ACCORDO PER IL TRATTAMENTO DEI DATI PERSONALI

ai sensi dell'art.28 Regolamento Generale sulla Protezione dei dati n. 2016/679
(RGPD)

TRA

l'Azienda Ospedaliera Universitaria San Luigi, **AOU San Luigi Gonzaga di Orbassano**, con sede legale in Orbassano, Regione Gonzole 10, C.F. 95501020010 e P. IVA 02698540016 rappresentata legalmente dal _____ in qualità di Direttore Generale, di seguito **TITOLARE**

E

il fornitore _____ *(denominazione della persona giuridica o fisica nel caso di Professionista)*, codice fiscale _____, con sede legale in _____, in persona del legale rappresentante/procuratore_____ *(in caso di persone* giuridiche*),* nato a _____ il _____, di seguito **RESPONSABILE**

Premesso che:

- con deliberazione/determinazione n. _____ del _____ l'A.O.U. San Luigi Gonzaga di Orbassano ha affidato alla Ditta/Società/Professionista _____la fornitura/servizio del servizi di _____
(oggetto servizi/fornitura)
_____
- l'espletamento di tale fornitura/servizio comporta il trattamento di dati personali da parte del Fornitore per conto dell'Azienda, come esplicitato nell'allegato PLA, oltre che nella documentazione di aggiudicazione;
- il fornitore, tramite i criteri previsti nella procedura di selezione, nonché degli ulteriori elementi sottoelencati, ha dimostrato la sua capacità di fornire garanzie sufficienti del rispetto dei requisiti contemplati dalla normativa vigente ed in ed in particolare delle misure di sicurezza:

    - certificazioni: ISO 27001- sicurezza informazioni, ISO 27000 - IT, ISO 9001 – qualità ecc.
    - poter dimostrare che esiste ed è applicata "una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento";
    - nomina DPO;
    - poter dimostrare che "chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal Responsabile del trattamento e non abbia ricevuto idonea formazione";
    - poter dimostrare che esiste una procedura per la gestione degli incidenti di sicurezza c.d. "data breach";
    - aver sottoscritto polizze assicurative che tengano conto dei risarcimenti danni di cui all'art. 82 del RGPD con massimali adeguati;
    - aver effettuato una DPIA sul prodotto/servizio;
    - utilizzare tecniche di cifratura e pseudonimizzazione;
    - rilevare e detenere a norma di legge copia dei log di accesso all'applicativo e di sistema.

- con il presente atto l'A.O.U. San Luigi Gonzaga di Orbassano, in qualità di Titolare del trattamento, intende nominare il fornitore, che accetta, quale Responsabile del trattamento dei dati personali ai sensi dell'art. 28 del regolamento UE 20216/679 (di seguito "GDPR");

Tutto ciò premesso e formante, unitamente all'allegato PLA, parte integrante e sostanziale del presente Accordo, si conviene e si stipula quanto segue:

1) Oggetto dell'Accordo

Il presente accordo definisce le modalità con le quali il Responsabile si impegna ad effettuare per conto del Titolare le operazioni di trattamento dei dati personali.
.
In particolare, con la sottoscrizione del presente accordo, il Responsabile del trattamento, sulla base dei suoi requisiti di esperienza, capacità e affidabilità, caratteristiche necessarie per lo svolgimento del presente incarico, si impegna a procedere al trattamento dei dati personali, attenendosi alle istruzioni di seguito impartite nel pieno rispetto di quanto imposto dall'art. 28 del RGPD.

Il presente accordo integra il contratto principale (di seguito "Contratto"), di cui in premessa, e per tale motivo non sarà riconosciuto alcun corrispettivo aggiuntivo rispetto alle condizioni contrattuali predefinite per la fornitura/'incarico o per le operazioni conseguenti agli obblighi qui di seguito indicati.

2) Obblighi del Responsabile

2.1. **Principi Generali** Il Responsabile garantisce di trattare i dati esclusivamente al fine di svolgere i Servizi regolati dal Contratto, in base alle specifiche istruzioni, anche di quelle eventualmente successive, fornite dal Titolare per il tramite del Direttore dell'Esecuzione (di seguito "DEC).

