MODELLO ORGANIZZATIVO PRIVACY

LUFTHANSA TECHNIK MILAN S.R.L.

Rev.	Data	Natura della modifica
00	02/05/2024	Prima adozione

Indice

INTRODUZIONE

Il presente Modello Organizzativo Privacy ("***MOP***") è il documento utilizzato da Lufthansa Technik Milan S.r.l. (di seguito anche la "**Società**" o "**LTMIL**") per descrivere le misure tecniche e organizzative adottate al fine di garantire un livello di sicurezza adeguato al rischio connesso al trattamento dei dati effettuati da LTMIL ai sensi dell'art. 32 del Regolamento Europeo n. 679/2016 (di seguito anche "***GDPR***" o "***Regolamento***").

Il MOP è inoltre sottoposto ad aggiornamento periodico, al fine di perseguire costantemente la piena conformità dello stesso alla normativa vigente, alle pronunce giurisprudenziali e alle pronunce del Garante Privacy.

Nel presente Modello Organizzativo Privacy trovano descrizione i principi fondamentali che regolamentano il trattamento dei dati personali e ne garantiscono la protezione, nonché i ruoli previsti dal GDPR e l'organizzazione privacy definita da LTMIL in qualità di Titolare.

Costituiscono, inoltre, parte integrante del presente MOP tutti i regolamenti/linee guida/istruzioni operative/procedure adottate da LTMIL al fine di fornire specifiche indicazioni relative alla produzione, gestione, conservazione e trasmissione dei dati personali. Tra essi si collocano, tra l'altro, i documenti atti a definire le modalità di gestione dei sistemi informativi impiegati, le precauzioni di tipo tecnologico e fisico adottate, nonché le procedure e policy interne atte ad individuare i tempi di conservazione di ciascuna macrocategoria di dati.

Costituiscono parte integrante del presente Modello, in particolare:

1. Procedura di *data breach management*;
2. Procedura di gestione delle nomine a *data processor*;
3. Procedura per la gestione dei trasferimenti in paesi terzi;
4. Procedura di valutazione dei rischi connessi al trattamento.

Definizioni

Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
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;
Titolare del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
Regolamento o GDPR	Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
Interessato	La persona fisica cui si riferiscono i dati personali
Autorità di controllo	L'autorità pubblica indipendente istituita da uno Stato membro. In Italia l'Autorità di controllo è il Garante Privacy.
Misure di sicurezza	Insieme di tutti gli accorgimenti tecnici ed organizzativi utilizzati per garantire che i dati non vadano distrutti o persi anche in modo accidentale, nonché l'accesso ai dati alle sole persone autorizzate.

1. Riferimenti normativi e documentali

Il Modello Organizzativo Privacy di LTMIL è stato redatto in modo da garantire la puntuale applicazione:

- del Regolamento Europeo n. 679/2016;
- delle Linee Guida adottate dal Gruppo WP291 in relazione alla corretta applicazione del Regolamento UE/679/2016.
- del Codice in materia di protezione dei dati personali, Decreto legislativo 30 giugno 2003, n. 196 (anche, di seguito, "**Codice Privacy**"), e ss.mm.ii.;
- dei successivi provvedimenti emanati dal Garante per la protezione dei dati personali, tra cui in particolare:
  - Provvedimento del Garante Privacy del 23 novembre 2006 in materia di trattamento dei dati personali dei lavoratori con riferimento alla gestione del rapporto di lavoro;
  - Provvedimento del Garante Privacy del 27 novembre 2008 e successive modificazioni relativamente agli Amministratori di Sistema;
  - Provvedimento del Garante Privacy del 29 aprile 2010 in materia di videosorveglianza;
- delle linee guida emanate da *European Data Protection Board* e delle decisioni della Commissione Europea, quali, ad esempio:
  - *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*, adottate il 18 giugno 2021;
  - Decisione di esecuzione (UE) 2021/914 della Commissione del 4 giugno 2021 relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi a norma del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio;
  - Decisione di esecuzione (UE) 2021/915 della Commissione del 4 giugno 2021 relativa alle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento a norma dell'art. 28, par. 7, del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio e dell'art. 29, par. 7, del Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio;
- delle procedure interne adottate dal Titolare.

2. Principi che regolano il trattamento dei dati

Nello svolgimento di ogni attività di trattamento dei dati, LTMIL opera in conformità ai seguenti principi sanciti dalla normativa nazionale e comunitaria.

- **Liceità, correttezza e trasparenza**

Art. 5, par. 1, lett. a) Reg. UE/679/2016

❖ Cfr. Considerando 39, 40, 44 Reg. UE/679/2016

"I dati personali sono … trattati in modo lecito, corretto e trasparente nei confronti dell'interessato".

LTMIL si impegna ad eseguire esclusivamente trattamenti leciti ai sensi della normativa nazionale ed europea. Pertanto, ogni autorizzato al trattamento tratta dati personali esclusivamente in forza delle diverse basi giuridiche previste dagli artt. 6 o 9 del GDPR.
LTMIL assicura, inoltre, la trasparenza dei trattamenti eseguiti, con particolare riferimento alle finalità e modalità del trattamento, attraverso la diffusione di informative facilmente accessibili, comprensibili e redatte con linguaggio chiaro e semplice.

- **Limitazione della finalità**

Art. 5, par. 1, lett. b), Reg. UE/679/2016

❖ Cfr. Considerando 28, 50 e art. 6, par. 1, lett. b) Reg. UE/679/2016

"I dati personali sono … raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'art. 89, par. 1, considerato incompatibile con le finalità iniziali".

LTMIL predefinisce le finalità di ogni trattamento eseguito e raccoglie dati personali solo se strettamente necessari al perseguimento di tali finalità.

- **Minimizzazione dei dati**

Art. 5, par. 1, lett. c), Reg. UE/679/2016

❖ Cfr. art. 25, par. 2, Reg. UE/679/2016

"I dati personali sono … adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati".

LTMIL raccoglie i dati funzionali ed essenziali al perseguimento delle finalità per cui il dato è trattato. Il trattamento non è eseguito in tutti i casi in cui le medesime finalità sono realizzabili mediante dati anonimi o altre modalità che rendano non determinabile l'identità dell'interessato.

Inoltre, LTMIL ha definito e formalizzato diversi livelli autorizzativi per ogni funzione aziendale. Pertanto, ogni soggetto autorizzato al trattamento dei dati può accedere esclusivamente alle categorie di dati essenziali per lo svolgimento della propria mansione lavorativa.

- **Esattezza dei dati**

Art. 5, par. 1, lett. d), Reg. UE/679/2016

"I dati personali sono … esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati".

