



ARCS
Azienda Regionale
di Coordinamento
per la Salute

**TRASFERIMENTI DI DATI PERSONALI
FUORI DALLO SPAZIO ECONOMICO EUROPEO**

Versione n. 00
del 22/12/2023

TRASFERIMENTI DI DATI PERSONALI FUORI DALLO SPAZIO ECONOMICO EUROPEO

SOMMARIO

1.	INTRODUZIONE.....	3
1.1.	Premessa.....	3
1.2.	Scopo	3
1.3.	Riferimenti normativi e regolamentari interni ed esterni.....	3
1.4.	Definizioni	3
1.5.	Acronimi e abbreviazioni.....	4
2.	DESCRIZIONE DELLA POLICY.....	5
2.1.	Generalità	5
2.1.1.	Definizione di «trasferimento».....	5
2.1.2.	Condizioni di liceità per il trasferimento	5
2.1.3.	Decisioni di adeguatezza.....	5
2.1.4.	Clausole contrattuali	6
2.1.5.	Norme vincolanti di impresa.....	7
2.1.6.	Deroghe ex art. 49	8
2.1.7.	Misure supplementari.....	8
2.2.	Istruzioni operative.....	9
3.	RESPONSABILITÀ E VIOLAZIONI.....	11
3.1.	Responsabilità	11
3.2.	Violazioni.....	11

1. INTRODUZIONE

1.1. Premessa

La presente policy disciplina l'individuazione e la gestione dei trasferimenti di dati personali al di fuori dello Spazio Economico Europeo.

1.2. Scopo

La presente policy ha lo scopo di fornire indicazioni sui principi applicabili ai trasferimenti di dati personali fuori dallo Spazio Economico Europeo, nonché sulle condizioni di liceità per effettuare tale trasferimento, sia qualora ARCS operi in qualità di Titolare che di Responsabile del trattamento.

1.3. Riferimenti normativi e regolamentari interni ed esterni

- Regolamento aziendale in materia di trattamento dei dati personali;
- EDPB - Linee Guida sull'interazione tra l'applicazione territoriale del GDPR e le disposizioni relative al trasferimento dei dati in paesi extra UE;
- Decreto Legislativo 10 agosto 2018, n. 101 - Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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). (18G00129) (GU Serie Generale n.205 del 04-09-2018).

1.4. Definizioni

- «Adeguatezza»: nel caso di trasferimenti dei dati, un paese terzo assicuri effettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello di protezione delle libertà e dei diritti fondamentali sostanzialmente equivalente a quello garantito all'interno dell'Unione.
- «Comunicazione»: è definita dal comma 4 dall'art. 2-ter del D. Lgs. n. 196/2003 e s.m.i., come il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del Titolare nel territorio dell'Unione europea, dal Responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione.
- «Decisione di adeguatezza»: è la decisione della Commissione europea, assunta a valle di una valutazione dell'adeguatezza del livello di protezione dei dati, che un paese terzo, un territorio, uno o più settori all'interno di un territorio o un'organizzazione internazionale garantiscono un livello di protezione adeguato per il trattamento dei dati personali.
- «Diffusione»: è definita dal comma 4 dall'art. 2-ter del D. Lgs. n. 196/2003 e s.m.i., come il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
- «Esportatore di dati»: si intende il Titolare del trattamento o il Responsabile del trattamento all'interno del SEE che trasferisce dati personali a un Titolare del trattamento o a un Responsabile del trattamento in un paese terzo.
- «Importatore di dati»: si intende il Titolare del trattamento o il Responsabile del trattamento in un paese terzo che riceve o ottiene accesso ai dati personali trasferiti dal SEE.

- «Organizzazione internazionale»: ai sensi dell'art. 4.26) del GDPR, è un'organizzazione o un organismo di diritto internazionale pubblico ad essa subordinato o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.
- «Paese terzo»: è uno Stato non appartenente all'UE o allo Spazio Economico Europeo comprendente anche la Norvegia, l'Islanda e il Liechtenstein.
- «Trasferimento occasionale e non ripetitivo»: si configurano tali quei trattamenti che possono ripetersi ma solo in circostanze non ordinarie e ad intervalli di tempo arbitrari, ovvero che sono conseguenti al manifestarsi di condizioni casuali o ignote e pertanto non hanno sicuramente cadenza regolare.
- «Trasferimento»: è una modalità di trattamento e avviene se i dati del Titolare, soggetto alle disposizioni del GDPR, sono oggetto di un qualsiasi trattamento in un paese terzo o sono destinati ad esserlo dopo il trasferimento verso un Titolare, Responsabile o destinatario stabilito fuori dell'ambito di applicazione del GDPR.
- «Trattamento»: è definito dall'art. 4.2) del GDPR come 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.