Il Responsabile **deve informare immediatamente,** tramite Posta Elettronica Certificata , il DEC e il Responsabile Unico del Procedimento (di seguito "RUP"), se non coincidente con il primo, qualora ritenga che un'istruzione impartita configuri una violazione del Regolamento sulla protezione dei dati o di tutte le altre disposizioni delle leggi dell'Unione o delle leggi degli Stati membri relative alla protezione dei dati,
In tal caso, considerato che l'oggetto del contratto è finalizzato all'erogazione di servizi pubblici (essenziali), il Responsabile deve procedere con quanto previsto dal Contratto stesso, mettendo in atto le cautele che a suo giudizio salvaguardino i diritti e le libertà fondamentali delle persone fisiche, senza causare maggiore lesione ai diritti stessi, dandone immediata comunicazione al Titolare tramite i soggetti sopra indicati, che, se ritiene, potrà fornire indicazioni diverse.

Il Responsabile s'impegna altresì a mettere in atto le misure di sicurezza specificate nella documentazione di fornitura e/o riportate nell'allegato PLA.
Qualora venissero meno una o più delle misure di sicurezza previste, spetta al Responsabile senza ritardo e a sua cura e spese, dopo aver informato il DEC, provvedere al ripristino delle stesse anche in modalità alternative.

2.2. **Organizzazione interna** .Il Responsabile garantisce che la sua organizzazione interna è stata progettata per rispettare i requisiti specifici di protezione dei dati e di aver adottato le misure tecniche ed organizzative segnatamente richieste dall'art. 28, comma 3, lett. c), e dall' art.32 del RGPD per proteggere adeguatamente i dati del Titolare, nonché per assicurare la confidenzialità, l' integrità e la disponibilità dei dati.

2.3.**Soggetti autorizzati**- Il Responsabile garantisce di nominare per iscritto "le persone autorizzate al trattamento" e che le stesse abbiamo ricevuto specifiche e dettagliate istruzioni dirette ad assicurare il pieno rispetto delle disposizioni di legge, ai sensi dell'art. 29 del GDPR..

In particolare il Responsabile è tenuto a garantire che le persone autorizzate:

- si siano impegnate ad assicurare la riservatezza o abbiano l'obbligo legale di riservatezza;
- siano state istruite sulla procedura di gestione degli incidenti di sicurezza.

2.4 **Amministratori di sistema (Solo se applicabile)** Il Responsabile garantisce di nominare gli "Amministratori di sistema", con l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato, e l'impegno di attenersi al rispetto di quanto contenuto nel provvedimento del Garante Privacy del 25.06.2009 : *"Modifiche del provvedimento del 27.11.2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema*" del 25.6.2009.

2.5. **Sub- Responsabili**. Il Responsabile può ricorrere ad altro Responsabile (di seguito "Sub Responsabile/i") per gestire attività del trattamento specifiche, solo previa autorizzazione da parte del Titolare.
In tal caso il Responsabile deve assicurare che il Sub-Responsabile presenti gli stessi requisiti di esperienza, capacità e affidabilità, nonchè le stesse garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo che il trattamento risponda alle esigenze del GDPR.

Il Responsabile è tenuto pertanto ad informare il Titolare, senza ritardo e per iscritto, per il tramite del DEC :

- di ogni cambiamento - aggiunta o sostituzione dei Sub-Responsabili;
- dei dati del contratto di esternalizzazione del servizio/fornitura
- delle attività di trattamento delegate, dell'l'identità e degli indirizzi del Sub-Responsabile.

Il Titolare del trattamento dispone di un tempo massimo di 10 giorni a partire dalla data di ricevimento della comunicazione del Responsabile per presentare le proprie obiezioni.

Il Sub-Responsabile deve rispettare gli obblighi del presente contratto per conto e secondo le istruzioni del Titolare. Nel caso di mancato adempimento delle obbligazioni in materia di protezione dei dati da parte del Sub-Responsabile, il fornitore conserva nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi del Sub Responsabile.