LTMIL effettua specifiche verifiche atte ad accertare l'esattezza dei dati dalla raccolta del dato fin alla sua cancellazione. A tal fine, durante il periodo di trattamento dei dati, LTMIL effettua verifiche periodiche atte ad accertare la correttezza dei dati originariamente raccolti.

- **Limitazione della conservazione**

Art. 5, par. 1, lett. e), Reg. UE/679/2016

❖ Cfr. Considerando 39 e art. 89 Reg. UE/679/2016

"I dati personali sono … conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'art. 89, par. 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato".

LTMIL ha definito i tempi di conservazione di ogni tipologia di dato personale trattato. I tempi di conservazione sono stati definiti in base alla finalità per cui il dato è trattato, nonché in attuazione a quanto previsto negli obblighi contrattuali e normativi.

- **Integrità e riservatezza**

Art. 5, par. 1, lett. f), Reg. UE/679/2016

❖ Cfr. Considerando 39 Reg. UE/679/2016

"I dati personali sono … trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali".

LTMIL ha adottato misure, tecniche e organizzative idonee a salvaguardare la correttezza del processo di raccolta e gestione dei dati, la loro sicurezza e protezione in caso di intrusioni e alterazioni non autorizzate. Il dettaglio dei presidi adottati è contenuto in apposita sezione del Registro del trattamento ex art. 30 GDPR.

- **Principio di *Accountability***

Art. 24, Reg. UE/679/2016

❖ Cfr. Considerando 74 Reg. UE/679/2016

"Il Titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento al Regolamento, compresa l'efficacia delle misure".

LTMIL ha implementato un sistema di gestione del rischio privacy, individuando i rischi connessi al trattamento, valutando tali rischi in termini di origine, natura, probabilità e gravità, nonché individuando le migliori prassi per attenuare il rischio.

- ***Privacy by design* e *by default***

Art. 25, Reg. UE/679/2016

❖ Cfr. Considerando 78 Reg. UE/679/2016

"Il Titolare del trattamento, al fine di dimostrare la conformità con il presente regolamento, dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default".

LTMIL ha previsto che il *Data Protection Coordinator* sia coinvolto ogniqualvolta si renda necessario adottare un nuovo processo organizzativo o nuovo sistema informatico o in caso di utilizzo di nuove tecnologie, in modo che possa valutare fin dalla fase di progettazione l'impatto privacy del nuovo processo, individuare eventuali misure adeguate al contenimento del rischio ed aggiornare il Registro dei trattamenti.

3. I soggetti coinvolti nel trattamento di dati personali

Il Regolamento delinea un sistema tripartito composto dal Titolare del trattamento, dal Responsabile del trattamento (d'ora in avanti definito anche "*Data Processor*") e dai soggetti autorizzati al trattamento, la definizione dei quali è fondamentale nell'applicazione del GDPR.

Ognuna di tali figure è caratterizzata da una diversa ampiezza di poteri e responsabilità, modulati in relazione al ruolo assegnato e alle attività concretamente svolte con riferimento al trattamento delle categorie di dati personali. La corretta individuazione di tali figure assume, infatti, un ruolo cruciale per la tenuta e l'efficienza del sistema privacy della Società, determinando chi è responsabile per il rispetto delle diverse norme sulla protezione dei dati ed il modo in cui gli interessati possono esercitare i loro diritti nel concreto.

Il **Titolare del trattamento** è l'ente che determina in modo autonomo ed esclusivo le finalità e i mezzi del trattamento. Inoltre, il Titolare è sempre l'organizzazione in quanto tale e non un individuo all'interno della stessa.
Ai sensi dell'art. 24 GDPR, il Titolare ha la responsabilità di valutare i rischi inerenti al trattamento, nonché di adottare le misure tecniche ed organizzative adeguate a garantire ed essere in grado di dimostrare che lo stesso venga svolto conformemente al GDPR.

Il **Responsabile del trattamento/*Data Processor*** è la persona fisica o giuridica, l'autorità pubblica o altro organismo che tratta dati personali per conto del Titolare del trattamento. Ai sensi dell'art. 28 GDPR, i trattamenti effettuati da parte del *Data Processor* devono poi essere disciplinati da un contratto o da altro atto giuridico che vincola il *Data Processor* e stabilisce la durata, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e diritti del Titolare.

I **soggetti autorizzati al trattamento** ex art. 29 GDPR e art. 2-*quaterdecies* Codice Privacy sono coloro che hanno accesso ai dati personali forniti dal Titolare e che ricevono da esso istruzioni per il trattamento, trovandosi sotto la responsabilità e nell'ambito dell'assetto organizzativo del Titolare.
Ai sensi della normativa vigente, è dunque necessario che ogni persona autorizzata al trattamento sia opportunamente informata/formata sull'ambito di estensione delle proprie mansioni e competenze.

3.2. L'organigramma privacy di Lufthansa Technik Milan S.r.l.

Alla luce dei principi di cui al paragrafo che precede **LTMIL è Titolare del trattamento** ai sensi dell'art. 24 GDPR.

La Società, dunque, tramite il proprio rappresentante legale provvede a:

i) definire le modalità e finalità dei trattamenti eseguiti e le categorie di dati trattati;
ii) adottare tutte le misure tecniche ed organizzative necessarie per garantire la sicurezza dei dati trattati;
iii) verificare ed aggiornare periodicamente le misure tecniche ed organizzative adottate;
iv) scegliere consapevolmente i soggetti coinvolti nel trattamento dei dati ed istruirli adeguatamente;
v) in caso di violazioni, porre in essere contro-misure tempestive ed effettive e effettuare le comunicazioni dovute ai sensi di legge.

LTMIL, in qualità di Titolare del trattamento, ha provveduto alla individuazione e alla designazione del ***Data Protection Coordinator***, ossia di una figura che possa fungere da punto di contatto tra il *management* aziendale ed il personale.

Il *Data Protection Coordinator* è tenuto a verificare l'effettiva applicazione della vigente normativa, nazionale ed europea, e del sistema di gestione privacy adottato da LTMIL nonché di ogni altro documento ad esso connesso, all'interno dell'area di sua competenza.

Pertanto, rientrano tra i compiti assegnati al *Data Protection Coordinator*:

- la nomina per conto del Titolare dei soggetti designati al trattamento dei dati personali;
- l'attività di sensibilizzazione dei soggetti designati sulla rilevanza del tema privacy nelle attività quotidiane;
- il supporto ad ogni soggetto designato al trattamento per l'analisi e la risoluzione di dubbi/difficoltà connesse al trattamento dei dati;
- la verifica che le istruzioni impartite dal Titolare – e comunicate attraverso qualsiasi strumento – siano effettivamente conosciute dai soggetti designati;
- la verifica che tutte le misure tecniche e organizzative, volte ad evitare rischi di distruzione, perdita, accesso non autorizzato o trattamento non consentito definite dal Titolare siano scrupolosamente osservate;
- la valutazione annuale circa l'adeguatezza delle misure di protezione, tecniche e organizzative, adottate;
- la compilazione del Registro dei trattamenti *ex* art. 30 GDPR ed il suo aggiornamento periodico, nelle parti di propria competenza;
- l'identificazione delle terze parti che assumo il ruolo di *Data Processor* e la vigilanza sul rispetto della designazione e delle istruzioni impartite.

