Sistema Socio Sanitario

Regione Lombardia

ATS Brianza

PUBBLICATA ALL'ALBO ON-LINE IL

16 OTT. 2018

DELIBERAZIONE N. 626 **DEL** - 8 OTT. 2018

OGGETTO: Mandato irrevocabile a Finlombarda spa per il pagamento dei fornitori di beni e servizi – Integrazione contratto

L'anno 2018 il giorno 08 del mese di ottobre , in Monza nella sede legale dell'ATS della Brianza, il Direttore Generale dr. Massimo Giupponi prende in esame l'argomento in oggetto e delibera quanto segue

IL DIRETTORE GENERALE

PREMESSO che con deliberazione n. 763 del 28.12.2017, in adesione alle disposizioni regionali. si è disposto di sottoscrivere il contratto allegato al presente provvedimento, quale parte integrante e sostanziale, in forza del quale viene rinnovato il mandato irrevocabile a Finlombarda Spa di effettuare pagamenti in nome e per conto della ATS Brianza, alle condizioni nello stesso dettagliate, per il periodo gennaio 2018 - 31.12.2020;

DATO ATTO che Finlombarda ha espresso la necessità di integrare e aggiornare il contratto sopraddetto con le seguenti disposizioni cogenti:

- Regolamento UE 2016/679 ("GDPR") che ha modificato la disciplina in materia di protezione dei dati e del D.lgs n. 101 del 10 agosto 2018 che, sulla base del GDPR, ha modificato il Codice Privacy ;
- Decreto MEF del 25 settembre 2017 che, a far data dal 1° ottobre 2018, ha introdotto l'obbligo delle rilevazioni Siope+ alle Aziende Sanitarie, agli Enti e alle Società che effettuano pagamenti per loro conto, ed ha comportato l'esigenza di sviluppare un nuovo applicativo informativo evolutivo rispetto al Sistema Informativo G3S

RITENUTO di acconsentire all'integrazione contrattuale richiesta, allegata al presente atto quale parte integrante e sostanziale, a decorrere dal 1.10.2018;

ATTESO che il mandato è a titolo oneroso, in considerazione dei compensi che Regione Lombardia corrisponde a Finlombarda Spa, per la gestione del "Fondo Socio-Sanitario" a favore della ATS Brianza, per il pagamento dei fornitori e che nessun onere economico grava direttamente su questa ATS ;

SU PROPOSTA del Responsabile del U.O.C Affari Generali e Legali;

VISTE:

- l'attestazione di regolarità tecnica e di legittimità del presente provvedimento espressa dal Responsabile del U.O.C Affari Generali e Legali proponente
- l'attestazione di regolarità contabile e della relativa copertura finanziaria da parte del Responsabile del Servizio Economico;

riportate in calce al presente provvedimento;

ACQUISITI i pareri favorevoli espressi dal Direttore Amministrativo, dal Direttore Sanitario e dal Direttore Sociosanitario

DELIBERA

per le motivazioni indicate in premessa

- di approvare e sottoscrivere l'integrazione al contratto di mandato irrevocabile a Finlombarda Spa, come da documento allegato al presente atto quale parte integrante e sostanziale, in forza del quale viene aggiornato lo stesso alle disposizioni normative cogenti specificate in premessa;

- di evidenziare che il mandato è a titolo oneroso, in considerazione dei compensi che Regione Lombardia corrisponde a Finlombarda Spa, per la gestione del "Fondo Socio-Sanitario" a favore della ATS Brianza, per il pagamento dei fornitori e che nessun onere economico grava direttamente su questa ATS;

- di incaricare il Dirigente dell' UOC Affari Generali e Legali, quale Responsabile del Procedimento, degli adempimenti legati al perfezionamento del contratto di cui trattasi ed il Direttore dell' UOC Contabilità e Finanza di ogni ulteriore adempimento conseguente l'adozione del presente provvedimento;

- di depositare copia del contratto, debitamente sottoscritto, agli atti dell' UOC Affari Generali e Legali;

- di dare atto che ai sensi e per gli effetti del combinato disposto dei commi 4 e 6 dell'art. 17 della L.R. n. 33/2009, come modificata dall'art. 1 della L.R. n. 23/2015, il presente provvedimento è immediatamente esecutivo;

- di disporre, ai sensi del medesimo art. 17, comma 6, della L.R. n. 33/2009, la pubblicazione del presente provvedimento all'albo on line dell'Ente;

- di disporre l'invio della presente deliberazione ai Settori ed Uffici interessati.