2-6-. Trasferimento dei dati verso paese terzi o organizzazioni internazionali

Qualsiasi trasferimento di dati personali verso paesi terzi o organizzazioni internazionali da parte del Responsabile deve avvenire esclusivamente sulla base di istruzioni documentate da parte del Titolare e deve sempre avvenire in conformità a quanto previsto al Capo V del GDPR.

Nel caso in cui il Responsabile del trattamento è tenuto a procedere ad un trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, in virtù delle leggi dell'Unione o delle leggi dello Stato membro al quale è sottoposto, lo stesso deve informare il Titolare del trattamento di quest'obbligo giuridico, prima del trattamento, a meno che le leggi interessate proibiscano una tale informazione per motivi importanti di interesse pubblico.

2.7- Supporto al Titolare del trattamento. Per quanto possibile, il Responsabile del trattamento deve far sì che il Titolare del trattamento sia coadiuvato nei propri obblighi di far seguito alle domande di esercizio dei **diritti delle persone interessate**: di cui articoli da 12 a 23 del RGPD: diritto di accesso, di rettifica, di cancellazione e di opposizione, diritto alla limitazione del trattamento, diritto a trasportare i dati (portabiità), diritto di non essere oggetto di una decisione individuale automatizzata (compreso il profilo).

Qualora le persone interessate esercitassero presso il Responsabile del trattamento domande d'esercizio dei propri diritti, questi deve inviare le domande ricevute all'indirizzo PEC del Titolare, aousanluigigonzaga@pec.sanluigi.piemonte.it
La comunicazione deve essere effettuata immediatamente e in nessun caso oltre il giorno lavorativo seguente alla ricezione dell'istanza, unitamente, ove necessario, con altre informazioni che possono

essere rilevanti per assolvere la richiesta.

2.8. Comunicazione della violazione di dati personali- Il Responsabile informerà il Titolare senza ritardo di ogni incidente di sicurezza, di una violazione o sospetta **violazione dei dati** del Titolare (c.d. **"data breach").** Tale comunicazione dovrà essere effettuata telefonicamente e con PEC (le modalità non sono alternative) ai soggetti individuati quali Riceventi nella procedura aziendale adottata per le violazioni in oggetto, reperibile sul sito aziendale nell'Area Privacy. Tale comunicazione dovrà avvenire, in ogni caso, entro e **non oltre 24 ore** dall'evento.
Il Responsabile in caso di data breach deve:

- fornire immediatamente al Titolare una descrizione dettagliata della violazione, e qualsivoglia ulteriore informazione il Titolare possa richiedere in relazione ad essa, tra cui a titolo esemplificativo e non esaustivo, la natura della violazione, il numero approssimativo di interessati coinvolti, le categorie di dati in questione, il numero approssimativo di registrazioni di dati in questione, il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere informazioni, le probabili conseguenze della violazione dei dati personali;
- attivarsi per mitigare gli effetti delle violazioni, comunicando al Titolare misure intraprese o proposte per rimediare alla violazione di dati, mitigare l'impatto sugli interessati, prevenire il ripetersi di violazioni;
- attuare tempestivamente tutte le azioni correttive approvate e/o richieste dal Titolare.

Il Responsabile non coinvolgerà né renderà comunicazione alcuna a terze parti in merito a violazioni senza la preventiva approvazione scritta da parte del Titolare.

Il Responsabile deve mantenere un registro degli incidenti di sicurezza, anche qualora non vi siano violazioni, per coadiuvare il Titolare nel suo obbligo relativo al paragrafo 5 dell'art. 33 del RGPD.
A seguito del verificarsi di detti incidenti il Titolare potrà:

1) fare attività di Audit, anche senza preavviso e avvalendosi di soggetti terzi;
2) prescrivere ulteriori misure di sicurezza anche apportando modifiche a quelle in essere con particolare riferimento al presente accordo;
3) attivare azioni di rivalsa nei confronti del Responsabile;
4) applicare le penali contrattuali;
5) risolvere il contratto.

