TO ISTITUTO NUTRIZIONALE CARAPELLI

DATE

signature

NOTE

Rif. **Olive Oil & Sustainability: a future forward**

Istituto Nutrizionale Carapelli Scholarship

ISTRUZIONE INCARICATI AL TRATTAMENTO [ITD] NON DIPENDENTI
(art. 29 Reg. UE 016/679)

Le nostre procedure volte al rispetto della normativa in tema di tutela dei dati personali (D. Lgs. 196/2003 e Reg. UE 2016/679) prevedono una gestione capillare e particolarmente attenta di tutti gli aspetti connessi alla piena garanzia della privacy. In quest'ottica, Le viene consegnato il presente documento allo scopo di amministrare nel dettaglio la materia in esame e metterLa in condizioni di effettuare correttamente i trattamenti di dati personali svolti per conto della Società.

Ciò premesso, le attività svolte in relazione al contratto in riferimento comportano necessariamente delle operazioni di trattamento di dati personali per le quali si rende necessario fornire particolari istruzioni e concedere le autorizzazioni necessarie ricordando le conseguenti responsabilità. L'Art. 29 del reg. UE 2016/679 prevede, infatti, che chiunque tratti dati personali su autorizzazione o sotto l'autorità del Titolare o del Responsabile debba elaborare i dati personali ai quali ha accesso attenendosi alle istruzioni e norme da questi indicate.

La validità delle autorizzazioni contenute sul presente documento sono subordinate al mantenimento degli incarichi che le hanno rese necessarie.

1. Il Collaboratore potrà effettuare tutti i trattamenti di dati personali necessari all'erogazione della prestazione professionale a Lui richiesta dalla Società o a garantire la sicurezza dei dati secondo le norme di comportamento di seguito specificate.
Resta inteso che ogni operazione consistente in:
- ⇨ comunicazione dei dati a soggetti diversi dall'interessato o dal personale della Società
- ⇨ diffusione di dati
- ⇨ cancellazione o distruzione

dovrà essere autorizzata dal Responsabile di riferimento.

2. Salvo diversi accordi il collaboratore è autorizzato ad effettuare i trattamenti sopra riportati esclusivamente mediante i sistemi hardware e software approvati o eventualmente messi a disposizione dalla Società.

3. In riferimento a specifici obblighi imposti dalla normativa, il Collaboratore è tenuto ad attenersi alle seguenti norme:
- ⇨ Elaborerà i dati personali ai quali ha accesso attenendosi alle norme aziendali ed alle istruzioni particolari eventualmente impartite, anche per tramite di propri incaricati, dal Suo Responsabile di riferimento.
- ⇨ Effettuerà il trattamento in modo che i dati siano sempre:
  a) trattati in modo lecito e secondo correttezza;
  b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni in termini non incompatibili con tali scopi;
  c) esatti e aggiornati;
  d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti e trattati.

  In ogni caso potrà effettuare solo i trattamenti:
  - ↳ imposti da norme di legge o regolamenti e direttive comunitarie,
  - ↳ necessari all'espletamento degli obblighi contrattuali assunti nei confronti della Società.
- ⇨ <u>Se contemplato dal contratto e secondo le istruzioni ricevute dal proprio Responsabile di Società di riferimento</u>:
  - ↳ al momento della raccolta dei dati, provvedere a consegnare all'interessato il modello "Informativa ex artt. 13-14 Reg. UE 2016/679" fornito dal Titolare richiedendo, se previsto, il consenso; l'informativa è strutturata sulla base dei trattamenti approvati ed effettuati dalla Società, ne consegue che qualsiasi trattamento non necessario all'espletamento dell'incarico ricevuto o estraneo a quanto previsto dal contratto in riferimento comporterebbe una grave violazione della normativa in parola, come peraltro la mancata applicazione di quanto previsto dal presente documento.

- rispondere direttamente alle richieste dell' interessato, quando esse riguardino i dati e trattamenti da Lui effettuati. In tale ipotesi eventuali risposte a richieste potranno essere date solamente dopo aver verificato con certezza l'identità della persona richiedente.

⇨ Trasmetterà tempestivamente al proprio Responsabile di riferimento in Società eventuali richieste o lamentele dell'interessato, unitamente a tutti gli elementi ritenuti necessari per la corretta valutazione della circostanza.