IL DIRETTORE GENERALE
(Dr. Massimo Giupponi)

IL DIRETTORE AMMINISTRATIVO
(Dr. Paolo Giuseppe Cogliati)

IL DIRETTORE SANITARIO
(Dott. Salvatore Silvano Lopez)

IL DIRETTORE SOCIOSANITARIO
(Dott. Oliviero Rinaldi)

ATTESTAZIONE DI REGOLARITA' TECNICA E CONTABILE

UOC PROPONENTE: AFFARI GENERALI E LEGALI

Si attesta la regolarità tecnica e la legittimità del provvedimento essendo state osservate le norme e le procedure previste per la specifica materia.

IL RESPONSABILE
(Dr.a Raffaella Clelia Borra)

(firma)

SERVIZIO ECONOMICO FINANZIARIO

Si attesta la regolarità contabile e la copertura finanziaria della spesa complessiva scaturente dal presente provvedimento:

Bilancio anno _____: ☐ Sanitario ☐ Socio Sanitario Integrato (ASSI) ☐ Sociale

Impegno: _____

Conto n. : _____ Importo : _____

IL RESPONSABILE SERVIZIO ECONOMICO FINANZIARIO
(Dr. Elena Sartori)

NOTE: _____

Parte riservata ad acquisti di beni e servizi al di fuori delle Convenzioni CONSIP, ARCA e MEPA

SERVIZIO/U.O. PROPONENTE: _____

☐ Si attesta che i beni/servizi oggetto di acquisto con il presente provvedimento non rientrano nelle categorie trattate dalla Concessionaria Servizi Informatici Pubblici (CONSIP S.p.A.) del Ministero dell'Economia e delle Finanze, per cui nella fattispecie non è applicabile il disposto di cui all'art. 26, comma 3, della Legge n. 488/1999 e successive modificazioni ed integrazioni e neppure in quelle trattate dall'Agenzia Regionale Centrale Acquisti (ARCA) di cui alla L.R. n. 33 del 28.12.2007 e ss.mm.ii.

☐ Si attesta che il bene/servizio da acquisire, oggetto del presente provvedimento, né si è reperito né è presente sul Mercato Elettronico della Pubblica Amministrazione (MEPA) di cui all'art. 11 DPR 101/2002 ovvero è presente ma trattasi di prodotto/servizio comune e standardizzato non idoneo, in quanto tale, a soddisfare le esigenze specifiche e particolari dell'Azienda.

IL RESPONSABILE

_____

CERTIFICATO DI PUBBLICAZIONE
Copia della presente deliberazione è stata pubblicata all'Albo pretorio on line dell'Azienda per la durata di giorni quindici consecutivi dal al inclusi. Monza, lì..... Il Funzionario addetto

ALLEGATO ALLA DELIBERAZIONE DEL DIRETTORE GENERALE

N. 626 DEL - 8 OTT. 2018

Contratto di Mandato irrevocabile

Atto integrativo

TRA

AGENZIA PER LA TUTELA DELLA SALUTE DELLA BRIANZA, con sede in Monza (MB), Viale Elvezia, 2, P.IVA e C.F. 09314190969, nella persona del Direttore Generale dott. Massimo Giovanni Giupponi
(di seguito anche la "***Mandante***")

- da una parte -

E

FINLOMBARDA S.P.A., con sede in Milano, via Filzi, 25/A, P.IVA e numero di iscrizione al Registro delle Imprese di Milano 01445100157, in persona del Direttore Generale Dott. Filippo Bongiovanni
(di seguito anche la "***Mandataria***" o "***Finlombarda***")

- dall'altra parte -

di seguito congiuntamente "**Le Parti**"

PREMESSO CHE

A. in data 03/01/2018 le Parti hanno sottoscritto un contratto di mandato irrevocabile (il "**Mandato**"), affinché Finlombarda potesse provvedere, in conformità ai termini e condizioni del Mandato medesimo, ad eseguire il pagamento dei crediti che i fornitori vantano nei confronti della Mandante attraverso il "Sistema Informativo G3S";