2.10Il Responsabile del trattamento, se previsto art. 30, comma 2 e 5, RGPD tiene per iscritto un **registro** di tutte le categorie di attività relative al trattamento svolte per conto del Titolare, e delle applicazioni informatizzate utilizzate, nel pieno rispetto del RGPD.

2.11.Il Responsabile garantisce l'applicazione dei principi (utilizzando i materiali, i prodotti, le applicazioni od i servizi) di **protezione dei dati a partire da quando questi vengono progettati** e della **protezione dei dati di default**.

2.12.Il Responsabile del trattamento assiste il Titolare del trattamento nel garantire gli obblighi di cui all'art. 35 "valutazione d'impatto sulla protezione dei dati" e all'art. 36 "consultazione preventiva", ove previsti.

2.13. Il Responsabile del trattamento comunica al Titolare del trattamento **il nome ed i dati di contatto del proprio Responsabile della Protezione dei Dati**, qualora ne abbia designato uno conformemente all'articolo 37 del RGPD, in caso contrario, il nome ed i dati di contatto di un referente privacy.

2.14.Il Responsabile mette a disposizione del Titolare del trattamento tutta la **documentazione e le informazioni** necessarie per dimostrare il rispetto degli obblighi di cui al GDPR, per permettere la realizzazione di revisioni, comprese le ispezioni, anche senza preavviso, realizzate dal Titolare del trattamento o da altro soggetto da questo incaricato. Per le ispezioni e la Direzione dell'Esecuzione in generale valgono le norme vigenti del Codice dei Contratti Pubblici.

2.15. Al termine della prestazione dei servizi relativi al trattamento di questi dati, il Responsabile del trattamento s'impegna ad eseguire le operazioni precisate nell'Allegato PLA.

2.16. In caso di contrasto tra le disposizioni della documentazione di fornitura prevale la versione più favorevole all'Azienda.

3. Obblighi del Titolare:

Il Titolare del trattamento è tenuto a:

1. fornire al Responsabile del trattamento le informazioni indicate in premessa per lo svolgimento del servizio oggetto del contratto;
2. supervisionare il trattamento, comprese le revisioni e le ispezioni presso il Responsabile del trattamento;
3. vigilare, in anticipo e durante la durata di tutto il trattamento, sul rispetto degli obblighi previsti dal GDPR sulla protezione dei dati da parte del Responsabile del trattamento;
4. documentare per iscritto tutte le istruzioni riguardanti il trattamento dei dati verso il Responsabile del trattamento;
5. effettuare una valutazione d'impatto sulla protezione dei dati personali relativamente alle operazioni di trattamento da svolgere da parte del Responsabile, ove previsto;
6. effettuare le consultazioni preventive necessarie, ove previsto;
7. fornire le informazioni alle persone interessate per le operazioni di trattamento dati, nel caso in cui non spetti al Responsabile.

4. Durata

La durata del presente accordo è pari alla durata del contratto.

Il Responsabile garantisce la riservatezza dei dati personali trattati nell'ambito del presente contratto anche oltre la scadenza dello stesso.

Il Titolare può risolvere il presente accordo ed il contratto in ogni momento per grave inadempimento, quale a titolo meramente esemplificativo e non esaustivo la violazione da parte del Responsabile delle normative in materia di protezione dei dati o delle disposizioni del presente accordo, ovvero nel caso in cui il Responsabile non sia in grado o non intenda seguire un'istruzione fornita dal Titolare, o qualora, in contrasto con quanto stabilito nel presente accordo, il Responsabile rifiuti di far accedere il Titolare nei propri locali al fine di monitorare il rispetto del presente accordo, con particolare riferimento alle misure tecniche ed organizzative adottate.
Al termine della fornitura/servizio, il Responsabile ha l'obbligo di eliminare tutti i dati personali elaborati per conto del titolare e certificare al titolare l'avvenuta cancellazione (oppure: restituire tutti i dati personali al titolare ed eliminare copie esistenti a meno che il diritto dell'Unione o degli stati membri non richieda la conservazione dei dati personali)

5. Comunicazioni

Tutte le comunicazioni previste dal presente Accordo, nonché in generale ogni comunicazione in materia di tutela dei dati personali e di data breach, dovranno essere effettuate:

a) quanto al Titolare presso AOU San luigi Gonzaga di Orbassano
aousanluigigonzaga@pec.sanluigi.piemonte.it

e-mail del RUP e del DEC ……..

e mail del DPO o RPD: rdp@sanluigi.piemonte.it

b) quanto al Responsabile presso……. (Ragione sociale del Fornitore)
Indirizzo Sede Legale ……..