1.5. Acronimi e abbreviazioni

Nel documento sono utilizzati i seguenti acronimi:

- DPIA: Data Protection Impact Assessment
- DPO: Data Protection Officer
- EDPB: European Data Protection Board
- GDPR: General Data Protection Regulation
- SEE: Spazio Economico Europeo
- SGI: Sistema di Gestione Integrato
- SGSI: Sistema di Gestione della Sicurezza delle Informazioni.

2. DESCRIZIONE DELLA POLICY

2.1. Generalità

Ai sensi dell'art. 44 del Regolamento europeo 2016/679, qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, può legittimamente avvenire soltanto se il Titolare del trattamento e il Responsabile del trattamento rispettano le condizioni previste al capo V del citato Regolamento.

2.1.1. Definizione di «trasferimento»

Si configura un trasferimento di dati personali ai sensi del Capo V del GDPR quando sussistono i seguenti tre criteri cumulativi:

- l'esportatore di dati (Titolare o Responsabile del trattamento) è soggetto al GDPR per il trattamento (anche se non stabilito all'interno dell'UE);
- l'esportatore di dati trasmette o rende disponibili i dati personali all'importatore di dati (altro Titolare, Contitolare o Responsabile del trattamento);
- l'importatore di dati si trova in un paese terzo o è un'organizzazione internazionale, indipendentemente dal fatto o meno che questo importatore è soggetto al GDPR ai sensi dell'art. 3.

Titolari e Responsabili del trattamento, che non sono stabiliti nell'UE, potrebbero essere soggetti al GDPR ai sensi dell'articolo 3, paragrafo 2, per un determinato trattamento e, pertanto, dovranno ottemperare al Capo V in caso di trasferimento di dati personali a un paese terzo o a un'organizzazione internazionale (a titolo esemplificativo la mera pubblicazione di dati personali su un sito internet non può considerarsi trasferimento ai sensi del Capo V).

2.1.2. Condizioni di liceità per il trasferimento

Ogniquale volta si configuri un trasferimento di dati personali fuori dal SEE è necessario verificare che il trasferimento sia legittimato da una condizione di liceità espressa nel Capo V del GDPR.

Nello specifico, si tratta di verificare la sussistenza/stipulazione di:

- decisione di adeguatezza (art. 45 GDPR);
- clausole contrattuali (art. 46 GDPR);
- norme vincolanti di impresa (art. 47 GDPR);
- altri strumenti previsti dall'art. 46 GDPR;
- deroghe in specifiche situazioni ai sensi dell'art. 49 GDPR.

2.1.3. Decisioni di adeguatezza

La Commissione europea può stabilire, valutati gli elementi indicati nell'art. 45, par. 2 del Regolamento UE 2016/679 e sulla base di un procedimento che prevede il parere del Comitato europeo per la protezione dei dati, che un Paese terzo o un'organizzazione internazionale garantiscano un livello di protezione adeguato e che pertanto è possibile trasferirvi dati personali.

Nel caso in cui sia stata adottata una decisione di adeguatezza, il trasferimento di dati verso lo Stato ritenuto «adeguato» può avvenire in modo automatico, senza necessità di autorizzazioni specifiche.

Ad oggi, sono state adottate Decisioni di adeguatezza nei confronti dei seguenti Stati¹:

- Andorra

¹ L'elenco aggiornato può essere rinvenuto sul sito web della Commissione Europea, al seguente link:
<https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions>.

- Argentina
- Baliato di Guernsey
- Canada
- EU-US Data Privacy Framework
- Giappone (Decisione di esecuzione 2019/419)
- Isola di Man
- Isole Faer Øer
- Israele
- Jersey
- Nuova Zelanda
- Regno Unito (Decisione di esecuzione 2021/1772)
- Repubblica di Corea (Decisione di esecuzione 2022/254)
- Repubblica orientale dell'Uruguay
- Svizzera

Per quanto riguarda i trasferimenti verso gli Stati Uniti, l'Ente dovrà verificare sul sito web del Data Privacy Framework² se il destinatario negli Stati Uniti è certificato e se il trasferimento dei dati pertinenti sia coperto da tale certificazione.

Nel caso in cui non sia presente una Decisione di adeguatezza, i trasferimenti di dati personali vengono limitati a quelli che sono legalmente vincolanti o essenziali per la fornitura dei servizi o nel migliore interesse dell'interessato.