⇨ Consentirà la visione dei dati solamente ai soggetti che ne abbiano effettiva necessità, tenendo presente che:
- deve controllare che il richiedente sia compreso tra le persone autorizzate, in funzione delle finalità che giustificano il trattamento, a conoscere i dati cui richiede l'accesso;
- l'accesso ai dati "particolari" da parte di altri soggetti diversi:
  - dall'interessato
  - dagli altri incaricati della Società,

  deve essere specificatamente autorizzata dal proprio Responsabile di riferimento in Società o da soggetti da questi specificatamente delegati, ed i documenti devono essere consultati esclusivamente nei locali in cui vengono abitualmente custoditi.

⇨ Consentirà l'accesso alle aree in cui vengono trattati dati "particolari" solamente alle persone autorizzate.

4. Nell'utilizzo degli strumenti elettronici eventualmente messi a disposizione del collaboratore dalla Società, mai in uso esclusivo, è obbligatorio rispettare le seguenti norme:

⇨ l'accesso ai dati è permesso utilizzando l'apposito codice identificativo personale (nome utente o user-id) a Lei eventualmente assegnato, associato ad una parola chiave (password). Gli incaricati non devono tenere traccia scritta identificabile delle password; la password di lavoro:
- è strettamente personale. Non è cedibile a terzi per nessun motivo;
- non deve contenere riferimenti agevolmente riconducibili all'incaricato e deve essere di adeguata complessità, anche ricorrendo nella sua formulazione a caratteri speciali, numeri, punteggiatura o aumentandone a discrezione la lunghezza;
- la sua lunghezza non può essere inferiore agli 8 caratteri;
- deve essere autonomamente modificata al primo utilizzo e, in seguito, almeno ogni 90 giorni o al minimo sospetto di compromissione della sua riservatezza.

Indipendentemente dall'impostazione dei sistemi, ciascun incaricato è personalmente responsabile della corretta gestione delle proprie credenziali per l'autenticazione, di cui sarà chiamato a rispondere

⇨ Ogni qual volta gli incaricati devono abbandonare il proprio ufficio o posto di lavoro, anche per breve tempo, devono aver cura di:
- verificare che persone non autorizzate non possano accedere ai dati personali, eventualmente uscendo dall'ambiente/sessione di lavoro in modo che sia necessaria la password per iniziare nuovamente le operazioni;
- non lasciare supporti per la memorizzazione dei dati o documenti incustoditi.

⇨ Qualora fosse dato in uso al collaboratore un apparato portatile vige l'obbligo:
- di effettuare un salvataggio dei dati almeno settimanale sull'area di rete indicata dal Responsabile di riferimento,
- di aggiornare il software antivirus con I sistemi indicati dal Responsabile Information Technology (RIT) della Società almeno una volta al mese,

⇨ **Gestione e conservazione dei supporti per la memorizzazione dei dati**. Non è consentito l'utilizzo di supporti esterni da parte del Collaboratore senza l'espressa autorizzazione del suo responsabile di riferimento in Società. In caso di autorizzazione i supporti, magnetici e non, contenenti dati personali:
- vanno custoditi con le stesse modalità valide per i documenti cartacei,
- non possono essere reimpiegati per altri scopi,
- in caso di malfunzionamenti, devono essere fisicamente distrutti.

⇨ **Non è consentito:**
- l'utilizzo sui sistemi aziendali di supporti esterni per l'archiviazione dei dati senza l'esplicita autorizzazione del proprio Responsabile di riferimento nella Società;
- eseguire qualunque attività installativa o manutentiva sui sistemi elaborazione dati, periferiche comprese, senza autorizzazione del Responsabile Information Technology (RIT) della Società;
- l'utilizzo di sistemi di interconnessione diversi da quelli autorizzati ed installati dal Responsabile delle risorse informatiche;
- l'impianto di qualsiasi opera, software, sistema o servizio accessorio agli apparati e relative periferiche, senza l'autorizzazione scritta del Responsabile Information Technology (RIT) della Società;
- limitare in alcun modo l'accesso da parte del Responsabile Information Technology (RIT) della Società o di suoi incaricati alle postazioni di lavoro;
- creare nuove banche dati senza l'autorizzazione del proprio Responsabile di riferimento nella Società.
- attivare la funzione "ricordami" o "ricorda password" su qualsiasi applicazione o piattaforma

⇨ **E' fatto obbligo di:**

- impostare lo screen saver (o sospensione della sessione in caso di inattività) in modo tale che alla ripresa delle attività riporti alla schermata di accesso e con un tempo di attesa ridottissimo in considerazione della estrema velocità con cui possono essere ricercati e/o letti su schermo dati personali ed informazioni meritevoli di tutela. In alternativa prestare massima attenzione a bloccare il computer ogni qual volta ci si allontani dallo stesso;
- denunciare o comunicare immediatamente al proprio Responsabile di riferimento eventuali smarrimenti compromissioni o alterazioni indebite su dati personali;
- salvare nelle aree e sistemi in rete indicate dal Responsabile Information Technology (RIT) della Società i file importanti, confidenziali o contenenti dati personali.