Contatto: nome e cognome della persona fisica : ……..

casella e-mail: ……..

nome e cognome del DPO: ……

casella e-mail del DPO: ……

Foro competente

Per tutte le controversie che dovessero sorgere con riferimento al presente Accordo sarà esclusivamente competente il Foro di Torino.

Data _____

Il Titolare del Trattamento	Il Responsabile del Trattamento
_____	_____

ALLEGATO PLA (Privacy Level Agreement)[1]

(VEDASI DOCUMENTAZIONE DELLA PROCEDURA DI SCELTA DEL CONTRAENTE);

Fornitura/Servizio _____
Durata Fornitura/Servizio _____

Operazioni di trattamento consentite (art. 4 GDPR)	□ Raccolta □ Registrazione □ Organizzazione □ Strutturazione □ Conservazione □ Adattamento/Modifica □ Estrazione □ Consultazione □ Uso □ Inteconnessione/Raffronto con altri trattamenti/archivi □ Comunicazione all'interessato □ Comunicazione a Terzi □ Diffusione □ Limitazione □ Cancellazione/Distruzione □ Altro (Specificare*)*
Finalità del trattamento	□ per l'Azienda il raggiungimento degli scopi istituzionali □ per il fornitore il soddisfacimento degli obblighi contrattuali assunti □
Categorie di interessati cui si riferiscono i dati	□ pazienti, anche minori, ricoverati in regime ordinario e in D.H. □ pazienti ambulatoriali (SSN e LP) □ familiari di assistiti □ dipendenti,altri collaboratori e assimilabili □ professionisti e legali rappresentanti/procuratori di impresa
Tipologia di dati personali trattati	□ dati identificativi (nome, cognome,e-mail, numero di telefono, etc,) □ dati relativi alla salute □ dati genetici

1 Tale allegato dovrà essere compilato in versione bozza a cura del richiedente la fornitura. Esso sarà aggiornato a cura del RUP/DEC a seguito dell'aggiudicazione (almeno nei casi in cui sia prevista la valutazione delle caratteristiche di sicurezza della fornitura oppure quando il fornitore abbia previsto utilizzo di mezzi di trattamento non strettamente richiesti dalla documentazione contrattuale). L'Ufficio Privacy può essere consultato. Il rispetto di quanto specificato in questo documento dovrà essere puntualmente verificato a cura di DEC/RUP con il supporto dell'Ufficio Privacy

	□ dati biometrici □ origine etnica □ convinzioni religiose □ convinzioni filosofiche □ adesione a partiti, sindacati, associazioni od organizzazioni religiose □ abitudini sessuali □ dati relativi a condanne penali e reati □ altro (specificare)
Sub-responsabili *(Indicare i Sub-responsabili già contrattualizzati, quelli che si intendono contrattualizzare, nonchè i loro ulteriori responsabili (fornitori dei sub-responsabili)*	

Istruzioni in merito al trattamento dei dati personali

Il Responsabile si impegna a mettere in atto e mantenere:

- le misure di sicurezza previste dal piano di gestione rischi predisposto dal Responsabile;
- le misure di sicurezza specificate di seguito:

  - *la pseudonomizzazione e la cifratura dei dati a carattere personale;*
  - *adozione di mezzi che permettono di garantire costantemente la confidenzialità, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;*
  - *l'adozione di mezzi che permettono di ristabilire la disponibilità dei dati a carattere personale e l'accesso a questi nei tempi appropriati in caso di incidente fisico o tecnico;*
  - *l'adozione di una procedura che mira a testare, ad analizzare ed a valutare regolarmente l'efficacia delle misure tecniche ed organizzative per assicurare la sicurezza del trattamento;*
  - *adozione di procedure per la gestione a norma di legge copia dei log di accesso all'applicativo e di sistema.*