Il *Data Protection Coordinator* è, inoltre, tenuto a comunicare al Titolare:

- ogni eventuale difficoltà riscontrata nell'esercizio della propria funzione;
- le variazioni apportate ai livelli di sicurezza vigenti;
- ogni carenza e/o inadeguatezza delle misure di protezione adottate dal Titolare nelle aree di propria competenza;
- le richieste di esercizio dei diritti ricevute dagli Interessati;
- ogni comportamento od evento che possa determinare una violazione del sistema di gestione privacy adottato dal Titolare o che, più in generale, sia rilevante ai fini della normativa in materia di protezione dei dati personali;
- ogni circostanza idonea a determinare anche solo potenzialmente una violazione dei dati (es. dispersione, distruzione, accesso non autorizzato e comunque trattamenti non consentiti).

I **dipendenti** di LTMIL che hanno accesso a dati personali sono **soggetti autorizzati al trattamento** e nello svolgimento della propria attività devono rispettare il presente Modello Organizzativo Privacy, le indicazioni in materia di protezione dei dati personali contenute nelle procedure di regolamentazione interne, nonché tutte le istruzioni impartite dal Titolare.

Al riguardo, il Titolare, in applicazione dell'art. 2-*quaterdecies* del D. Lgs. 196 del 2003, fornisce a ciascuno di questi una specifica lettera di designazione, in cui sono ampiamente descritti il ruolo e i compiti loro attribuiti nel trattamento dei dati, nonché le istruzioni cui dovranno attenersi

nell'esercizio delle loro funzioni e attribuzioni. In particolare, questi sono tenuti ad operare con la massima diligenza e attenzione, in modo tale che i dati siano:

- trattati in modo lecito, corretto e non eccedente rispetto alle finalità per le quali sono stati raccolti;
- registrati, utilizzati e raccolti per scopi attinenti alle mansioni assegnate a ciascun Ufficio;
- conservati per un periodo non superiore a quello necessario per gli scopi del trattamento;
- non comunicati e/o diffusi all'esterno a soggetti non autorizzati in qualunque forma e per qualunque finalità, se non previa autorizzazione del Titolare del trattamento.

Ogni soggetto autorizzato al trattamento è poi tenuto a comunicare al *Data Protection Coordinator*:

- ogni eventuale difficoltà riscontrata nell'esercizio della propria mansione,
- ogni comportamento od evento che possa determinare una violazione della normativa interna in materia di protezione dei dati personali o che, più in generale, sia rilevante ai fini della normativa nazionale ed europea sul punto;
- ogni circostanza idonea a determinare potenzialmente una violazione dei dati (es. dispersione, distruzione, accesso non autorizzato e comunque trattamenti non consentiti), nel rispetto della Procedura di *data breach* allegata al presente MOP;
- ogni richiesta di esercizio dei diritti formulata dagli interessati e le informazioni necessarie per assolvere le legittime richieste provenienti dall'interessato.

La Società provvede inoltre alla nomina dei *Data Processor*, ossia i Responsabili del trattamento ex art. 28 GDPR.
Nell'individuare i soggetti da nominare, il *Data Protection Coordinator* – avvalendosi del supporto di professionisti specializzati – applica i seguenti criteri fondamentali:

- ✓ che sia un'entità distinta e separata rispetto al Titolare del trattamento;
- ✓ che tratti dati personali per conto ed in nome del Titolare del trattamento e su sua documentata istruzione (fermo restando che le istruzioni del Titolare del trattamento possono lasciare un certo grado di discrezionalità consentendo al *Data Processor* di scegliere la soluzione tecnica e organizzativa più adatta al caso concreto).

Sono Responsabili del trattamento alcuni fornitori che svolgono servizi per conto della società, ad esempio, gli *outsourcers* che forniscono applicativi *software*, nonché le società e i consulenti che forniscono servizi e consulenza.

La circostanza per cui il *Data Processor* sia tenuto a trattare dati per conto del Titolare implica necessariamente che il *Data Processor* "entri a far parte del "sistema privacy" del Titolare e, di conseguenza, sia tenuto a trattare i dati secondo le istruzioni del Titolare. Per tale ragione, il Titolare deve preliminarmente verificare, in una fase precedente alla sottoscrizione di un contratto con un fornitore, se la controparte, al fine di eseguire il contratto, necessiti di trattare i dati personali di titolarità di LTMIL. In caso affermativo, al Titolare è richiesto di accertare che la controparte possa mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti di cui al GDPR e garantisca la tutela dei diritti dell'interessato (art. 28, par. 1 del GDPR).

Qualsiasi trattamento di dati personali da parte di un *Data Processor* deve essere regolato da un contratto o da un altro atto giuridico vincolante, da concludere in forma scritta, anche in formato elettronico.

Tutti i fornitori nominati *Data Processors* sono essere inseriti nel Registro dei *Data Processors*, nel quale andrà annotato anche il giorno di sottoscrizione della nomina a *Data Processor* ed eventuali verifiche svolte sul *Data Processor*, ed in cui si darà atto degli ulteriori *Data Processor* eventualmente nominati e del trasferimento di dati extra-UE, se realizzato. La regolare tenuta ed il costante aggiornamento del Registro dei *Data Processors* rientra nei compiti del *Data Protection Coordinator*.

Le modalità di individuazione e nomina dei *Data Processors* sono dettagliate in apposita procedura aziendale.

Tutta la documentazione che riguarda le attività in oggetto è conservata in apposito spazio di condivisione *cloud* posto a disposizione del *Data Protection Coordinator*.

3.3. Rapporto con l'Autorità di controllo

Ogni Stato membro istituisce una o più autorità pubbliche indipendenti con il compito di *sorvegliare l'applicazione del presente regolamento 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 all'interno dell'Unione* (art. 51 GPDR).
L'Autorità di controllo italiana è il **Garante della Privacy** ed esso è competente a conoscere eventuali violazioni di dati personali (*Data breach*) e ad accogliere, nonché decidere su eventuali reclami presentati dagli interessati.
In caso di ispezioni in materia di protezione dei dati personali o di richieste di informazioni e documentazione da parte del Garante della privacy o di altre Autorità, ogni soggetto autorizzato è tenuto a informare tempestivamente il *Data Protection Coordinator*, che si coordina con il Titolare del trattamento coinvolto.

