MODELLO ORGANIZZATIVO PROTEZIONE DEI DATI (MOP)

Identificazione del documento

Codice: IT-TW-MOP00-2019-00V1
Titolo: Modello Organizzativo Privacy

Stato delle edizioni

Edizione n°	*Motivo dell'edizione*	*Data*
1	DPS – D.lgs. 193/ 2003	Marzo 2003
2	Aggiornamento al Regolamento 679/2016	Maggio 2018
3	Aggiornamento per modifica sede e riorganizzazione interna	Settembre 2019

Approvazione ed emissione

	Data	Firma
Verificato ed approvato	23/09/2019	

Sommario

1.FINALITA'

Il Regolamento in materia di protezione dei dati personali (UE) n. 2016/679 (nel seguito, "**GDPR"**) enuclea il principio di *"accountability"* ossia di responsabilizzazione dei soggetti che pongono in essere attività di trattamento di Dati personali.
A tale riguardo, l'art. 24 GDPR prevede che il Titolare del trattamento adotti misure tecniche ed organizzative adeguate ed efficaci al fine di garantire che il trattamento dei Dati personali abbia luogo in conformità alle Leggi sulla protezione dei dati applicabili.
A tal fine Timeware S.r.l. e Timeware Digital hanno ritenuto necessario adottare il presente Modello Organizzativo Privacy (nel seguito, anche il **"MOP"**) al fine di identificare e strutturare i modelli organizzativi e i processi di cui si è dotata per garantire una tutela effettiva ed efficace dei Dati personali di cui è Titolare del Trattamento.

2. AMBITO DI APPLICAZIONE

Il presente MOP si applica agli amministratori, dirigenti, dipendenti, collaboratori, Responsabili del trattamento dei dati, fornitori, consulenti e ad ogni altro soggetto terzo che effettua operazioni di trattamento di Dati personali di cui la Società è Titolare del trattamento.

3. MODIFICHE RISPETTO ALL'EDIZIONE PRECEDENTE

Il documento è stato completamente aggiornato rispetto alle versioni precedenti in base al fatto che le due società hanno ritenuto di sottoscrivere un accordo di Contitolarità successivamente allo spostamento delle sedi e alla riorganizzazione interna.
Dato che le modifiche sono state numerose non si è reputato di evidenziarle in modo puntuale.

4. PIANIFICAZIONE DEGLI INTERVENTI PREVISTI PER IL PROSSIMO PERIODO (2019-2021)

Per il prossimo periodo sono previsti i seguenti interventi.

Attività area tecnologica (Sicurezza Informatica	Stato e scadenza
Misure di sicurezza relative all'accesso ai server sia del personale preposto, sia dei Clienti.	Stato: In pianificazione Scadenza: Entro settembre 2020
Estensione delle misure organizzative e di sicurezza anche al dato non personale legato alla riservatezza e alla sicurezza informatica;	Stato: In pianificazione Scadenza: Entro novembre 2020
Redazione di una nuova policy per l'utilizzo dei mezzi informatici	Stato: in corso Scadenza: Entro dicembre 2020

Attività area amministrativa	Stato e scadenza
Integrazione delle misure di sicurezza fisiche relative ai documenti cartacei e non ancora informatizzati;	Entro dicembre 2020
Redazione di un nuovo documento che contenga tutti i riferimenti e i contatti dei Fornitori e dei Clienti	Entro dicembre 2020
Valutazione dell'introduzione della figura del DPO (anche se non obbligatoria ex lege)	Entro dicembre 2020
Introduzione di una policy relativa ai nuovi colleghi	Entro dicembre 2020

4. DEFINIZIONI

Ai fini della seguente Policy, i termini e le espressioni definite avranno il significato nel seguito indicato. Le espressioni al singolare manterranno lo stesso significato al plurale, ove il contesto lo richieda. Si riportano nel seguito le definizioni rilevanti ai fini della presente Procedura:

Atto di Nomina o Nomina	Indica l'atto di nomina di volta in volta adottato dal Titolare volto a regolamentare il Trattamento dei dati personali effettuato da parte dei Responsabili del trattamento. Tale Nomina costituisce parte integrante e sostanziale della presente Policy.
Autorità	indica l'Autorità Garante per la Protezione dei Dati personali**.**
Autorizzati	indica i dipendenti della Società autorizzati dal Titolare a compiere operazioni di trattamento nell'esercizio delle funzioni agli stessi affidate.
Cancellazione dei Dati personali	indica la distruzione definitiva – fisica o tecnica – idonea a rendere non più recuperabili mediante gli ordinari mezzi disponibili in commercio le informazioni contenute in un supporto elettronico e/o cartaceo.
Consenso dell'Interessato	indica qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'Interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i Dati personali che lo riguardano siano oggetto di trattamento.
Data Breach	indica una 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 oggetto di trattamento.
Data Breach Policy	indica la Procedura adottata dalla Società al fine di disciplinare le opportune modalità di gestione del Data Breach.