⇨ Nel caso fosse data in uso al Collaboratore una casella di posta elettronica di proprietà della Società:

- Essa potrà essere utilizzata esclusivamente nell'ambito dell'incarico ricevuto dalla Società, con esclusione assoluta di qualsiasi utilizzo per scopi personali, in considerazione del fatto che la Società potrà accedere alla casella in qualsiasi momento ove ciò fosse necessario in relazione ad esigenze di lavoro o di manutenzione della rete e dei sistemi informatici.
- Comunicazioni (inviate o ricevute) non più necessarie o pertinenti alle attività aziendali devono essere cancellate, con particolare attenzione a quelle contenenti dati personali in modo da evitare una loro conservazione o trattamento eccedenti.
- Per prevenire utilizzi non corretti delle caselle di posta elettronica a piè di pagina di ogni comunicazione inviata verso l'esterno sarà riportato un avviso che, ovviamente, non è consentito cancellare.
- Dovranno essere evitate e-mail oltraggiose e offensive.
- In quanto strumento di lavoro, la casella di posta elettronica è utilizzata dalla Società per inviare/trattare informazioni anche confidenziali destinate solo a ristretti gruppi di incaricati, è pertanto proibito abilitare altro personale o terze persone all'apertura della propria casella di posta elettronica senza autorizzazione del proprio Responsabile di riferimento.
- Pur non essendo previste ipotesi di utilizzo della casella postale a fini personali, non è possibile escludere a priori una sia pur improbabile ed incidentale presenza di informazioni non attinenti all'attività lavorativa contenute in comunicazioni ricevute, che devono essere immediatamente cancellate. In riferimento a tali informazioni si fa comunque presente che il sistema (server e pc locale) per default ne tiene traccia ed effettua una copia di backup, accessibile per questioni tecniche dal system manager, che ha istruzione di cancellare, previo avviso all'interessato, tutti i dati non attinenti alle attività ogni qual volta li rilevi, salvo che non costituiscano prova di illeciti che devono essere obbligatoriamente segnalati alle Autorità competenti.

⇨ **Servizio Internet:**

Il servizio Internet è disponibile esclusivamente per attività attinenti alle prestazioni professionali da Lei svolte.

Anche in questo caso è importante far presente che i sistemi tengono traccia dei siti visitati e delle operazioni effettuate su internet associate a ciascun profilo utente. Tale traccia è accessibile per questioni tecniche al system manager, che ha istruzione:

- di segnalare tutti gli elementi che creano danno alla Società o pregiudizio per la sicurezza dei sistemi e, conseguentemente, per i dati su di essi gestiti,
- di cancellare tutti i dati non attinenti alle attività lavorative ogni qual volta li rilevi.

qualora il collaboratore avesse necessità di accedere ad internet per scopi diversi potrà richiedere un accesso alla rete wi-fi guest.

⇨ **Trasmissione dei dati**:

- è categoricamente proibito l'utilizzo di sistemi di interconnessione diversi da quelli autorizzati ed installati dal Responsabile delle risorse informatiche.

⇨ **Utilizzo dei telefoni, fax e fotocopiatrici aziendali:**

- Il telefono messo a disposizione è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per attività attinenti alle prestazioni professionali svolte.
- non è consentito l'utilizzo dei fax aziendali per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte del proprio Responsabile di riferimento della Società.
- non è consentito l'utilizzo delle fotocopiatrici aziendali per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di riferimento della Società.

⇨ **UTILIZZO DI DEVICES (NOTEBOOK, TABLET):**

- **I Devices eventualmente affidati all'utente sono strumenti di lavoro**. Ne viene consentito l'uso esclusivamente per attività attività svolte dal collaboratore, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti all'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentito solo nel caso di comprovata necessità ed urgenza.
- Si ricorda che molti devices offrono funzionalità simili a quelle di un pc portatile (memorizzazione dati, ricezione mail, etc.) spesso aggiunte alla possibilità di archiviazione ed invio di immagini e suoni (sia foto che filmati). A tal proposito si fa presente:

- l'obbligo di impostare il device in modo che sia necessario il PIN per accedere alla memoria interna ed alla possibilità di effettuare telefonate; ovviamente il PIN dovrà essere gestito con le stesse norme precedentemente descritte per le password. Nell'utilizzo di sistemi più evoluti, quali smartphone e tablet, valgono tutti gli obblighi previsti per i PC portatili;
- il divieto di utilizzare in modo improprio i sistemi di registrazione video e audio offerti dall'apparato;
- il divieto di memorizzare in via permanente sul device messaggi ricevuti di natura personale, prestando particolare attenzione a procedere alla loro cancellazione in caso di restituzione dell'apparato e tenendo presente che, in caso di avaria, tale operazione potrebbe non essere effettuabile e che l'Azienda potrebbe richiedere in qualsiasi momento la restituzione del device, anche con brevissimo o senza preavviso senza dover fornire motivazioni circa tale decisione.