4. Gli standard applicati al trattamento dei dati

Ogni dipendente di LTMIL che, nell'esercizio delle proprie mansioni aziendali, tratti dati personali, deve attenersi scrupolosamente alle istruzioni fornite nei seguenti paragrafi nonché alle *policies* e procedure allegate al presente Modello.

4.1. Prescrizioni generali

Tutti i soggetti autorizzati al trattamento dei dati per conto di LTMIL devono:

I. effettuare solo i trattamenti espressamente indicati all'interno del Registro dei trattamenti;
II. osservare scrupolosamente tutte le misure di sicurezza tecniche e organizzative, volte ad evitare rischi di distruzione, perdita, accesso non autorizzato o trattamento non consentito descritte nel presente MOP e nelle procedure in esso richiamate;
III. osservare le misure di protezione e sicurezza per il trattamento dei dati su supporto cartaceo, consistenti nella custodia in contenitori muniti di serratura e comunque di difficile accesso ai soggetti non autorizzati;
IV. mantenere il proprio spazio lavorativo in ordine e libero da documenti contenenti dati personali e/o riservati, in quanto presidio necessario per il rispetto della privacy, nonché della normativa interna a tutela della riservatezza dei dati;
V. rispettare tutte le istruzioni previste nel presente Modello.

Si precisa che non è consentito raccogliere dati personali se non previsto esplicitamente da norme, regolamenti e procedure del Titolare del trattamento o su formale richiesta dell'interessato, previa autorizzazione di questo.

4.2. Informative e consenso

Ogni soggetto autorizzato al trattamento che raccoglie dati personali direttamente dall'interessato o tramite terzi deve preventivamente verificare che il medesimo abbia ricevuto l'informativa privacy, documento in cui trovano specificazione le modalità e finalità del trattamento, diversamente fornire all'interessato l'idonea informativa.

Ciascuno deve prestare particolare attenzione a tale adempimento, che si configura con un elemento cruciale per la liceità del trattamento. L'eventuale acquisizione di dati personali in assenza di un'idonea base giuridica rende inutilizzabili i dati stessi e l'eventuale conseguente trattamento illegittimo.

Specificamente, quando le informazioni sono raccolte direttamente presso l'interessato, l'informativa deve essere rilasciata al momento di acquisizione dei dati stessi.

Nel caso in cui i dati personali non sono ottenuti presso l'interessato, l'informativa deve essere resa al momento di prima comunicazione con l'interessato (si pensi al caso della selezione del personale affidata a un *head hunter* esterno; al momento del primo contatto con il candidato per lo svolgimento del colloquio, dovrà essere fornita la relativa informativa).

Inoltre, per ogni categoria di soggetti interessati sono predisposte informative specifiche che devono essere rilasciate seguendo le seguenti istruzioni:

- l'informativa ai potenziali dipendenti/collaboratori (coloro che inviano la propria spontanea candidatura ad una posizione professionale all'interno di LTMIL) deve essere resa al momento del primo contatto utile successivo all'invio del *curriculum* (ad esempio al primo colloquio);
- l'informativa deve essere resa al dipendente contestualmente alla lettera di assunzione;

- l'informativa al cliente e al fornitore è presente nel *footer* delle e-mail del personale con cui lo stesso entra in contatto ed è richiamata nel correlato contratto/ordine;
- l'informativa al visitatore è inclusa nel modulo di accesso che il visitatore è tenuto a compilare al momento dell'ingresso nei locali aziendali.

Per le ipotesi sopra non specificate, si rimanda ai principi generali e si precisa che l'informativa deve essere resa in tutte le ipotesi in cui il Titolare tratti dati personali precedentemente raccolti per finalità diverse da quelle originariamente comunicate all'interessato.

Nel caso in cui nell'informativa si chieda all'interessato l'espressione del consenso per un determinato trattamento, il soggetto che sottopone l'informativa deve tenere traccia del consenso eventualmente prestato in modo tale che sia:

1. rinvenibile la data esatta in cui il consenso è stato prestato;
2. tracciabile lo specifico trattamento e la specifica finalità per cui l'interessato ha prestato il consenso;
3. accessibile anche agli altri autorizzati al trattamento del Titolare.

Le informative sottoscritte dagli interessati sono archiviate dal soggetto autorizzato al trattamento che raccoglie dati personali direttamente nella cartella dedicata all'interessato (ad esempio fascicolo del dipendente).

4.3. Trattamento dei dati archiviati in formato cartaceo

Non è consentita l'archiviazione di dati personali al di fuori degli archivi ufficiali.
Nel caso in cui un soggetto incaricato necessitasse di costituire un archivio locale dovrà darne preventiva comunicazione al *Data Protection Coordinator* che valuterà la sussistenza di idonee garanzie (es. collocazione in un locale chiuso a chiave, uso di armadi chiusi a chiave, ecc.).

4.4. Trattamento dei dati archiviati su sistemi informatici

Non è consentita l'archiviazione di dati personali o di documenti contenenti dati personali al di fuori dei device aziendali (computer personale) o al di fuori dei data base, gestionali e applicativi messi a disposizione da ciascun Titolare.
Nel caso in cui un soggetto incaricato necessitasse di costituire un apposito e separato archivio elettronico dovrà darne preventiva comunicazione al *Data Protection Coordinator* che valuterà la sussistenza di idonee garanzie con il supporto dei Sistemi Informativi Aziendali.

4.5. Formazione

Il Titolare del trattamento, avvalendosi del supporto del *Data Protection Coordinator*, organizza sessioni di formazione in materia di protezione dei dati personali nei seguenti momenti:

- al momento dell'ingresso di nuovo personale;
- al cambio mansione;
- a seguito di modifiche organizzative interne o di modifiche normative che abbiano influenza sulla gestione e protezione dei dati personali.

5. I Registri del Trattamento

A norma dell'art. 30, GDPR, LTMIL ha predisposto ed aggiorna il Registro dei trattamenti eseguiti in qualità di Titolare e di *Data Processor* al fine di fornire un quadro aggiornato dei trattamenti in essere all'interno della Società.

Il presente paragrafo è finalizzato a supportare tutti i soggetti coinvolti a vario titolo nella tenuta e nell'aggiornamento del Registro del trattamento *ex* art. 30, par. 1 e 2, del GDPR.

5.1. Il Registro dei Trattamenti in qualità di Titolare (art. 30, par. 1 del GDPR)

Il Registro dei Trattamenti predisposto da LTMIL in qualità di Titolare è tenuto in forma scritta ed in formato elettronico (Excel e tramite applicativo software "*Prime*", fornito dal Gruppo).