In ogni caso, occorre verificare che il paese terzo o l'organizzazione internazionale abbia fornito garanzie adeguate e che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi.

Nello specifico, tali garanzie adeguate comprendono i seguenti strumenti.

2.1.4. Clausole contrattuali

Si tratta di testi contrattuali sottoscritti da ambo le parti, allegati ai contratti di servizio. Si distinguono in:

- clausole tipo adottate dalla Commissione europea (anche definite SCC – Standard Contractual Clauses), le più recenti sono state approvate dalla stessa Commissione il 4 giugno 2021. Si tratta di una combinazione di clausole generali con un approccio modulare per rispondere ai diversi scenari di trasferimento e alla complessità delle catene di trattamento. I 4 moduli comprendono:
 - da Titolare a Titolare;
 - da Titolare a Responsabile;
 - da Responsabile a Responsabile;
 - da Responsabile a Titolare.

Oltre alle clausole generali, i Titolari del trattamento e i Responsabili del trattamento dovrebbero scegliere il modulo applicabile alla loro situazione, in modo da adattare gli obblighi derivanti dalle clausole contrattuali tipo al loro ruolo e alle loro responsabilità in relazione al trattamento di dati in questione.

² Cfr. <https://www.dataprivacyframework.gov/s/>.

Le clausole contrattuali tipo adottate dalla Commissione europea non possono essere modificate, eccetto per:

- selezionare moduli e/o opzioni specifiche offerte nel testo;
 - completare il testo se fosse necessario (indicato tra parentesi quadre), ad esempio per indicare i tribunali competenti e l'autorità di controllo, e per specificare i periodi di tempo;
 - compilare gli allegati;
 - aggiungere ulteriori garanzie che aumentano il livello di protezione dei dati.
- clausole tipo adottate da un'Autorità di Controllo e approvate dalla Commissione europea: esse possono essere comunicate come "decisione di adozione" da parte del GDPR al Comitato europeo per la Protezione dei Dati (EDPB), secondo l'art. 64.1.d, e approvate dalla Commissione europea secondo atti d'esecuzione, al fine di garantire un'omogenea applicazione della normativa all'interno di ciascuno stato membro e dell'UE;
 - clausole contrattuali ad hoc tra le parti: questa condizione di garanzia esplicita un requisito precedentemente più vago e, nel caso in cui le clausole standard siano stipulate tra il Titolare o Responsabile (esportatore) e l'importatore (altro Titolare o Responsabile extra UE), impone che tali contratti, anche di natura privata, siano sottoposti all'autorità nazionale per autorizzazione.

2.1.5. Norme vincolanti di impresa

Si tratta di uno strumento volto a consentire il trasferimento di dati personali dal territorio dello Stato verso Paesi Terzi nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune.

Le norme vincolanti di impresa (BCR - Binding Corporate Rules) costituiscono un meccanismo in grado di semplificare gli oneri amministrativi a carico delle società di carattere multinazionale con riferimento ai flussi intra-gruppo di dati personali.

Sono costituite da un documento contenente una serie di clausole che fissano i principi vincolanti espressamente individuati all'art. 47, paragrafi 1 e 2 del Regolamento UE 2016/679, al cui rispetto sono tenute tutte le entità (che agiscono in qualità di controller o di processor) appartenenti ad uno stesso gruppo (corporate).

I modelli di riferimento disponibili sono di due tipologie e differiscono a seconda del ruolo ricoperto dalle entità – Titolari o Responsabili – che esportano ed importano i dati all'interno del gruppo:

- le BCR for Controller (trasferimento di dati tra un Titolare in Europa ed un Titolare in altro paese);
- le BCR for Processor (trasferimento di dati tra un Titolare in Europa ed un Responsabile del trattamento in altro paese).

Il gruppo richiedente deve compilare l'*application form* secondo quanto indicato nel documento WP 264, per le BCR for controller, e nel documento WP 265, in ordine alle BCR for processor, rivolgendosi all'Autorità di Controllo, individuata sulla base dei criteri indicati nel paragrafo 1 del WP 263.

Sul sito dell'EDPB è presente e consultabile un registro aggiornato dell'elenco delle BCR approvate dalle autorità nazionali degli Stati Membri³.

³ Si rinvia al seguente link https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en.