Data Manager	indica i dipendenti designati direttamente dal Titolare che, nello svolgimento delle proprie funzioni e nei limiti dei poteri loro attribuiti, sono deputati alla gestione e al monitoraggio dei Trattamenti effettuati nell'ambito della propria attività.
Dati personali	indica qualsiasi informazione riguardante una persona fisica identificata o identificabile e che possa fornire dettagli sulle sue caratteristiche fisiche, le sue abitudini, il suo stile di vita, lo stato di salute, l'orientamento politico, la situazione economica, etc.
Destinatari	indica gli amministratori, i dirigenti, i dipendenti, i collaboratori, i Responsabili del trattamento dei dati, i fornitori e i soggetti terzi che effettuano operazioni di trattamento dei dati di cui la Società è Titolare e nei confronti dei quali trova applicazione la presente Policy e le relative Procedure che formano parte integrante della stessa.
Informativa	indica le informative ai sensi degli artt. 13 e 14 del GDPR che il Titolare rende di volta in volta in favore degli interessati. Tali informativo costituiscono parte integrante e sostanziale della presente Policy.
Interessato	indica la persona fisica a cui si riferiscono i Dati personali oggetto di trattamento.
Leggi sulla protezione dei dati	indica tutte le leggi e i regolamenti, inclusi ma non limitati al Regolamento (UE) 2016/679 in materia di protezione delle persone fisiche con riguardo al Trattamento dei Dati personali, nonché alla libera circolazione dei dati (GDPR) e al Codice in materia di protezione dei Dati personali ex D.lgs. 196/2003 e successive modifiche (Codice Privacy) nonché provvedimenti di volta in volta in vigore che sono applicabili al Trattamento dei Dati personali.

Policy Privacy	indica la presente Policy organizzativa adottato dalla Società al fine di garantire la corretta gestione e implementazione dei presidi previsti dalle Leggi sulla protezione dei dati. Costituiscono parte integrante e sostanziale della presente Policy, le Procedure e il Registro dei Trattamenti.
Paese terzo	indica un paese esterno allo Spazio Economico Europeo.
Privacy Officer	indica la funzione individuata dal Titolare che sovraintende all'implementazione e all'aggiornamento dei presidi previsti dalle Leggi sulla protezione dei dati.
Procedura	Si indicano le policy e procedure adottate dalla Società al fine di regolamentare i diversi aspetti legati al trattamento dei Dati personali. A mero titolo esemplificativo, rientrano nella definizione di Procedura: Registro delle attività di trattamento Data Retention Policy (Allegato A) la Data Breach policy (Allegato B), la Procedura per l'esercizio dei diritti degli Interessati (Allegato C). Le Procedure formano parte integrante e sostanziale del presente Modello.
Procedura per l'esercizio dei diritti degli Interessati	indica la procedura adottata dal Titolare al fine di disciplinare le azioni da compiere da parte dei soggetti coinvolti nelle operazioni di Trattamento di Dati personali di cui Timeware S.r.l. è Titolare al fine di agevolare e garantire l'esercizio dei Diritti degli Interessati.
Procedura sulla conservazione dei Dati Personali o *Data Retention Policy*	indica la procedura volta a illustrare le linee guida che la Società ha inteso adottare in materia di conservazione dei Dati personali e garantire che tali prescrizioni, nonché le misure di sicurezza. Tale procedura individua, infine, il rispetto dei diritti di cancellazione dei Dati personali esercitati dagli Interessati.

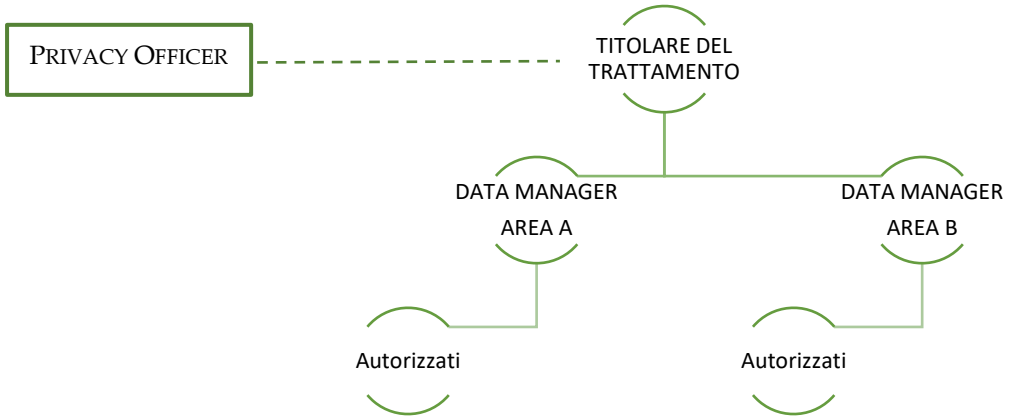
Registro dei Trattamenti	indica il presidio che la Società, ai sensi dell'art. 30 GDPR, ha implementato al fine di mappare le operazioni di trattamento dei Dati personali di cui è Titolare del trattamento dei dati.
Responsabile del trattamento dei Dati (Data Processor)	indica l'entità esterna alla Società che tratta Dati personali per conto del Titolare del trattamento dei dati.
GDPR	indica il Regolamento Generale sulla protezione dei dati n. 2016/679.
Titolare del trattamento dei dati o il Titolare (Data Controller)	indica l'entità che determina le finalità e i mezzi di trattamento dei Dati personali, in questo caso Timeware S.r.l., con sede legale in Strada 1, palazzo F5 Milanofiori 20090, Assago (MI).
Trattamento	indica 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
WP29	Indica il Gruppo Articolo 29 ossia un organismo consultivo indipendente composto da un rappresentante delle varie autorità nazionali, dal Garante Europeo della protezione dei dati, nonché da un rappresentante della Commissione Europea.