La creazione e l'aggiornamento del Registro del Trattamento di cui all'art. 30, par. 1, del GDPR costituiscono un valido strumento di valutazione, analisi e gestione dei rischi connessi ai trattamenti effettuati dal Titolare.

L'aggiornamento del Registro è di competenza del *Data Protection Coordinator* e l'impulso e supporto dei Responsabili di Dipartimento.

L'aggiornamento è necessario ogniqualvolta venga effettuato un nuovo trattamento oppure modificato uno già registrato.

5.2. Il Registro dei Trattamenti in qualità di *Data Processor* (art. 30, par. 2 del GDPR)

Al momento della redazione del presente Modello Organizzativo Privacy, LTMIL non svolge trattamenti in qualità di *Data Processor*.

Ad ogni modo, si forniscono le indicazioni cui la predisposizione, l'aggiornamento e la regolare tenuta di un Registro del *Data Processor* devono ispirarsi.

Al pari del Registro del Titolare, anche il Registro del *Data Processor* è tenuto in forma scritta ed in formato elettronico; è costituito da più righe dedicate a specifici trattamenti, ai quali corrispondono almeno le seguenti colonne:

I. Titolare del trattamento in nome e per conto del quale si effettuano i trattamenti di dati personali;
II. Soggetto interno di LTMIL, che segue e supervisiona il trattamento;
III. Denominazione del trattamento effettuato in nome e per conto del Titolare;
IV. Una serie di ulteriori informazioni a completamento, quali:
    a. le tipologie di dati personali trattati e di interessati coinvolti;
    b. le informazioni relative ad eventuali trasferimenti verso un paese terzo o un'organizzazione internazionale;
    c. ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.

La predisposizione e l'aggiornamento del Registro quale *Data Processor* si svolge secondo quanto prescritto nel par. 5.1 che precede.

5.3. Assegnazione delle basi giuridiche

In ossequio al principio di liceità, trasparenza e correttezza, il Titolare del trattamento esegue i trattamenti di dati personali solo nei casi in cui ricorra una delle basi giuridiche di cui all'art. 6 del

GDPR, nonché, in relazione ai dati appartenenti a categorie particolari di dati o ai dati relativi a condanne penale e a reati, rispettivamente in relazione agli artt. 9 e 10 del GDPR.

Nella maggior parte dei trattamenti, il Titolare ricorre alle basi giuridiche di cui all'art. 6, par. 1, lett. b) - esecuzione di misure precontrattuali adottate su richiesta dell'interessato ed esecuzione del contratto -, di cui all'art. 6, par. 1, lett. c) - obbligo legale – in alcuni casi in correlazione con l'art. 10 GDPR relativo al trattamento di dati relativi a condanne penali e a reati, nonché di cui all'art. 9, par. 2, lett. b) del GDPR.

Il ricorso alla base giuridica dell'interesse legittimo è del tutto residuale e limitato a specifici trattamenti. In tal caso, il Titolare si impegna a svolgere preventivamente un bilanciamento tra l'interesse proprio o di terzi e degli interessi, diritti e libertà fondamentali dell'interessato. Tale bilanciamento sarà eseguito a cura del *Data Protection Coordinator* con il supporto dei Responsabili di Dipartimento eventualmente coinvolti. Il bilanciamento dovrà dare evidenza delle ragioni a sostegno della prevalenza dell'interesse legittimo del Titolare sui diritti dell'interessato.

Nelle ipotesi in cui il bilanciamento attesti la prevalenza dell'interesse del Titolare o di terzi, il trattamento è legittimamente avviato e traccia scritta del bilanciamento con correlato esito è archiviato a cura del *Data Protection Coordinator*. Di contro, nei casi in cui prevalgano gli interessi, le libertà e i diritti dell'interessato, il trattamento non può essere avviato per carenza di un'idonea base giuridica.

6. Il *Data Breach*

Per *data breach* si intende 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 trasmessi, conservati o comunque trattati.

In particolare, gli eventi di *Data Breach* possono essere suddivisi in tre macrocategorie:

- **Violazione di confidenzialità** *(confidentiality breach)*: divulgazione o accesso non autorizzato o accidentale ai dati personali;
- **Violazione di disponibilità** *(availability breach)*: perdita accidentale o non autorizzata dell'accesso ai dati o distruzione di dati personali;
- **Violazione di integrità** *(integrity breach)*: alterazione non autorizzata o accidentale dei dati personali.

A titolo esemplificativo, e non esaustivo, vengono riportate di seguito alcune tipologie di violazione dei dati personali:

- **distruzione di dati informatici o documenti cartacei**, intesa come indisponibilità irreversibile di dati con accertata impossibilità di ripristino degli stessi, conseguente a eliminazione logica (es. errata cancellazione dei dati nel corso di un intervento manuale o automatizzato o fisica, rottura di dispositivi di memorizzazione informatica, incendio/allagamento di locali dove sono archiviati i contratti e altri documenti dei clienti);
- **perdita di dati, conseguente a smarrimento/furto di supporti informatici** (es. laptop, tablet, HD, memory card) **o di documentazione contrattuale o altri documenti cartacei** (in originale o in copia);
- **accesso non autorizzato o intrusione a sistemi informativi**, inteso come lo sfruttamento di vulnerabilità dei sistemi interni e delle reti di comunicazione oppure attraverso la compromissione o rilevazione abusiva di credenziali di autenticazione (es. userid e password) per l'accesso ai sistemi;
- **modifica non autorizzata di dati**, derivante, ad esempio, da un'erronea esecuzione di interventi sui sistemi informatici o da interventi umani;
- **rivelazione di dati e documenti a soggetti terzi non legittimati, anche non identificati**, conseguenti ad esempio alla fornitura di informazioni, anche verbali, a persone diverse dal soggetto legittimato (in assenza di delega formale di quest'ultimo), all'invio di fatture o altri documenti di valore contrattuale o esecutivo, all'errata gestione di supporti informatici.

6.1. Riferimenti normativi e linee guida

Ai sensi degli artt. 33 e 34 del GDPR, in caso di *data breach*, il Titolare del trattamento deve notificare il *data breach*, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne sia venuto a conoscenza, all'Autorità di controllo, a meno che sia improbabile che il *data breach* presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'Autorità di controllo non avvenga effettuata entro 72 ore, è corredata dei motivi del ritardo.