↳ **I devices non devono <u>mai</u> essere lasciati incustoditi**, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni, sia all'esterno che all'interno della sede aziendale e durante gli spostamenti, tenendo presente che gli strumenti assegnati possono essere utilizzati per il trattamento di dati personali ed informazioni costituenti know-how aziendale, protetti dalla normativa vigente.

Inoltre, si ricorda che, salvo diverse esigenze/istruzioni, si dovrà prestare attenzione all' attivazione/disattivazione del sistema di geo-localizzazione presente su smartphone e tablet, che potrebbe incidentalmente portare l'Azienda a conoscenza di informazioni relative alla posizione del device e, conseguentemente, del suo assegnatario.

Qualora l'incaricato fosse autorizzato ad impiegare strumenti elettronici propri, egli dovrà adottare, per quanto applicabili, le norme suesposte e garantirà la piena rispondenza di tali sistemi alle misure di sicurezza imposte dalla normativa in vigore con particolare riguardo alla cancellazione sicura e non recuperabilità dei dati dai supporti per la memorizzazione.

5. Premesso che tutte le informazioni relative alle procedure interne, alle misure di sicurezza adottate, alle caratteristiche tecnico-funzionali delle attrezzature utilizzate per effettuare i trattamenti sono sottoposte alle stesse cautele valide per i dati "particolari", **nell'espletamento dei suoi incarichi il collaboratore dovrà attenersi alle seguenti norme** di comportamento imposte dalla Legge:

⇨ operare nell'assoluto rispetto della riservatezza di qualsiasi dato o informazione ovvero quant'altro venga a conoscenza per effetto delle attività svolte nell'ambito delle proprie competenze attenendosi alle misure di sicurezza, norme di comportamento e regolamenti interni predisposti e periodicamente aggiornati, che Le verranno comunicati, evitando di:
  ↳ parlarne al di fuori degli uffici destinati alla loro trattazione o in presenza di persone non autorizzate a conoscere i dati oggetto della conversazione,
  ↳ farne oggetto di conversazione con chiunque non sia autorizzato.

⇨ **Comportamento al telefono – Comunicazioni Verbali:** dati personali comuni e "particolari" non possono essere trattati telefonicamente tranne che nei seguenti casi:
  ↳ l'interlocutore è una persona autorizzata ad accedere ai dati richiesti e non vi sono dubbi circa la sua identità (Es.: deve essere conosciuto personalmente dall'incaricato),
  ↳ in particolare, nella gestione dei servizi che comportano il trattamento via telefono di dati personali relativi a soggetti (sia persone fisiche che persone giuridiche) che hanno rapporti con la Società, l'interlocutore telefonico dovrà essere identificato con la richiesta di dati che lo riguardano già presenti nelle banche dati della Società che solo l'interessato può avere prontamente disponibili.
  ↳ la comunicazione è necessaria per salvaguardare l'incolumità fisica dell'interessato o di terzi.

  Ovviamente durante la conversazione non devono essere presenti persone non autorizzate a conoscere i dati eventualmente comunicati.

Nel caso sia necessario trattare verbalmente dati personali in situazioni di promiscuità con terzi estranei al trattamento stesso, dovranno essere adottate cautele atte ad evitare l'indebito ascolto della conversazione, ad esempio usando toni di voce adeguati o evitando di ripetere a voce alta dati identificativi degli interessati.

Relativamente alle attività di controllo e gestione tecnica si fa presente che, partendo dal presupposto che, per effetto delle norme ricordate sul presente documento, i dati trattati per mezzo degli strumenti assegnati dalla Carapelli Firenze Spa e le informazioni inerenti il loro utilizzo, ivi compresi i dati di traffico telefonico e telematico (registri chiamate, e log di navigazione), costituiscono dati aziendali e potranno essere utilizzati per finalità amministrative e per esigenze connesse alla sicurezza, alla gestione tecnica dei sistemi informatici, alla gestione di incidenti di sicurezza, alla tutela di un diritto anche in sede giudiziaria.
Così come per gli altri strumenti elettronici dati in uso all'incaricato, l'Azienda potrà effettuare dei controlli sul loro corretto utilizzo e sul rispetto delle norme aziendali richiamate anche sul presente documento. I controlli verranno effettuati nel pieno rispetto della normativa applicabile.