- le misure di sicurezza previste da norme e migliori prassi attuali e future, a cui si impegna a conformarsi (senza ulteriori oneri per il Titolare), tra cui (*EVADERE/INTEGRARE secondo l'oggetto del contratto*:
  - Le norme specifiche in materia di Privacy eventualmente applicabili al Responsabile (per esempio Regolamento e Privacy);
  - Le disposizioni attuative emanate dalla Commissione Europea in materia di Privacy;
  - Le disposizioni emanate dal Comitato Europeo per la Protezione dei Dati;
  - Le Linee Guida del gruppo di lavoro (WP) Art.29;
  - Le Opinioni e Raccomandazioni del gruppo di lavoro (WP) Art.29;
  - Le norme nazionali italiane (per esempio derivanti dalla L.25 ottobre 2017, n. 163, art. 13);

- Le autorizzazioni generali e specifiche del Garante;
- i provvedimenti del Garante applicabili e in particolare:
    - Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008;
    - Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali - 13 ottobre 2008;
    - Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie - 8 maggio 2014 e relative FAQ;
    - Provvedimento in materia di videosorveglianza - 8 aprile 2010;
    - Adempimenti semplificati per il customer care (inbound) - 15 novembre 2007
    - RFID Etichette intelligenti: prescrizioni - 9 Marzo 2005;
    - Provvedimento generale prescrittivo in tema di biometria - 12 novembre 2014;
    - Sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro - 4 ottobre 2011;
    - Sistemi di videosorveglianza per il controllo della procedura di raccolta del campione urinario a fini certificatori o di cura della salute - 15 maggio 2013;
- Le Linee Guida del Garante in materia di:
    - Posta elettronica e internet – 1° marzo 2007;
    - Trattamento di dati personali per profilazione on line - 19 marzo 2015;
    - Trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati – 15 maggio 2014;
    - Dossier sanitario - 4 giugno 2015
    - Svolgimento di indagini di customer satisfaction in ambito sanitario - 5 maggio 2011;
- Le norme del Codice Privacy non in contrasto con il Regolamento Europeo e non oggetto di abrogazione/modifica
- Le buone prassi in materia di sicurezza o Privacy:
    - Proposte da ENISA (Agenzia europea per la sicurezza delle reti e dell'informazione)
    - Emanate dall'Agenzia per l'Italia Digitale
    - Misure minime di sicurezza ICT per le pubbliche amministrazioni
    - Proposte da associazioni:
        - Center for Internet Security
        - Critical Security Controls for Effective Cyber Defense
        - CIS Benchmarks

- ISO 27001, ISO 29151, ISO 27002, ISO 27005, ISO 27035

[Nella misura in cui l'articolo 32 del regolamento europeo sulla protezione dei dati prevede che la messa in opera delle misure di sicurezza spetti al Titolare del trattamento ed al responsabile del trattamento, si raccomanda di determinare precisamente le responsabilità di ciascuna parte riguardo alle misure da mettere in opera]

Trasferimenti all'estero

Sono vietati tutti i trasferimenti di dati personali al di fuori dello Stato Italiano.

Informativa

(se previsto)

Il Responsabile del trattamento, al momento della raccolta dei dati, deve fornire alle persone interessate dalle operazioni del trattamento le informazioni relative ai trattamenti dei dati che realizza, tra le quali anche l'eventuale uso di strumenti di profilazione. La formulazione ed il formato dell'informazione deve essere concordata con il Titolare del trattamento prima della raccolta dei dati.

Gestione di fine contratto

Al termine della prestazione dei servizi relativi al trattamento di questi dati, il Responsabile del trattamento s'impegna a:

1. trasmettere i dati a carattere personale al fornitore subentrante designato dal Titolare del trattamento
2. restituire tutti i dati a carattere personale al Titolare del trattamento
3. distruggere tutti i dati a carattere personale in loro possesso

Una volta distrutte, il responsabile del trattamento deve dare evidenza per iscritto della distruzione.