Inoltre, l'art. 34 GDPR (*Comunicazione di una violazione dei dati personali all'interessato*) al par. 1 dispone che quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

Nel caso in cui la violazione si verifichi nell'ambito di un trattamento dei dati che un *Data Processor* svolge per conto di un Titolare, il *Data Processor* è tenuto ai sensi dell'art. 33, par. 2 GDPR a informare il Titolare senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione. La comunicazione, in ogni caso, indica i dati, le categorie e il numero degli interessati, la violazione circostanziata, le conseguenze attuali e potenziali, le misure prese in risposta.

Ulteriori riferimenti normativi ed interpretativi sono contenuti:

- nelle Linee Guida dell'Agenzia dell'Unione Europea per la sicurezza delle reti e dell'informazione (ENISA) e ulteriori parametri tratti dall'art. 3, par. 2 reg. (UE) n. 611/2013;
- nelle Linee Guida del Gruppo di Lavoro WP29 sulla notifica delle violazioni dei dati personali – WP250 rev.01;
- nelle comunicazioni della Commissione al Parlamento europeo e al Consiglio (tra cui COM (2018), 24.1.2018, Maggiore protezione, nuove opportunità).

Il Titolare, in recepimento degli obblighi normativi richiesti in materia di gestione di una violazione di dati personali, nonché dei riferimenti interpretativi sopra citati, ha adottato una specifica procedura per la gestione del c.d. *data breach*, allegata al presente MOP.

7. I diritti degli interessati

Il Regolamento UE 679/2016 riconosce all'interessato alcuni diritti, come previsti dagli articoli 15 e ss. del Regolamento, che possono essere esercitati in qualunque momento. In caso di rapporti di contitolarità, l'interessato può esercitare i propri diritti nei confronti di e contro ciascun Titolare del trattamento (art. 26, par. 3 del GDPR).

Al fine di rendere consapevole l'interessato dei diritti riconosciutigli, il Titolare ha inserito nelle informative *ex* art. 13 del GDPR il dettaglio dei diritti e l'indicazione sintetica delle modalità con cui esercitarli.

- **Diritto di accesso** (art. 15)

L'interessato ha il diritto di chiedere la conferma che sia in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso alle informazioni riguardo il trattamento nonché copia dei dati. Il Titolare è tenuto a fornire gratuitamente la copia, in forma cartacea o elettronica, potendo addebitare il costo di eventuali ulteriori copie in capo all'interessato.

- **Diritto di rettifica** (art. 16)

Ogni interessato ha il diritto di ottenere la correzione di eventuali inesattezze, nonché l'integrazione di dati personali non completi, anche fornendo una dichiarazione integrativa.

L'inesattezza potrà in ogni caso essere inerente esclusivamente a dati di valore oggettivo. Di conseguenza, l'interessato potrà chiedere la rettifica esclusivamente di dati fattuali e non invece di valutazioni soggettive e personali.

- **Diritto di cancellazione - diritto all'oblio** (art.17)

Nel caso di espressa richiesta dell'interessato, il Titolare ha l'obbligo di cancellare i dati che lo riguardano da qualunque supporto su cui sono stati archiviati. Inoltre, se tali dati sono stati diffusi (es. pubblicazione su un sito web), il Titolare deve informare della richiesta di cancellazione gli altri Titolari che trattano i dati personali oggetto della richiesta di cancellazione, invitandoli a rimuovere ogni copia degli stessi.

In ogni caso, si precisa che la richiesta di cancellazione deve essere accolta solo al ricorrere di una delle ipotesi previste dal GDPR: a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'art. 6, par. 1, lettera a), o all'art. 9, par. 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento; c) l'interessato si oppone al trattamento ai sensi dell'art. 21, par. 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'art. 21, par. 2; d) i dati personali sono stati trattati illecitamente; e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento; f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'art. 8, par. 1.

- **Diritto di limitazione del trattamento** (art. 18)

L'interessato può chiedere al Titolare di limitare il trattamento dei propri dati solo con riferimento ad alcune specifiche finalità unicamente nelle quattro ipotesi elencate all'art. 18 GDPR, ovvero, a) in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), b) nel caso in cui l'interessato chieda la rettifica dei dati (in attesa di tale rettifica da parte del titolare) o c) si opponga al loro trattamento ai sensi dell'art. 21 del Regolamento (in attesa della

valutazione da parte del titolare), d) nelle ipotesi in cui i dati non siano più necessari al Titolare per il perseguimento delle proprie finalità ma divengano necessari per l'esercizio o la difesa di un diritto dell'interessato in sede giudiziaria.

- **Diritto alla portabilità dei dati** (art. 20)

Il diritto alla portabilità dei dati consente all'interessato a) di ricevere, su richiesta, i propri dati personali da parte del Titolare del trattamento e b) la loro trasmissione ad un nuovo Titolare.

La richiesta di portabilità può essere accolta solo al ricorrere di determinati presupposti: 1) sono portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato; 2) solo i dati che siano stati "forniti" dall'interessato al Titolare; 3) il trattamento è effettuato con mezzi automatizzati; 4) il diritto alla portabilità può essere soddisfatto solo se non lesivo di diritti e libertà altrui.

Si precisa che la portabilità non comporta la cancellazione automatica dei dati conservati nei sistemi del Titolare.

- **Diritto di opposizione** (art. 21)

L'interessato può opporsi, in modo permanente, del trattamento dei suoi dati personali che avviene ai sensi degli articoli 6, par. 1, lettere e) e f) del GDPR. La richiesta di opposizione sarà accolta esclusivamente al ricorrere delle ipotesi previste dall'art. 21 par. 1 GDPR. Quando accolta, la richiesta di opposizione obbliga il Titolare ad interrompere il trattamento in modo definitivo e permanente.

Infine, l'interessato ha il diritto di proporre reclamo al Garante della privacy ai sensi dell'art. 77 del GDPR.

A norma dell'art. 2-*undecies*, c. 1, lett. a) del Codice privacy, i diritti di cui agli articoli da 15 a 22 del Regolamento non possono essere esercitati con richiesta al Titolare del trattamento ovvero con reclamo ai sensi dell'art. 77 del Regolamento qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto agli interessi tutelati in base alle disposizioni in materia di riciclaggio.

Al *Data Protection Coordinator* è demandata, quindi, la valutazione, caso per caso, della ricorrenza dei presupposti per l'esercizio del diritto da parte dell'interessato.

Ai sensi dell'art. 12, par. 3 del GDPR, il Titolare fornisce riscontro all'interessato senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto delle complessità e del numero delle richieste. Il Titolare è tenuto, però, ad informare l'interessato di tale proroga e dei motivi del ritardo, entro un mese dal ricevimento della richiesta.

Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con messi elettronici, salvo diversa indicazione dell'interessato.