⇨ **Documenti cartacei contenenti dati personali:**

- Devono essere opportunamente custoditi in modo tale da impedirne la visione da parte di persone non autorizzate.
- Quando contengono dati "particolari", non devono essere assolutamente riprodotti (anche solo in parte), se non previa autorizzazione del Suo Responsabile di riferimento.
- Possono essere consultati solamente dal personale che, per ragioni inerenti il proprio incarico, ne ha effettiva necessità.
- Non possono essere dati in consegna ad alcuno se non previa autorizzazione del Responsabile.
- Non possono mai essere lasciati incustoditi e devono essere sempre riposti prima di lasciare l'area di lavoro in modo da impedirne la visione da parte di persone non autorizzate.
- Inoltre, al termine della giornata lavorativa, tutte le minute, veline, residui di carta in genere, usati per trattare i dati riconducibili a persona identificabile, non possono essere normalmente gettati tra i rifiuti ma devono essere distrutti.

Principali Definizioni	
DATO PERSONALE	La normativa definisce dato personale "*qualunque informazione relativa a persona fisica identificata o identificabile;* 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".
I DATI PERSONALI "PARTICOLARI"	**NECESSITANO DI MAGGIORE TUTELA E PARTICOLARE ATTENZIONE** Dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art. 9 del Reg. UE 2016/679) ***dati genetici****: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;* ***dati biometrici****: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;* ***dati relativi alla salute:*** *i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;*
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
INTERESSATO	La persona fisica cui si riferiscono i dati personali.
TITOLARE	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
INCARICATI	Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

RESPONSABILITÀ E SANZIONI

La normativa prevede pesanti **sanzioni** sia **amministrative** sia **penali**, a cui si aggiunge l'**obbligo di risarcimento** degli eventuali danni patiti dall'interessato a causa del trattamento stesso. Più in Particolare il Reg. UE 2016/679 prevede sanzioni che possono arrivare sino a € 20.000.000 (ovviamente tenendo conto della gravita della violazione, delle sue conseguenze e dello stato economico della persona che si è ressa responsabile della violazione) per comportamenti quali, ad esempio:

> non applicare le misure di sicurezza previste o utilizzare per i trattamenti sistemi non autorizzati,
> trattare dati senza consenso, ove previsto, o altro presupposto di legittimità previsto dagli artt. 6 e 9 Reg UE. 2016/679,
> comunicare o rendere disponibili i dati a soggetti non autorizzati o non contemplati nelle informative (violazione dell'obbligo di riservatezza),
> effettuare altri trattamenti non consentiti, quali copie non autorizzate, esportazione.

Il D. Lgs. 196/2003, come modificato dal D. Lgs. 101/2018, aggiunge alle sanzioni amministrative anche pesanti sanzioni penali (artt. 167 - 167 bis - 167 ter - 168 - 170) nei casi ritenuti di maggiore gravità in quanto:

- commessi con dolo e con danno per l'interessato,
- riguardanti dati particolari o giudiziari,
- riguardanti trattamenti su larga scala.

Ad esempio:

- *comunicare o diffondere,* in violazione della normativa, *al fine trarne profitto per se' o altri ovvero di arrecare danno un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala* costituisce condotta punibile *con la* ***reclusione da uno a sei anni****;* parimenti
- *chiunque, al fine trarne profitto per se' o altri ovvero di arrecare danno, acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala è punito con la* ***reclusione da uno a quattro anni****.*

- chiunque proceda al trattamento di dati "particolari" o giudiziari (con particolare riferimento ai genetici, biometrici e relativi alla salute) senza adottare i principi e le misure di garanzia previste dalla normativa, *con l'intento di trarre per se' o per altri profitto ovvero di arrecare danno all'interessato* provocando effettivamente un danno all'interessato (anche lieve) è punito con la **reclusione da uno a tre anni;** la stessa pena si applica a chiunque "esporta" i dati verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti dalla normativa.

Le responsabilità sopra descritte ricadono in prima istanza sul Titolare del trattamento, sul Responsabile nell'ambito della delega ricevuta dal Titolare, sugli incaricati al trattamento che non si attengono alle istruzioni, ai mansionari, alle procedure aziendali ricevute dal proprio Responsabile di riferimento e/o nell'ambito delle attività di formazione.