4. RUOLI E RESPONSABILITÀ

Il Modello Organizzativo Privacy di cui si è dotata la Società si articola su diversi livelli, riconoscendo poteri e relative responsabilità in capo a diversi soggetti:

- **Il Titolare del trattamento (Data Controller)**
  È il soggetto che determina le finalità e i mezzi del Trattamento dei Dati personali.
  Il Titolare del trattamento è la società Timeware S.r.l. ed alla stessa spetta il compito di adottare le misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il Trattamento dei Dati personali sia effettuato conformemente alle Leggi sulla protezione dei dati. In particolare, il Titolare è chiamato, a titolo esemplificativo e non esaustivo, a:
  - Adottare le soluzioni di *privacy by design* e *privacy by default;*
  - Aggiornare il Registro dei trattamenti;
  - Predisporre le Informative relative al Trattamento dei Dati personali;
  - Predisporre ogni adempimento organizzativo necessario per garantire agli Interessati l'esercizio dei diritti;
  - Disporre l'adozione dei provvedimenti imposti dall'Autorità;
  - Effettuare la valutazione d'impatto ai sensi dell'Art. 35 GDPR;
  - Consultare l'Autorità nei casi e secondo le modalità previste dall'Art. 36 GDPR;
  - Nominare i Responsabili del trattamento.
- Il **Privacy Officer** è il soggetto che è chiamato a supervisionare e a sovrintendere il rispetto del Modello Organizzativo Privacy da parte dei Destinatari. Nell'espletamento delle sue funzioni, il Privacy Officer deve assistere il Titolare nell'attuazione delle Procedure, fungendo altresì da punto di contatto per gli Interessati e i Destinatari.
- **I Data Manager** sono i soggetti designati direttamente dal Titolare che, nello svolgimento delle proprie funzioni e nei limiti dei poteri loro attribuiti, sono deputati alla gestione e al monitoraggio dei Trattamenti effettuati nell'ambito della propria attività. Il Data Manager, nell'esercizio delle sue funzioni, deve assistere il Titolare nell'attuazione delle Procedure, fungendo altresì da punto di contatto per gli Interessati e i Destinatari
- **Gli Autorizzati/Incaricati al trattamento** sono tutti i soggetti che effettuano operazioni di trattamento di Dati personali, ivi inclusi i dipendenti e collaboratori che operano a qualsiasi titolo sotto la diretta autorità e secondo le istruzioni impartite dal Titolare e/o del Data Manager gerarchicamente superiore.
- **I Responsabili del trattamento** sono i soggetti terzi, esterni all'organizzazione della Società, che effettuano per conto e sotto le istruzioni del Titolare le operazioni di trattamento dei dati di cui la Società è Titolare. I Responsabili del trattamento devono essere nominati mediante atto di nomina in conformità alle prescrizioni di cui all'art. 28 GDPR.
- **I Sub-responsabili del trattamento** sono i soggetti terzi, esterni all'organizzazione della Società, nominati dal Responsabile del trattamento mediante apposito atto di nomina che impone al Sub-responsabile gli stessi obblighi in materia di protezione dei dati contenuti nell'atto di nomina a responsabile esterno del trattamento.

4.1 Flow Chart Data Protection Governance



5. LICEITÀ

I Trattamenti effettuati dalle Società avvengono esclusivamente nel rispetto dei criteri di liceità individuati ai sensi dell'art. 6 del GDPR.
In particolare, il trattamento è lecito solo e nella misura in cui ricorra almeno una delle seguenti condizioni:

a) L'Interessato ha espresso il **consenso al trattamento** dei propri Dati personali per una o più specifiche finalità;
b) Il trattamento è necessario **all'esecuzione di un contratto di cui l'Interessato è parte** o all'esecuzione di **misure precontrattuali** adottate su richiesta dello stesso;
c) Il trattamento è necessario **per adempiere un obbligo legale** al quale è soggetto il Titolare;
d) Il trattamento è necessario **alla salvaguardia degli interessi vitali dell'Interessato o di un'altra persona fisica;**
e) Il trattamento è necessario per **l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri** di cui è investito il Titolare;
f) Il trattamento è necessario per il perseguimento del **legittimo interesse** del Titolare, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'Interessato che richiedono la protezione dei Dati personali, in particolare se l'Interessato è un minore.

A tal riguardo i Destinatari sono tenuti ad accertarsi, prima di porre in essere qualsivoglia operazione di Trattamento di Dati Personali, la sussistenza di almeno uno dei requisiti di liceità sopra indicati.
In caso di dubbi relativi alla liceità del trattamento o in merito alla base giuridica da utilizzare in relazione allo specifico trattamento i Destinatari possono inviare una mail al seguente indirizzo privacy@timeware.it.

5.1 Consenso

Nel caso in cui il Trattamento dei Dati personali si fondi sul consenso al Trattamento espresso dall'Interessato, il Titolare deve essere in grado di dimostrare che l'Interessato abbia effettivamente fornito il suo consenso. Il consenso reso dagli Interessati deve essere:

- ✓ **Informato:** ossia preceduto da adeguata informativa;
- ✓ **Libero:** ossia senza condizionamenti o vincoli;
- ✓ **Specifico:** ossia riferibile ad una singola finalità;
- ✓ **Inequivocabile:** ossia deve risultare certo che l'Interessato lo abbia prestato;
- ✓ **Espresso:** ossia non deve risultare dal silenzio o inattività dell'Interessato.