B. nel frattempo, in data 25 maggio 2018, è entrato in vigore il Regolamento UE 2016/679 ("**GDPR**") che ha modificato la disciplina in materia di protezione dei dati e, in data 19 settembre 2018, il decreto legislativo 10 agosto 2018 n. 101 che, sulla base del GDPR, ha modificato il Codice Privacy;

C. in aggiunta, l'obbligo introdotto con decreto MEF del 25 settembre 2017 delle rilevazioni Siope+ alle Aziende Sanitarie e agli enti e alle società che effettuano pagamenti per loro conto, a far data dal 1° ottobre 2018, ha comportato l'esigenza di sviluppare un nuovo applicativo informativo evolutivo rispetto al Sistema Informativo G3S;

D. a tal fine, Regione Lombardia ha dato incarico a Lombardia Informatica S.p.A. di sviluppare il nuovo applicativo informatico;

E. alla luce di quanto sopra si è reso, quindi, necessario rivedere il Mandato per adeguarlo alle nuove previsioni normative di cui al GDPR e al Codice Privacy, così come modificato dal d. lgs. n. 101/2018 e per integrare la procedura di pagamento di cui all'Allegato 1: "Operating Memorandum" del Mandato in seguito all'implementazione del nuovo sistema informativo;

F. ai sensi dell'art. 6.4 del Mandato "*la Mandante si rende disponibile sin d'ora a sottoscrivere ogni ulteriore atto finalizzato a permettere il pieno svolgimento delle attività di cui al presente mandato che si dovesse rendere necessario, ivi compreso il conferimento alla Mandataria, su richiesta di quest'ultima, di eventuali procure speciali*";

In forza di tutto quanto indicato in premessa, le Parti convengono di modificare ed integrare il Mandato come segue:

1. la dicitura "Sistema Informativo G3S" si intende sostituita con "Sistema Informativo G3S o successive evoluzioni";

2. all'art. 13, il richiamo all'art. 29 del Codice Privacy, si intende sostituito con il riferimento all'art. 28 del GDPR;

3. l'Allegato 1 "Operating Memorandum" è sostituito con il documento "Allegato 1: Operating Memorandum" al presente atto integrativo;

4. l'allegato 2 "Privacy" è sostituito con il documento "Allegato 2: Privacy" al presente atto integrativo;

5. il presente atto integrativo diviene efficace a decorrere dal 1° ottobre 2018;

6. fatto salvo quanto previsto nel presente atto integrativo, le altre disposizioni e pattuizioni del Mandato restano invariate.

Luogo e data

(La Mandante)

Luogo e data

Per accettazione

(La Mandataria)

Allegato 1: Operating Memorandum

La procedura di pagamento attraverso il Sistema Informativo G3S si compone delle seguenti fasi:

1. definizione da parte della Regione dei criteri di pagamento;
2. comunicazione dei criteri di pagamento alla Mandante anche attraverso il Sistema Informativo G3S;
3. trasmissione, da parte della Mandante, dei dati necessari per il pagamento ("Proposte di mandato") attraverso il sistema informativo G3S. Sarà responsabilità della Mandante inserire nelle Proposte di mandato firmate digitalmente unicamente fatture e note di credito che rispettino:
    a. i criteri di cui al punto 1,
    b. i termini di pagamento previsti,
    c. gli adempimenti amministrativi propedeutici al pagamento delle fatture;
4. effettuazione del pagamento da parte di Finlombarda, mediante l'invio al proprio tesoriere di apposito flusso, generato dal Sistema Informativo G3S, in seguito all'effettuazione dei seguenti controlli:
    a. verifica automatica da parte del Sistema Informativo G3S della completezza e della correttezza formale delle informazioni ricevute dalla Mandante,
    b. verifica da parte di Finlombarda delle disponibilità del Fondo e di eventuali ulteriori indicazioni ricevute dalla Regione;
5. messa a disposizione, da parte di Finlombarda, attraverso il Sistema Informativo G3S, delle informazioni circa gli esiti dei pagamenti. Il Sistema Informativo G3S invierà in automatico ai beneficiari il dettaglio dei pagamenti effettuati a loro favore comunicandoli altresì alla Mandante che, tramite apposito sito web, potrà consultare gli esiti dei pagamenti e scaricare la relativa reportistica.

