenti al trattamento e, qualora ritenesse sussistenti detti rischi, individua le misure specifiche richieste per attenuare o eliminare il rischio.

La valutazione di impatto deve contenere almeno:

- la descrizione sistematica dei trattamenti previsti, la finalità del trattamento, compreso l'interesse legittimo perseguito dal Titolare;
- la valutazione dei rischi;
- le misure previste per affrontare i rischi, incluse le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati e dimostrare la conformità al regolamento.

Coerentemente a quanto previsto dall'articolo 35 del regolamento europeo, la valutazione d'impatto, è necessaria nei casi in cui 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:

A. 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;
B. il trattamento riguarda dati sensibili o giudiziari su larga scala;
C. sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

In relazione a tali principi, nell'ambito delle attività svolte dalla Società sono previsti specifici processi valutativi automatizzati e di profilazione verso la clientela nell'ambito dell'espletamento degli adempimenti Antiriciclaggio e di Finanziamento al Terrorismo.

4 CORSI DI FORMAZIONE

Specifica formazione sull'argomento deve essere in ogni caso fornita:

- al momento dell'entrata in servizio, con qualsiasi tipo di contratto di lavoro, ovvero di collaborazione;
- al mutamento delle mansioni che comporti trattamenti di dati diversi da quelli in precedenza lavorati o sensibili;
- all'introduzione di nuovi significativi strumenti in relazione al trattamento di dati;
- al mutamento del quadro di riferimento normativo;
- comunque, almeno una volta all'anno.

5 ATTIVITÀ DI VERIFICA

Il Consiglio di Amministrazione annualmente verifica, anche per il tramite dei *reports* prodotti dalle funzioni di controllo aziendali, le misure di sicurezza adottate.

6 GLOSSARIO

- Dati personali

Tutte le informazioni relative a persone fisiche che consentano l'identificazione, diretta o indiretta, degli individui a cui i dati si riferiscono. Ad esempio, sono dati personali oggetto di tutela, oltre ai dati anagrafici ed economici, anche le immagini ed i codici identificativi riconducibili ad un individuo

- Categorie particolari di dati personali

Dati capaci di rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale

- Dati relativi alla salute

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

- Dati relativi a condanne penali e a reati

Dati relativi a condanne penali e reati o a connesse misure di sicurezza. Il loro trattamento è ammesso solo sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'UE o degli Stati membri, in presenza di garanzie appropriate per i diritti e le libertà degli interessati

- Dati biometrici

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

- Dati genetici

Dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica

- Trattamento

Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione

- Archivio

Qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentrato o ripartito in modo funzionale o geografico

- Titolare del trattamento

La persona fisica o giuridica, l'autorità pubblica o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento

- Contitolare del trattamento

La persona fisica o giuridica che determina congiuntamente ad uno o più titolari le finalità e i mezzi del trattamento. I contitolari definiscono i rispettivi ambiti di responsabilità e compiti in un accordo scritto

- Responsabile del trattamento

La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento. E' nominato dal Titolare, qualora un trattamento debba essere effettuato per suo conto

- Incaricato/Addetto autorizzato

Il soggetto che tratta dati personali sotto l'autorità del Titolare del trattamento o del Responsabile del trattamento su loro specifiche istruzioni

- Amministratore di sistema

Le persone incaricate di gestire e mantenere gli impianti di elaborazione di dati personali o sue componenti. L'attribuzione delle funzioni di Amministratore di sistema avviene previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle disposizioni in materia di trattamento di dati personali. La designazione ad Amministratore è individuale e reca l'elencazione analitica degli ambiti di operatività in base al profilo di autorizzazione assegnato

- Responsabile della protezione dei dati personali (DPO)

La persona fisica che deve essere designata dal Titolare del trattamento e dal Responsabile del trattamento, in specifici casi (ad esempio, se le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala)

- Rappresentante

La persona fisica o giuridica stabilita nell'Unione Europea che, designata per iscritto dal Titolare del trattamento/Responsabile del trattamento non stabilito nell'EU, li rappresenta per quanto riguarda gli obblighi di cui al GDPR

- Profilazione

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

- Pseudonimizzazione

Il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative

- Cifratura

Modalità di conversione del testo originale in una sequenza apparentemente casuale di lettere, numeri e segni speciali che solo la persona in possesso della corretta chiave di decifratura potrà riconvertire nel file di testo originale

- Violazione dei dati personali (*data breach*)

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

- Autorità di controllo

L'autorità pubblica indipendente istituita da uno Stato membro con lo scopo di sorvegliare l'applicazione della normativa sulla protezione dei dati personali, al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali

- Dipendenti

Ogni dipendente assunto con contratto a tempo indeterminato o determinato, *full time* o *part time*, al personale in somministrazione lavoro o *staff leasing*, stagisti e collaboratori, comprese le filiali estere.

FORTNES
CREDIT MANAGEMENT