8. La valutazione dei rischi connessi al trattamento

Ai sensi dell'art. 35 del Regolamento, il Titolare del trattamento è tenuto ad effettuare una valutazione d'impatto privacy (di seguito "*Data Protection Impact Assessment*" o "DPIA") nel caso in cui il trattamento, consideratane la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Il *Data Protection Impact Assessment* deve essere svolto **prima** di procedere al trattamento. Tale valutazione consiste in una procedura finalizzata a descrivere il trattamento, valutarne necessità e proporzionalità, e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche connessi al trattamento dei dati personali, attraverso la valutazione di tali rischi e la definizione di misure idonee a gestirli.

Nella valutazione del rischio si deve tenere conto delle fonti di rischio, degli impatti sui diritti e le libertà degli interessati in caso di eventi negativi (accesso illegittimo, modifiche indesiderate e indisponibilità di dati), si identificano le minacce che potrebbero comportare tali eventi, si stimano la probabilità e gravità dell'evento ed infine si individuano le misure previste per gestire i rischi.

Coerentemente con l'approccio basato sul rischio previsto dal GDPR, lo svolgimento di un DPIA non è obbligatorio per ogni tipo di trattamento. Infatti, in ossequio al Considerando n. 75 del GDPR, il DPIA è obbligatorio solo nel caso in cui il trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Sulla base di queste istruzioni, la Società ha costruito un processo di valutazione e gestione del rischio privacy seguendo le indicazioni contenute nei Considerando del GDPR, nelle Linee Guida WP248 rev.1 adottate in materia dal Gruppo WP29 e nell'Allegato 1 al provvedimento n. 467 dell'11 ottobre 2018 del Garante privacy italiano.

Il Garante per la protezione dei dati individua dei trattamenti che, per loro stesse caratteristiche, presentano sempre un rischio elevato e che richiedono, dunque, lo svolgimento di una valutazione dei rischi, per il dettaglio di quali si rinvia procedura per la gestione dei rischi connessi ai trattamenti di dati personali, in cui si dà inoltre atto dei ruoli dei soggetti coinvolti, delle loro attribuzioni nonché delle tempistiche.

9. Il trasferimento di dati Extra-UE

Per trasferimento di dati personali deve intendersi ogni ipotesi in cui i dati personali siano accessibili in uno stato Extra UE, non solo mediante un vero e proprio trasferimento, ma anche tramite il semplice accesso da remoto.

A tal proposito, l'*European Data Protection Board* stabilisce, all'interno delle *recommendations* approvate il 10 novembre 2020, che **l'accesso di un soggetto da un Paese terzo a dati personali che sono collocati in Europa è altresì considerato trasferimento**.

Ai sensi del Capo V GDPR (art. 44 e ss.) i dati personali degli interessati possono essere trasferiti verso un Paese terzo o un'organizzazione internazionale dal Titolare del trattamento che sia stabilito nel territorio dell'Unione.

Tuttavia, tale trasferimento transfrontaliero può essere effettuato solo se sussiste almeno una delle seguenti condizioni:

1. presenza di una decisione di adeguatezza (art. 45 GDPR),
2. garanzie adeguate fornite dal Titolare con annessi diritti azionabili e mezzi di ricorso effettivi a vantaggio degli interessati (art. 46 GDPR),
3. norme vincolanti d'impresa (art. 47 GDPR),
4. specifiche situazioni sancite dall'art. 49 GDPR.

Nello specifico, laddove non vi sia una decisione di adeguatezza della Commissione Europea, prima di procedere con il trasferimento di dati personali in un Paese Terzo, mediante utilizzo di diverse condizioni di trasferimento, quali le Clausole Contrattuali Standard o le Norme Vincolanti d'Impresa, l'esportatore congiuntamente con l'importatore deve verificare che il Paese terzo assicuri un livello di protezione dei dati personali sostanzialmente equivalente a quello garantito dalla legislazione europea.

Le *recommendations* dell'EDPB, sopra citate, delineano un percorso valutativo che occorre seguire prima di procedere al trasferimento affinché possano valutarsi le garanzie sottese.
Le *recommendations* sono state, infatti, approvate allo scopo di fornire supporto agli esportatori ed importatori di dati personali dopo che la Corte di Giustizia dell'Unione Europea, nella sentenza Schrems II del 16 luglio 2020, ha invalidato il c.d. *Privacy Shield*, che legittimava il trasferimento di dati dall'Unione Europea verso gli Stati Uniti, affermando che l'esportatore e l'importatore di dati personali devono verificare che nell'ambito del trasferimento sia assicurato un livello di garanzia sostanzialmente equivalente a quello previsto dalla normativa europea.
Con le proprie *recommendations*, dunque, l'EDPB fornisce una *roadmap* per determinare le garanzie ed elenca, altresì, delle misure supplementari da adottarsi nei casi in cui, all'esito del procedimento valutativo, emerga che le garanzie assicurate dal Paese terzo non sono equivalenti a quelle dettate dalla disciplina del GDPR.

Successivamente alle *recommendations* del 2020 sopra citate sono state approvate dalla Commissione Europea le nuove Clausole Contrattuali Standard (Decisione di esecuzione della Commissione Europea 2021/915) che prevedono al proprio interno delle clausole in base alle quali, al fine di garantire la sicurezza nei trattamenti, sono previsti specifici obblighi in capo all'importatore e all'esportatore,

nonché precise indicazioni ed adempimenti in caso di richieste e/o accessi delle autorità pubbliche locali.

Per quanto sopra, nel caso in cui – nell'ambito dei trattamenti eseguiti da LTMIL – dovesse emergere la necessità di procedere con il trasferimento, questo sarebbe ammesso solo se anticipato dalla verifica che sussista una delle condizioni di cui al Capo V del GDPR o una delle deroghe di cui all'art. 49 del GDPR di seguito riepilogate:

1. l'interessato ha acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti per l'interessato;
2. il trasferimento è necessario all'esecuzione di un contratto stipulato tra il Titolare del trattamento e l'interessato ovvero all'esecuzione di misure precontrattuali su richiesta dell'interessato;
3. il trasferimento è necessario per la conclusione o l'esecuzione di un contratto stipulato tra il Titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato;
4. il trasferimento è necessario per importanti motivi di interesse pubblico;
5. il trasferimento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
6. il trasferimento è necessario per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
7. il trasferimento sia effettuato a partita da un registro che, a norma del diritto dell'Unione o degli Stati Membri, mira a fornire informazioni al pubblico e può essere consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati Membri.