La procedura di pagamento attraverso l'evoluzione del Sistema Informativo G3S si compone delle seguenti fasi:

1. definizione da parte della Regione dei criteri di pagamento;

2. comunicazione dei criteri di pagamento alla Mandante anche attraverso il Nuovo Sistema Informativo;
3. trasmissione, da parte della Mandante, dei dati necessari per il pagamento ("OPI") attraverso il Nuovo Sistema Informativo e per l'assolvimento degli obblighi previsti dal Decreto Siope+. Sarà responsabilità della Mandante inserire negli OPI unicamente fatture e note di credito che rispettino:
   a. i criteri di cui al punto 1,
   b. i termini di pagamento previsti,
   c. gli adempimenti amministrativi propedeutici al pagamento delle fatture;
4. trasmissione da parte di Finlombarda, tramite il Nuovo Sistema Informativo, all'infrastruttura Siope+ dei dati relativi ai pagamenti da effettuare in seguito all'effettuazione dei seguenti controlli:
   a. verifica automatica da parte del Nuovo Sistema Informativo della completezza e della correttezza formale delle informazioni ricevute dalla Mandante,
   b. verifica da parte di Finlombarda delle disponibilità del Fondo e di eventuali ulteriori indicazioni ricevute dalla Regione;
5. effettuazione del pagamento degli OPI da parte del tesoriere di Finlombarda, sulla base degli esiti restituiti dall'infrastruttura Siope+;
6. messa a disposizione, da parte del Nuovo Sistema Informativo, delle informazioni circa gli esiti dei pagamenti trasmessi dalla banca tesoriera alla infrastruttura Siope+. Il Nuovo Sistema Informativo invierà in automatico ai beneficiari il dettaglio dei pagamenti effettuati a loro favore comunicandoli altresì alla Mandante. Il Nuovo Sistema Informativo, inoltre, provvederà all'aggiornamento del giornale di cassa.

Si sottolinea che, data l'architettura del Nuovo Sistema Informativo, gli scambi di informazioni tra lo stesso e l'infrastruttura Siope+ sono interamente automatizzati. La Mandataria non può in alcun modo accedere alla base dati sottostante fornita dalla Mandante o dall'infrastruttura Siope+, né tantomeno modificarne il contenuto.

Allegato 2: Privacy

Nota: Le definizioni utilizzate nel Mandato cui la presente nomina è allegata, si intendono di seguito interamente richiamate. Si intendono altresì richiamate le definizioni utilizzate nel GDPR e nel Decreto Legislativo 30 Giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), così come modificato dal d. lgs. 10 agosto 2018 n. 101.

Nomina a responsabile del trattamento ai sensi dell'articolo 28 del GDPR.

Per effetto della presente ed in conseguenza del Mandato, ai sensi dell'articolo 28 del GDPR.

L'Azienda/Fondazione AGENZIA PER LA TUTELA DELLA SALUTE DELLA BRIANZA, Titolare del trattamento, nella persona del responsabile privacy dott. Massimo Giovanni Giupponi, conferisce l'incarico di Responsabile Esterno del trattamento a Finlombarda.

Finlombarda accetta tale nomina.
Finlombarda si impegna a non divulgare né utilizzare per fini diversi da quelli inerenti il Mandato, anche successivamente alla cessazione dello stesso, le notizie riservate di cui verrà a conoscenza e come tali definite dal Titolare del Trattamento. Le parti dichiarano reciprocamente di essere informate e di acconsentire che i dati personali forniti o raccolti in conseguenza della stipulazione del Mandato saranno trattati esclusivamente per le finalità ivi indicate ed in conformità a quanto previsto dal GDPR; Finlombarda non potrà diffondere né comunicare tali dati, salvo che a regione Lombardia, oltre ai casi previsti nel mandato o nei casi strettamente necessari per il corretto adempimento dello stesso.

Il Responsabile del trattamento individuato è tenuto ad effettuare il trattamento dei dati nel rispetto di quanto disposto dal GDPR, dal Codice in materia di Protezione dei dati personali, D. Lgs. n. 196/2003 e s.m.i. e di ogni ulteriore provvedimento del Garante per la Protezione dei dati personali, secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità degli Interessati, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.
Il Responsabile è tenuto a trattare i dati personali nel rispetto dei principi di necessità, pertinenza e non eccedenza, in modo lecito e secondo correttezza, per scopi legittimi e determinati, assicurando l'esattezza e la completezza dei dati e conservando i dati in una forma che consenta l'identificazione dell'Interessato per un periodo non superiore a quello occorrente alle finalità per i quali sono stati raccolti e trattati, e provvedendo, quando necessario, alla loro rettifica e aggiornamento.
Il Responsabile è tenuto ad iniziare eventuali nuovi trattamenti solo in seguito a richiesta da parte del Titolare del trattamento.