Nel caso in cui il consenso sia fornito nel quadro di una dichiarazione scritta riguardante anche altri temi, la richiesta di consenso dovrà essere presentata in maniera chiaramente distinguibile dagli altri temi, in una forma comprensibile e facilmente accessibile, con un linguaggio chiaro e semplice. È necessario altresì prevedere dei meccanismi che consentano all'Interessato di poter revocare in qualsiasi momento il consenso precedentemente prestato. La revoca del consenso non compromette la liceità del Trattamento sulla base del consenso prestato precedentemente.

A tal riguardo i Destinatari sono tenuti ad assistere il Titolare in sede di raccolta del consenso da parte degli Interessati e di relativa conservazione dello stesso. Gli Autorizzati e i Data Manager, ove nominati, sono, inoltre, tenuti ad assistere il Titolare affinché lo stesso possa garantire il diritto di revoca del consenso eventualmente esercitato dagli Interessati nei confronti del Titolare.

5.2 Legittimo interesse

Nel caso in cui il Titolare intenda fondare il Trattamento dei Dati personali sul legittimo interesse di cui è portatore, è necessario che il Titolare effettui **preliminarmente** un **test comparativo** atto a verificare la liceità del Trattamento medesimo. L'anzidetto test comparativo consta delle seguenti fasi:

a) **Purpose Test:** è necessario, in primo luogo, stabilire se l'interesse perseguito dal Titolare sia legittimo. Pertanto, tale interesse è conforme alle Leggi sulla protezione dei dati applicabili, qualora sia sufficientemente concreto e/o reale, e non meramente teorico.
b) **Necessity Test:** è necessario, in secondo luogo, che il Titolare stabilisca se il Trattamento dei Dati personali sia necessario al fine di perseguire l'interesse aziendale legittimo, verificando se il trattamento sia proporzionato ed adeguatamente mirato al raggiungimento dei suoi scopi. A tale riguardo è altresì necessario verificare se possano essere utilizzati altri mezzi, meno invasivi, per raggiungere tale scopo.
c) **Balancing Test:** è necessario, in terzo luogo, effettuare una comparazione tra il legittimo interesse di cui è portatore il Titolare e i diritti o gli interessi fondamentali dell'Interessato.

Tale valutazione deve necessariamente tenere conto dei seguenti indici:

- ✓ L'interesse del Titolare;
- ✓ Le conseguenze derivanti da un eventuale mancato Trattamento;
- ✓ Il carattere sensibile dei dati oggetto di eventuale trattamento;
- ✓ La posizione dell'Interessato rispetto a una posizione dominante del Titolare (e.g. dipendente/datore di lavoro);
- ✓ Le modalità con cui i Dati personali sarebbero trattati;

- ✓ Le conseguenze derivante da tale tipologia di trattamento sui diritti e/o gli interessi fondamentali dell'Interessato
- ✓ Le ragionevoli aspettative dell'Interessato;
- ✓ Le conseguenze negative del trattamento sull'Interessato rispetto al beneficio auspicato.

Nel caso in cui all'esito delle predette valutazioni emerga che il legittimo interesse del Titolare prevale sugli interessi degli Interessati, il Titolare dovrà informarli in merito alle motivazioni per le quali il Titolare ha ritenuto di essere portatore di un interesse legittimo, i presidi adottati e le ragioni poste a fondamento della prevalenza degli interessi del Titolare su quelli dell'Interessato.
Nel caso in cui all'esito del test comparativo emerga la permanenza di conseguenze significative sull'Interessato, le operazioni di trattamento dei dati non potranno fondarsi sull'interesse legittimo del Titolare ma dovrà essere utilizzata una differente base giuridica che legittimi il Trattamento dei Dati personali.
In ogni caso, il Titolare è tenuto a documentare per iscritto il test comparativo, avendo cura di archiviare la documentazione inerente al bilanciamo effettuato e ai relativi esiti. A tale riguardo, il Data Manager coinvolto nel Trattamento, ove nominato, e/o gli Autorizzati sono tenuti ad assistere il Titolare nell'espletamento del test comparativo. Il Data Manager coinvolto e il Privacy Officer, sono tenuti a conservare, sotto la sua responsabilità, tutte la documentazione inerente, conseguente ed accessoria al test comparativo.

6. TRASPARENZA

Il Titolare può raccogliere ed effettuare operazioni di Trattamento dei Dati personali solo nella misura in cui il Trattamento sia corretto e legittimo.
In particolare, il GDPR e le raccomandazioni formulate dal WP29 pongono a carico del Titolare un obbligo di *trasparenza* nei confronti degli Interessati.
In particolare, l'Informativa resa agli Interessati deve essere **concisa, trasparente, intellegibile e facilmente accessibile**, con linguaggio semplice e chiaro.
Le Informative rese agli Interessati devono contenere almeno le seguenti informazioni:

- ➢ Identità e dati di recapito del Titolare e, ove applicabile, del rappresentante del Titolare e del DPO;
- ➢ Le categorie di Dati personali raccolti e trattati, nonché la fonte da cui sono stati raccolti;
- ➢ Le finalità del Trattamento, nonché la base giuridica del Trattamento;
- ➢ Gli eventuali destinatari o le eventuali categorie di destinatari dei Dati personali;
- ➢ L'intenzione del Titolare di trasferire i Dati personali a paesi o organizzazioni internazionali terzi e l'esistenza o l'assenza di una decisione di adeguatezza da parte della Commissione Europea, ovvero il riferimento ad adeguate o idonee tutele, nonché i mezzi per ottenere una copia di tali dati o il luogo ove sono stati resi disponibili.
- ➢ Il periodo di conservazione dei Dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- ➢ L'esistenza dei seguenti diritti in capo all'Interessato:
  - Diritto di accesso,
  - Diritto di rettifica,
  - Diritto di cancellazione,
  - Diritto alla limitazione del trattamento,

- Diritto di opporsi al trattamento,
- Diritto alla portabilità dei dati,
- Diritto di presentare reclami all'Autorità.

- Nel caso in cui il Trattamento si fondi sul **Consenso dell'Interessato**, è necessario informare quest'ultimo della possibilità di revocare il consenso precedentemente prestato in qualsiasi momento, senza pregiudicare la liceità del trattamento basato sul consenso prestato prima della revoca;
- Se la comunicazione di Dati personali è un obbligo legale o contrattuale ovvero un requisito necessario per la conclusione di un contratto, e se l'Interessato ha l'obbligo di fornire i Dati personali, nonché le possibili conseguenze della mancata comunicazione dei Dati personali;
- L'esistenza di decisioni automatizzate tra cui la profilazione e, in tal caso, informazioni significative sulla logica adottata e la rilevanza e le conseguenze di tale trattamento per l'Interessato.
- Chi contattare in caso di domande e/o richieste di accesso.

Nel caso in cui la base giuridica del Trattamento sia il legittimo interesse del Titolare, occorre che l'Informativa rechi l'indicazione di tali interessi.
I Destinatari sono incaricati della corretta diffusione delle Informative in favore degli interessati.
In caso di nuove operazioni di Trattamento il Privacy Officer e il Data Manager di riferimento, ove nominato, sono tenuti a coinvolgere il Titolare al fine di verificare che l'Informativa precedentemente resa sia coerente con il nuovo trattamento che si intende effettuare e se vi sia o meno la necessità di informare nuovamente l'Interessato.

Es. Se viene introdotta una nuova area all'interno dell'organizzazione aziendale.

➔ Bisognerà provvedere ad un'analisi dei dati trattati e procedere all'informazione dei vari Interessati

7. NOMINA DEI RESPONSABILI DEL TRATTAMENTO DEI DATI

Il Titolare si impegna a trasferire i Dati personali nei confronti di soggetti terzi che effettuano operazioni di Trattamento dei dati per conto del Titolare stesso.
A tale riguardo, tutte le volte in cui un soggetto terzo effettui operazioni di Trattamento di Dati personali per conto e su istruzione documentata del Titolare, quest'ultimo provvede a nominare il soggetto terzo mediante Atto di Nomina a Responsabile esterno del trattamento ai sensi dell'art. 28 GDPR.
Nel caso in cui il soggetto terzo nominato Responsabile esterno del trattamento si avvalga di un altro responsabile (**Sub-responsabile**), il Titolare provvede a rilasciare autorizzazione scritta al responsabile esterno del trattamento.

L'elenco completo dei soggetti terzi nominati in qualità di responsabili esterni del trattamento e degli eventuali sub-responsabili è disponibile facendone opportuna richiesta al seguente indirizzo mail privacy@timeware.it.
Per la gestione del Trattamento dei Dati personali effettuato da parte di soggetti terzi per conto del Titolare la Società ha adottato dei format di Atti di Nomina.
A tal riguardo, il Privacy Officer e i Data Manager, ove nominati, ogni qualvolta vi sia la necessità di provvedere alla nomina di soggetti terzi quali Responsabili del trattamento sono tenuti ad assistere il Titolare al fine di garantire la corretta implementazione di tale presidio.

ES. Se i dati dei dipendenti vengono inviati al consulente lavoro per le buste paga.

➔ Bisognerà inviare una nomina a Responsabile del Trattamento

7. FUNZIONE INTERNE

7.1. Referente Privacy (Privacy Officer)

Il Referente Privacy (Privacy Officer) è nominato dal Titolare del in funzione dell'esperienza professionale, delle competenze specialistiche in materia di protezione dei dati personali nonché della conoscenza del business aziendale.

Il Referente privacy svolge un ruolo di collegamento tra il DPO, gli Incaricati e gli Organi aziendali del Titolare e collabora con il DPO svolgendo le attività dettagliate nell'allegato F al presente Modello Organizzativo Policy.

8. TRASFERIMENTO DEI DATI PERSONALI VERSO PAESI TERZI

Il trasferimento di Dati personali oggetto di un Trattamento o destinati ad essere oggetto di un Trattamento dopo il trasferimento verso un Paese terzo può avvenire solo qualora ricorra almeno una delle seguenti condizioni:

(A) il Paese terzo abbia ricevuto da parte della Commissione Europea **una decisione di adeguatezza**;

(B) il Titolare può trasferire Dati personali verso un paese terzo o un'organizzazione internazionale solo se ha fornito **garanzie adeguate** e a condizione che gli Interessati dispongano di diritti azionabili e mezzi di ricorso effetti. Possono costituire garanzie adeguate, a titolo esemplificativo:

- le norme vincolanti d'impresa;
- le clausole tipo di protezione dei dati adottate dalla Commissione Europea;
- le clausole tipo di protezione dei dati adottate da un'autorità di controllo e approvate dalla Commissione Europea;
- un codice di condotta ex art. 40 GDPR;
- un meccanismo di certificazione approvato ai sensi dell'art. 42 GDPR.