2.1.6. Deroghe ex art. 49

In mancanza di una delle precedenti condizioni di legittimità, è possibile trasferire i dati personali solo se si verifica una delle seguenti situazioni vincolanti, che sono da considerare residuali nel loro utilizzo rispetto quelle riportate in precedenza e che, per il loro utilizzo, richiedono la concomitante presenza di altri fattori. Le condizioni sono, in alternativa:

- che l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate;
- che il trasferimento sia necessario all'esecuzione di un contratto concluso tra l'interessato e il Titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato;
- che il trasferimento sia 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;
- che il trasferimento sia necessario per importanti motivi di interesse pubblico;
- che il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
- che il trasferimento sia 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;
- che il trasferimento sia effettuato a partire da un registro che, a norma del diritto dell'Unione europea o degli Stati membri, mira a fornire informazioni al pubblico e può esser 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 europea o degli Stati membri;
- se non è ripetitivo, se riguarda un numero limitato di interessati, se è necessario per il perseguimento degli interessi legittimi cogenti del Titolare del trattamento, su cui non prevalgano gli interessi o i diritti e le libertà dell'interessato. Il Titolare del trattamento deve aver valutato tutte le circostanze relative al trasferimento e sulla base di tale valutazione ha fornito garanzie adeguate relativamente alla protezione dei dati personali. Il Titolare del trattamento informa del trasferimento l'Autorità di Controllo. In aggiunta alla fornitura di informazioni di cui agli artt. 13 e 14 GDPR, il Titolare del trattamento informa l'interessato del trasferimento e degli interessi legittimi cogenti perseguiti.

2.1.7. Misure supplementari

Nel caso in cui vi siano elementi nella legge o nella prassi del paese terzo che possano incidere sull'efficacia delle garanzie adeguate degli strumenti di trasferimento (la valutazione deve concentrarsi principalmente sulla legislazione del paese terzo rilevante per il trasferimento e sullo strumento di trasferimento ai sensi dell'articolo 46 del RGPD e che potrebbe pregiudicarne il livello di protezione), occorre valutare l'introduzione di misure supplementari.

Sul punto, l'EDPB con le Raccomandazioni 01/2020 ha definito quali misure supplementari devono essere adottate nel caso in cui la valutazione rivela che la legislazione e/o le prassi del paese terzo incidono sull'efficacia dello strumento di trasferimento.

La ratio sottostante riguarda la necessità di impedire all'importatore e a terzi l'accesso ai dati personali oggetto di trasferimento. Ad esempio:

- pseudonimizzazione: l'esportatore trasferisce i dati personali in modo tale che non possano essere direttamente riconducibili all'interessato senza l'utilizzo di informazioni aggiuntive, che devono essere detenute dall'esportatore stesso e conservate separatamente.
- cifratura: l'esportatore trasferisce dati personali crittografati e le parti coinvolte nella comunicazione si accordano su un'autorità o un'infrastruttura di certificazione a chiave pubblica affidabile. È consigliabile, a seconda delle esigenze, eseguire due tipologie di cifratura:
 - cifratura in transito (cifratura del trasporto);
 - cifratura end-to-end sul livello dell'applicazione.

In ogni caso, l'algoritmo di cifratura e la sua parametrizzazione (ad esempio la lunghezza della chiave o la modalità di funzionamento, se applicabili) deve essere conforme allo stato dell'arte e le chiavi devono essere conservate esclusivamente sotto il controllo dell'esportatore di dati, o di un soggetto incaricato dall'esportatore nel SEE o in una giurisdizione che offre un livello di protezione sostanzialmente equivalente a quello garantito all'interno del SEE.

Per un'analisi approfondita delle possibili misure da implementare, si rinvia alle citate Raccomandazioni⁴.

2.2. Istruzioni operative

2.2.1. Modalità di formalizzazione

Nel caso in cui nell'ambito del rapporto contrattuale siano previsti trasferimenti di dati personali fuori dallo Spazio Economico Europeo, occorre finalizzare le attività istruttorie ai seguenti obiettivi:

- inserire/allegare allo schema di capitolato/contratto un modello con il quale viene richiesto al Fornitore di dare evidenza della presenza di trasferimenti di dati personali fuori dallo Spazio Economico Europeo;
- verificare la sussistenza di una condizione di legittimità per il trasferimento dei dati, come meglio specificato al punto 2.2:
 - decisione di adeguatezza ex art. 45;
 - garanzie adeguate: qualora non vi sia decisione di adeguatezza, il trasferimento può essere effettuato in presenza di garanzie adeguate e in forza di condizioni per le quali gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi. Esse sono costituite da (alternativamente):
 - uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici;
 - le norme vincolanti d'impresa (BCR) in conformità dell'art. 47 GDPR;
 - le clausole contrattuali tipo o standard di protezione dei dati, adottate dalla Commissione europea secondo la procedura d'esame di cui all'art. 93, par. 2 GDPR. A tal proposito, si precisa che esistono quattro modelli di clausole che devono essere scelte in base all'inquadramento privacy individuato:

⁴ Si rinvia al seguente link https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_it

- trasferimenti da Titolare a Titolare;
- trasferimenti da Titolare a Responsabile;
- trasferimenti da Responsabile a Responsabile;
- trasferimenti da Responsabile a Titolare;
- le clausole contrattuali tipo o standard di protezione dei dati, adottate da un'Autorità di Controllo e approvate dalla Commissione europea secondo la procedura d'esame di cui all'art. 93, par. 2 GDPR;
- un Codice di Condotta (CC) approvato a norma dell'art. 40 GDPR, unitamente all'impegno vincolante ed esecutivo da parte del Titolare del trattamento o del Responsabile del trattamento nel Paese Terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati;
- un Meccanismo di Certificazione (MC) approvato a norma dell'art. 42 GDPR, unitamente all'impegno vincolante ed esigibile da parte del Titolare del trattamento o del Responsabile del trattamento nel Paese Terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli Interessati;
- (con l'autorizzazione dell'Autorità di Controllo competente) le Clausole Contrattuali tra il Titolare del trattamento o il Responsabile del trattamento e il Titolare del trattamento, il Responsabile del trattamento o il destinatario dei dati personali nel Paese Terzo o nell'organizzazione internazionale;
- (con l'autorizzazione dell'Autorità di Controllo competente) le disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli Interessati.
- le autorizzazioni rilasciate da uno Stato membro o dal GDPR in base alla precedente direttiva 95/46/CE, che restano valide fino a quando non vengono modificate, sostituite o revocate dalla medesima autorità di controllo (art. 46.5);
- registrazione del trasferimento di dati personali all'interno del Registro dei trattamenti, ex art. 30 GDPR, riportando i paesi terzi od organizzazioni internazionali a cui i dati personali sono stati o saranno comunicati, la valutazione del rischio effettuata e la descrizione delle garanzie attuate per il trasferimento, in relazione ai rischi valutati (ciò affinché l'interessato benefici di un adeguato livello di protezione dei suoi dati personali sia nel trasferimento dei dati verso un paese terzo sia nell'eventuale ulteriore trasferimento da questi ad altro paese terzo, secondo le disposizioni del Capo V del GDPR);
- inserimento nell'informativa per l'interessato, riportando quali siano i paesi terzi o organizzazioni internazionali destinatarie e le motivazioni per cui ha luogo il trasferimento. Devono essere inoltre riportate le valutazioni del Titolare in merito alla scelta dello strumento di garanzia adottato, tra quelli previsti dal GDPR, in caso di assenza di una decisione di adeguatezza.

La valutazione dell'adeguatezza della tutela offerta da un paese terzo va considerata in funzione di tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti, che riguardano anche la modalità, la frequenza, la durata e il contesto del trasferimento.

Sia nella valutazione del rischio sia nelle garanzie attuabili, l'Ente presta attenzione anche ai trasferimenti che potrebbero subentrare tra l'importatore dei dati e un successivo sub-incaricato, in virtù di un subcontratto dell'importatore.

3. RESPONSABILITÀ E VIOLAZIONI

3.1. Responsabilità

La presente policy potrà essere riesaminata in tutte le situazioni per le quali si realizzi una modifica relativa all'attività istituzionale che può avere impatto sui dati personali e sul relativo trattamento degli stessi ovvero anche a seguito di revisione dei livelli di rischio associati ai trattamenti.

I responsabili dell'attuazione della presente policy sono:

- Direzione strategica
- Affari Generali
- Tecnologie informatiche
- DPO
- tutto il personale dipendente ARCS, il quale ha il compito di rispettare la presente policy e avere una pronta risposta in termini di attuazione, segnalare eventuali difformità e suggerire potenziali miglioramenti finalizzati a garantire l'applicazione dei principi sanciti dal GDPR e dalla normativa privacy e sicurezza applicabile.

3.2. Violazioni

Ogni azione non conforme alla presente policy aziendale può generare violazioni del Regolamento UE n. 2016/679, pertanto i casi più gravi dovranno essere segnalati all'Autorità competente e potranno essere soggetti ad azioni disciplinari o legali.