In caso di cessazione di un trattamento, il Responsabile dovrà seguire le istruzioni impartite dal Titolare e, in assenza di queste, provvedere alla distruzione dei dati personali in suo possesso, ai sensi della vigente normativa in materia di protezione dei dati.
Il Responsabile è tenuto ad adottare, in relazione al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, tutte le misure di sicurezza idonee a evitare rischi di distruzione, danneggiamento o perdita, anche accidentale, dei dati, nonché pericoli di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, secondo quanto previsto dalla vigente normativa privacy. In particolare, deve assicurare in ogni momento che la sicurezza fisica e logica dei dati oggetto di trattamento sia conforme alle norme vigenti.

Le misure di sicurezza adottate dovranno in ogni situazione uniformarsi allo "standard" di maggiore sicurezza fra le disposizioni di legge e gli elementi contrattuali e/o progettuali.
Il Responsabile, è inoltre tenuto a, limitatamente ai propri sistemi informativi legati all'esecuzione del Mandato:

1. individuare per iscritto le persone autorizzate al trattamento dei dati personali (gli Incaricati, persone fisiche o gruppi omogenei), impartire loro le istruzioni idonee alle attività da svolgere e vigilare sul loro operato;
2. elaborare un piano di formazione destinato agli Incaricati;
3. assicurarsi che ad ogni Incaricato sia assegnata una credenziale di autenticazione. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'Incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'Incaricato, eventualmente associato a un codice identificativo o a una parola chiave;
4. prescrivere necessarie cautele per assicurare la segretezza della componente riservata della credenziale e/o la diligente custodia del dispositivo in possesso ed uso esclusivo dell'Incaricato;
5. assicurare che la parola chiave, quando è prevista dal sistema di autenticazione, sia composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non deve contenere riferimenti agevolmente riconducibili all'Incaricato e deve essere modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi;
6. assicurare che il codice per l'identificazione, laddove utilizzato, non possa essere assegnato ad altri Incaricati, neppure in tempi diversi;
7. assicurare che sia operata la cancellazione del codice identificativo personale in caso venga a cessare la necessità di accesso da parte dell'Incaricato o intervenga un'inattività per più di sei mesi;

8. predisporre le necessarie procedure affinché, in caso di prolungata assenza o impedimento dell'Incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, si possa comunque assicurare la disponibilità di dati o strumenti elettronici.
   In tal caso la custodia delle copie delle credenziali deve essere organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia;
9. prevedere, con criteri restrittivi, profili di autorizzazione di accesso per ogni singolo Incaricato o gruppo omogeneo e configurarli prima dell'inizio dei trattamenti;
10. prevedere l'impiego di sistemi di autorizzazione che, secondo il concetto che "è vietato ciò che non è espressamente permesso", consentono di accedere ai dati per effettuare le operazioni di trattamento secondo il proprio specifico profilo utente;
11. verificare, ad intervalli almeno annuali, la sussistenza delle ragioni che hanno portato al rilascio della autorizzazione;
12. assicurare che nel caso di Operatori telefonici, Incaricati del trattamento, questi nelle comunicazioni vocali scambiate durante lo svolgimento delle proprie attività si conformino alle disposizioni specificatamente emesse dal Responsabile del trattamento per il rispetto dell'Utenza e la riservatezza delle informazioni trattate;
13. redigere e mantenere aggiornato un elenco con gli estremi identificativi delle persone fisiche che rivestono il ruolo di Amministratori di Sistema e, per ciascuno di essi, la descrizione delle funzioni che gli sono state attribuite nell'ambito delle attività svolte per conto del Titolare e implementare le ulteriori misure, come definito nel Provvedimento dell'Autorità Garante per la Protezione dei dati personali del 27/11/2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratori di sistema" e s.m.i.;
14. installare sugli elaboratori idonei programmi contro il rischio di intrusione e accesso abusivo in accordo ai requisiti di legge da aggiornare comunque ogni sei mesi ed in occasione di ogni versione disponibile dalla casa costruttrice;
15. prevedere, ogni qualvolta vi sia la segnalazione della presenza di vulnerabilità nei programmi utilizzati e la contemporanea disponibilità delle opportune modifiche, all'aggiornamento, entro un periodo di tempo non superiore a sei mesi, dei programmi utilizzati, o almeno alla valutazione degli impatti sull'aggiornamento;
16. prevedere l'adozione di copie di back-up e il ripristino dei dati in tempi certi e comunque non superiori a sette giorni.