A tal riguardo i Destinatari sono tenuti ad accertarsi, prima di porre in essere qualsivoglia operazione di trasferimento di Dati Personali, la sussistenza di almeno uno dei requisiti sopra

indicati. In caso di dubbi relativi alla possibilità di trasferire tali dati verso paesi terzi devono rivolgersi al Privacy Officer**.**

***Attualmente**, i seguenti paesi hanno ricevuto una decisione di adeguatezza da parte della Commissione Europea ai sensi dell'art. 25, comma 6 Direttiva 95/46/CE:*
- Andorra - Israele
- Argentina - Jersey
- Australia - Nuova Zelanda
- Canada - Uruguay
- Faer Oer - Guernsey

UE – USA
Il Privacy Shield fra UE e USA è un meccanismo di autocertificazione per le società stabilite negli USA che intendano ricevere dati personali dall'Unione europea, al fine di tutelare la riservatezza dei dati personali dei cittadini europei in caso di trasferimento oltreoceano a scopo commerciale.

***Importante:** è necessario verificare preliminarmente se il soggetto terzo americano risulti certificato all'interno della c.d. Privacy Shield List consultando il sito: https://www.privacyshield.gov/list*

9. PRINCIPIO DI PROPORZIONALITÀ, MINIMIZZAZIONE DEI DATI E LIMITAZIONE DELLA CONSERVAZIONE

Il Titolare può raccogliere e trattare solo i Dati personali rilevanti, non oltre la finalità specifica del Trattamento definito. Pertanto, in caso di raccolta di Dati personali è necessario che il Titolare si chiede i Dati personali raccolti sono necessari per perseguire la finalità della società e se la finalità è legittima. Bisogna che il Titolare si chieda, inoltre, se le finalità da perseguire possano essere raggiunte anche senza la necessità di trattare i Dati personali.
Ove possibile, i dati dovranno essere trattati in forma anonimizzata o pseudonomizzata.
Il Titolare e i Destinatari trattano i Dati personali esclusivamente per le finalità indicate al momento della raccolta dei Dati personali. Nel caso in cui le finalità del trattamento fossero oggetto di modifica è necessario ottenere, ove necessario, il consenso da parte dell'Interessato per il perseguimento delle nuove finalità ovvero verificare se il perseguimento delle nuove finalità sia ammesso dalla normativa applicabile. I Destinatari sono tenuti a consultare il Titolare per ottenere maggiori informazioni e supporto nello stabilire la legittimità delle finalità, su come documentarla e ottenere l'ulteriore consenso degli Interessati.
Fermo quanto precede, i Destinatari trattano i Dati personali per il **tempo strettamente necessario a conseguire gli scopi per cui i Dati personali sono stati raccolti,** a meno che obblighi legali prevalenti impongano periodi di conservazione più lunghi o più brevi. I Dati personali non più utilizzati devono essere distrutti o anonimizzati.
A tale scopo, il Titolare ha provveduto ad adottare la Procedura sulla conservazione dei Dati personali (i.e. *Registro delle attività di trattamento e Data Retention Policy*), di cui all'Allegato A, finalizza all'individuazione di precisi limiti temporali nella conservazione delle varie tipologie e categorie di dati (in ossequio al principio della "limitazione della conservazione del dato" sancito dal GDPR), nonché i soggetti responsabili dei processi di cancellazione e anonimizzazione dei Dati

personali. A tale ultimo riguardo, per garantire la conformità al predetto principio sono stati implementati dei sistemi di archiviazione configurati in modo tale da garantire la cancellazione completa o l'anonimizzazione dei Dati personali, oltre che una revisione periodica di tutti i sistemi di archiviazione contenenti Dati personali.

10. PROCEDURA DI GESTIONE DELLE VIOLAZIONI DEI DATI

Un Data Breach è una 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 oggetto di trattamento**.**

Non tutte le violazioni della sicurezza rientrano nella definizione di Data Breach. Affinché si configuri un Data Breach la violazione deve **comportare un rischio per i diritti e le libertà delle persone.**

Ciò significa che tale violazione deve essere suscettibile di avere un effetto significativo e dannoso sugli individui, ad esempio, causare discriminazione, danni alla reputazione, perdita finanziaria, perdita di riservatezza o qualsiasi altro significativo svantaggio economico o sociale. Si rende quindi necessario effettuare una valutazione caso per caso al fine di verificare se sia occorso o meno un Data Breach.

Al fine di garantire una maggiore comprensione, indichiamo nel seguito alcuni esempi di incidenti di sicurezza che potrebbero comportare un Data Breach:

- Perdita di backup contenente Dati personali;
- Accesso a banche dati da parte di soggetti non autorizzati;
- Attacco Hacker al sistema informatico;
- Furto o smarrimento di computer, laptop, devices elettronici portatili, chiavette USB, smartphones/iPad aziendali;
- Ransomware;
- Phishing.