Nei casi in cui il trasferimento di dati verso Paesi extra-UE avvenga nell'ambito del rapporto tra un *Data Processor* nominato *ex* art. 28 GDPR ed un suo fornitore, **il Titolare deve espressamente e previamente autorizzare il trasferimento.**

A tal fine, il *Data Processor* è tenuto a rivolgere al Titolare la richiesta di autorizzazione al trasferimento dei dati in Paesi Extra-UE fornendo la documentazione attestante la legittimità del trasferimento nel rispetto del Regolamento. La documentazione deve essere inviata, da chiunque la riceva, al *Data Protection Coordinator* che svolge le valutazioni di cui sopra. Il *Data Protection Coordinator*, se ritiene che le condizioni di cui al Capo V siano soddisfatte, procede con l'autorizzazione.

Si rammenta che il Titolare rilascia l'autorizzazione a suo insindacabile giudizio e comunque previa verifica del rispetto delle condizioni di cui al capo V del Regolamento.

LTMIL si è dotata di una procedura che disciplina i ruoli dei soggetti coinvolti e soprattutto lo strumento giuridico che legittima ciascun trasferimento da porre in essere adeguato al caso concreto. Le ipotesi di trasferimenti extra-UE posti in essere dal Titolare sono residuali. Tuttavia, l'adozione della procedura di cui trattasi rientra nell'applicazione del principio di *accountability*.

Ruolo principale è ricoperto dal *Data Protection Coordinator*, che, tra l'altro, compila per ciascun trasferimento il Report del *transfer impact assessment* (c.d. TIA) in cui dà evidenza della condizione legittimante il trasferimento e cura l'archiviazione della documentazione rilevante.

10.Controllo e sanzioni

10.1. Controllo sugli incaricati al trattamento

Un primo livello di controllo è in carico al *Data Protection Coordinator*, il quale dovrà verificare che le istruzioni fornite agli autorizzati con il presente Modello e con specifiche lettere di incarico siano effettivamente rispettate e applicate.

Un secondo livello di controllo è invece in carico al Titolare del Trattamento (tramite il proprio rappresentante legale), il quale, ha la facoltà di effettuare specifici assesment e verifiche a campione, finalizzate a monitorare la corretta applicazione del Modello, delle procedure e delle istruzioni fornite, nonché effettua verifiche su tutto il sistema privacy del Titolare.

Il terzo livello di controllo è, da ultimo, in capo alle funzioni di controllo del Gruppo.

10.2. Sanzioni Amministrative e risarcimento del danno

In caso di violazione della disciplina prevista dal Regolamento UE, ai sensi dell'articolo 83 GDPR e dell'art. 166 del D. Lgs. 196/2003, l'Autorità di controllo provvede ad infliggere sanzioni amministrative pecuniarie.

In particolare, in base alla tipologia di violazione le sanzioni possono ammontare fino a 10 milioni di euro, o fino al 2% del fatturato mondiale annuo della società se superiore, ovvero fino a 20 milioni di euro, o fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente se superiore.

Ancora, il Titolare del trattamento ovvero il Responsabile del trattamento devono, ai sensi dell'articolo 82 del GDPR, risarcire il danno all'interessato che abbia subito un danno materiale o immateriale causato dalla violazione e che ne faccia richiesta.
Inoltre, le Autorità di controllo possono limitare, sospendere ovvero anche bloccare un trattamento di dati.

10.3. Sanzioni penali

Il GDPR non prevede direttamente delle sanzioni penali in materia di protezione dei dati personali; tuttavia, nel Considerando 149 stabilisce che gli Stati membri dovrebbero poter stabilire disposizioni relative a sanzioni penali per violazioni del Regolamento.

Sono state inserite, pertanto, delle sanzioni penali nel Codice Privacy mediante il D. Lgs. n. 101 del 2018, di seguito riepilogate.

Norma incriminatrice	**Descrizione**	**Sanzione**
Art. 167 Trattamento illecito di dati	Sanziona chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, **arreca nocumento all'interessato**in violazione di specifiche disposizioni di legge. È punito chi al fine di trarre per sé o per altri profitto o di arrecare danno all'interessato procedendo al trasferimento dei dati personaliverso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti, arreca nocumento all'interessato	Reclusione da sei mesi aun anno e sei mesi Reclusione da uno a treanni

Art. 167 *bis* Comunicazionee diffusione illecita di dati personali oggetto di trattamento su larga scala	**Sanziona la comunicazione e diffusione**, al finedi trarre profitto per sé o altri ovvero al fine di arrecare danno, di un **archivio automatizzato** ouna parte sostanziale dello stesso contenente dati personali oggetto di trattamento su larga scala anche quando lo si fa senza consenso quando questo è richiesto per le operazioni di comunicazione e di diffusione.	Reclusione da uno a sei anni
Art. 167 *ter* Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala	Sanziona la condotta per cui, al fine di trarne profitto per sé o altri, ovvero di arrecare danno, si acquisiscano con **mezzi fraudolenti** un **archivio automatizzato** o una parte sostanziale dello stesso contenente dati personali oggetto di trattamento su larga scala	Reclusione da uno a quattro anni
Art. 168 Falsità nelle dichiarazioni al Garante einterruzione dell'esecuzione dei compitio dell'esercizio dei poteri del Garante	Sanziona chiunque, in un procedimento o nel corso di accertamenti dinanzi al Garante, dichiario attesti falsamente notizie o circostanze o produce atti o documenti falsi Sanziona altresì colui che **cagioni intenzionalmente un'interruzione** o turbi la regolarità di un procedimento dinanzi al Garanteo degli accertamenti da questi svolti.	Reclusione da sei mesi atre anni Reclusione fino a unanno
Art. 170 Inosservanza di provvedimenti del Garante	Sanziona l'inosservanza di provvedimenti del Garante	Reclusione da 3 mesi a 2 anni
Art. 171 Violazione delle disposizioni in materia di Controlli a distanza e indagini sulle opinioni dei lavoratori	Sanziona l'utilizzo da parte dei datori di lavoro degli impianti audiovisivi e degli altri strumenti dai quali derivi anche la possibilità di controllo adistanza dell'attività dei lavoratori (possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale epossono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali o, in mancanza di accordo,previa autorizzazione dell'Ispettorato). Sanziona altresì la violazione del divieto al datoredi lavoro, ai fini dell'assunzione e nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore.	Arresto da 15 giorni a un anno

10.4. Violazioni del Modello Organizzativo Privacy

Nel caso in cui i soggetti incaricati al trattamento violino, eludano o applichino parzialmente o non correttamente il MOP e i documenti allo stesso allegati, saranno sanzionati ai sensi della disciplina relativa ai contratti di lavoro, con particolare riferimento agli illeciti disciplinari, e la sanzione sarà modulata rispetto al livello di responsabilità ed autonomia del dipendente, all'intenzionalità del

comportamento e alla gravità del medesimo rispetto agli effetti a cui il Titolare può ragionevolmente ritenersi esposto.