In forza del principio di *accountability*, ossia di responsabilizzazione, che informa la normativa in materia di protezione dei Dati personali, il Titolare ha implementato la *Data Breach Policy*, di cui all'Allegato B, ossia una Procedura tesa ad individuare le azioni necessarie da implementare tutte le volte in cui sia occorsa una violazione dei Dati personali ovvero vi sia una sospetta violazione dei Dati personali.

I Destinatari sono tenuti a segnalare ogni potenziale violazione dei dati di cui possano venire a conoscenza, inviando un'e-mail a privacy@timeware.it.

11. PROCEDURA PER L'ESERCIZIO DEI DIRITTI DEGLI INTERESSATI

Il GDPR consente agli Interessati di richiedere al Titolare di:

- ✓ accedere ai propri dati e ricevere informazioni relative ai trattamenti effettuati dal Titolare (Art. 15 GDPR);
- ✓ ottenere la rettifica dei Dati personali inesatti che lo riguardano (Art. 16 GDPR);
- ✓ richiedere la cancellazione dei propri dati (Art. 17 GDPR);
- ✓ ottenere, ove consentito, la limitazione del trattamento (Art. 18 GDPR);
- ✓ ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i Dati personali che lo riguardano (Art. 20 GDPR);
- ✓ opporsi in qualsiasi momento al trattamento dei Dati personali che lo riguardano (Art. 21 GDPR);

- ✓ non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla persona (Art. 22 GDPR).

Da ultimo, il GDPR conferisce agli Interessati il diritto di proporre reclamo all'Autorità ai sensi dell'art. 77 GDPR nel caso in cui l'Interessato ritenga che il trattamento che lo riguardi violi il GDPR.
Al fine di favorire e garantire il corretto ed efficace esercizio dei diritti da parte degli Interessati, il Titolare ha predisposto la Procedura per l'esercizio dei diritti dell'Interessato, di cui all'Allegato 3, finalizzata ad individuare le modalità attraverso le quali gli Interessati possono esercitare agevolmente i loro diritti. L'anzidetta Procedura individua altresì i soggetti deputati alla gestione delle richieste avanzate dagli Interessati e le relative modalità e tempistiche di gestione delle richieste.
A tal riguardo, i Destinatari sono tenuti, in conformità con quanto previsto dalla Procedura per l'esercizio dei diritti degli interessati, ad assistere il Titolare al fine di consentire allo stesso la corretta gestione delle richieste presentate dagli Interessati.

12. REGISTRO DEI TRATTAMENTI

Il Titolare ha provveduto ad implementare il Registro dei Trattamenti finalizzato a mappare le diverse operazioni di trattamento dei Dati personali effettuate sotto la responsabilità dei Data Manager.
Il Registro dei Trattamenti è un utile strumento per la completa ricognizione e valutazione dei Trattamenti effettuati e, pertanto, è finalizzato anche all'analisi del rischio e ad una corretta pianificazione dei Trattamenti.
Il Titolare è responsabile alla corretta tenuta del Registro dei Trattamenti, nonché alla sua integrazione ed aggiornamento. A tale riguardo i Data Manager di riferimento, ove nominati e/o gli Autorizzati sono tenuti ad assistere il Titolare al fine di espletare le predette funzioni inerenti la tenuta del Registro dei trattamenti.

13. VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

In linea generale, in forza del principio di ***privacy by design*** è necessario che il Titolare, al fine di tutelare i diritti e le libertà degli Interessati con riguardo al Trattamento dei Dati personali, attui adeguate misure tecniche e organizzative fin al momento della progettazione del Trattamento stesso.
Tutte le volte in cui un determinato tipo di Trattamento dei Dati personali possa presentare **un rischio elevato per i diritti e le libertà delle persone fisiche**, il Titolare 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.
La valutazione d'impatto è tesa a descrivere il Trattamento dei Dati personali, valutandone la necessità e la proporzionalità, nonché a contribuire alla gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal Trattamento stesso, valutando detti rischi e determinando le misure per affrontarli.
La valutazione d'impatto deve essere effettuata fin dalla fase di progettazione del Trattamento, benché alcune operazioni di trattamento non siano ancora note.
Ai sensi dell'Art. 30 RGPD il Registro dei Trattamenti contiene tutte le seguenti informazioni:

i. *il nome e i dati di contatto del Titolare e, ove applicabile, del Contitolare del trattamento, del rappresentante del Titolare e del RPD;*

ii. ***le finalità*** *del trattamento;*
iii. *c) una descrizione delle* ***categorie di Interessati*** *e delle* ***categorie di dati personali***
iv. *le* ***categorie di destinatari*** *a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;*
v. *ove applicabile,* ***i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale****, compresa l'identificazione del paese terzo o dell'organizzazione internazionale, nonché la documentazione delle garanzie adeguate, ove applicabile;*
vi. *ove possibile,* ***i termini*** *ultimi previsti* ***per la cancellazione*** *delle diverse categorie di dati;*
vii. *ove possibile, una* ***descrizione generale delle misure di sicurezza tecniche e organizzative*** *implementate.*

A titolo esemplificativo: un rischio elevato potrebbe presentarsi qualora il trattamento comporti:
- l'uso di nuove tecnologie;
- la profilazione degli Interessati;
- il trattamento di dati sensibili o aventi carattere altamente personale;
- il monitoraggio sistematico degli Interessati (ivi inclusa la sorveglianza);
- il trattamento di dati relativi a Interessati vulnerabili

Nel caso in cui ricorra la necessità e/o l'opportunità di effettuare una valutazione di impatto, il Data Manager di riferimento e i Destinatari sono tenuti ad assistere il Titolare fornendo tutte le informazioni necessarie ai fini della valutazione.
Il Titolare è tenuto a conservare, sotto la sua responsabilità, tutta la documentazione inerente, conseguente ed accessoria alla valutazione d'impatto.
Al fine di effettuare una valutazione d'impatto, il Titolare è tenuto ad effettuare:

- una descrizione sistematica dei Trattamenti previsti e delle finalità del Trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal Titolare;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità perseguita;
- una valutazione dei rischi per i diritti e le libertà degli Interessati;
- 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 presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli Interessati e delle altre persone in questione.

Nel caso in cui, all'esito della valutazione di impatto, il Titolare ritenga che il rischio non possa essere ragionevolmente attenuato in termini di tecnologie disponibili e di costi di attuazione e dovesse risultare dalla valutazione d'impatto che il trattamento (in mancanza delle garanzie, delle misure di sicurezza e dei meccanismi per attenuare il rischio) possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, dovrà ricorrere alla **consultazione preventiva dell'Autorità** ai sensi dell'art. 36 GDPR.

14. FORMAZIONE

Per un efficace funzionamento del Modello, la formazione degli Autorizzati e dei Data Manager, ove nominati, è gestita dalla Società in stretta cooperazione con un consulente esterno.
In particolare, i corsi di formazione hanno ad oggetto l'intero Policy in tutte le sue componenti nonché le nozioni relative alle Leggi sulla protezione dei dati applicabili.
La partecipazione ai corsi di formazione è monitorata attraverso un sistema di rilevazione delle presenze.
Al termine di ogni corso di formazione è sottoposto al partecipante un test finalizzato a valutare il grado di apprendimento conseguito ed ad orientare ulteriori interventi formativi.
La partecipazione ai corsi di formazione è obbligatoria per tutto il personale in servizio presso la Società.
Tale obbligo costituisce una regola fondamentale della presente Policy, alla cui violazione sono connesse le sanzioni previste nel sistema disciplinare.
I Destinatari della formazione, sono tenuti a:

- ➔ acquisire conoscenza dei principi e dei contenuti della Policy;
- ➔ conoscere le modalità operative con le quali deve essere realizzata la propria attività;
- ➔ contribuire attivamente, in relazione al proprio ruolo e alle proprie responsabilità, all'efficace attuazione della Policy, segnalando eventuali carenze riscontrate nello stesso.

15. INOSSERVANZA DELLA POLICY PRIVACY

Si porta a conoscenza di tutti i Destinatari che la presente Policy Privacy, nonché le Procedure che ne formano parte integrante, ha carattere vincolante per i Destinatari.
Eventuali violazioni della presente Policy e delle Procedure allegate che formano parte integrante e sostanziale della presente, da intendersi integralmente richiamate e trascritte, possono avere gravi ripercussioni sulla Società e comportare, nei confronti del dipendente inadempiente, l'applicazione di provvedimenti disciplinari, in conformità alle disposizioni di legge e del CCNL applicabile e nei confronti degli altri Destinatari anche la cessazione del rapporto contrattuale.
I comportamenti che costituiscono violazione della presente Policy possono determinare, nel contempo, la violazione di disposizioni di legge tali da implicare per l'utilizzatore inadempiente conseguenze di natura civile e penale.
Anche la Società può essere perseguita e sanzionata in conseguenza della condotta dei Destinatari.
Agli stessi potrà dunque venire richiesto di risarcire i danni derivati dalle violazioni della presente Procedura.

16. CONTATTI

In caso di quesiti o dubbi in merito all'applicazione del presente Policy Privacy e/o in merito a qualsivoglia Procedura, si prega di contattare:

- Privacy Officer: Massimo Goldaniga
- E-mail: privacy@timeware.it
- Responsabile IT: Angelo Galli
- E-mail: angelo.galli@timeware.it
- Tel.: +39 02 87209260

17. ELENCO DEGLI ALLEGATI

- ALLEGATO A – REGISTRO DELLE ATTIVITA' DI TRATTAMENTO E DATA RETENTION POLICY
- ALLEGATO B – DATA BREACH
- ALLEGATO C – POLICY PER IL DIRITTO DEGLI INTERESSATI
- ALLEGATO D - MODELLI UTILIZZATI NEL MODELLO ORGANIZZATIVO PRIVACY
    - D.01. Informativa dipendenti
    - D.02. Informativa Clienti / Fornitori
    - D.03. Informativa Sito Internet
    - D.04. Informativa Cookie
    - D.05. Informativa Videosorveglianza
    - D.06. Informativa Visitatori Sede
    - D.07. Informativa Covid – 19
    - D.08. Moduli Data Breach
    - D.09. Moduli Esercizio diritti degli Interessati
    - D.10. Atto Nomina Responsabile Esterno al Trattamento
    - D.11. Atto Nomina Amministratore di sistema
    - D.12. Piano di Formazione
- ALLEGATO E - ELENCO DEI RESPONSABILI ESTERNI AL TRATTAMENTO NOMINATI
- ALLEGATO F –NOMINA PRIVACY OFFICER E MANSIONI ATTRIBUITE