Inoltre, nel caso di trattamento di dati sensibili, ai sensi della vigente normativa in materia di protezione dei dati, il Responsabile deve, limitatamente ai propri sistemi informativi legati all'esecuzione del Mandato:

1) prevedere che il riutilizzo dei supporti di memorizzazione sia possibile solamente nel caso in cui le informazioni precedentemente contenute non siano recuperabili; in caso contrario i supporti dovranno essere distrutti. In questo ambito risulta necessario procedere a:
   a) emanare adeguate istruzioni di comportamento a tutti gli Incaricati;
   b) effettuare una ricognizione completa di tutti i supporti di memoria che possano essere riutilizzabili, sia essi di tipo asportabile che presenti in aree di memoria interne al sistema operativo od in programmi, ove possano trovarsi dati sensibili;
   c) esaminare tutti i nuovi supporti, sistema operativo e programmi, che vengono inseriti nel sistema di trattamento dei dati, analizzando i possibili rischi ed impartendo specifiche istruzioni agli Incaricati.
2) assicurare che la memorizzazione dei dati sensibili su elenchi, registri o banche dati, avvenga in maniera da non permettere la diretta identificazione dell'interessato, ovvero che la memorizzazione dei dati sensibili sia cifrata o in alternativa che vi sia separazione tra i dati sensibili e gli altri dati personali che possano permettere l'identificazione dell'interessato;
3) assicurare che il trasferimento dei dati sensibili in formato elettronico, avvenga attraverso "canali sicuri" o in maniera cifrata.

Il Responsabile deve procedere ad un controllo periodico sui rischi effettivi e sulla efficacia delle contromisure adottate, e deve tenere in qualità di Responsabile il Registro del trattamento ai sensi dell'art. 30 del GDPR aggiornato e allineato ai trattamenti del Titolare per cui Finlombarda sia stata individuata quale Responsabile del trattamento.

In merito al trattamento dei dati personali con strumenti diversi da quelli elettronici, il Responsabile è tenuto a predisporre un archivio per gli atti e i documenti con dati personali individuando per iscritto gli Incaricati con i relativi profili di accesso ai dati ed ai documenti. Devono essere definite le procedure di deposito, custodia, consegna o restituzione e compartimentazione dei dati stessi (ad esempio un registro e degli armadi separati e chiusi). Il trattamento di dati sensibili, dovrà infine prevedere l'utilizzo di appositi contenitori con lucchetti o serrature e definire una procedura di gestione delle chiavi.

Il Responsabile è chiamato ad evadere tempestivamente le richieste del Titolare e degli Interessati e a proporre e/o adottare tempestivamente -se del caso d'intesa con altri soggetti Responsabili nel rispetto delle indicazioni espresse dal Titolare -, ogni soluzione organizzativa, logistica, tecnica e procedurale idonea ad assicurare l'osservanza delle disposizioni vigenti in materia di trattamento dei dati personali in modo da consentire l'esercizio dei diritti da parte degli Interessati.

Il Titolare del trattamento, come previsto dall' art. 4 del GDPR vigilerà sulla puntuale osservanza delle istruzioni impartite al Responsabile, effettuando periodiche azioni di verifica.

Il Responsabile è tenuto a comunicare al Titolare eventuali violazioni dei dati personali ai sensi degli artt. 33 e 34 del GDPR al fine di attivarsi secondo le

procedure previste dalla normativa alla comunicazione all'autorità di controllo, nonché ad avvisarlo tempestivamente qualora ricevesse ispezioni o richieste di informazioni, documenti od altro da parte dell'Autorità Garante in merito ai trattamenti effettuati per conto del Titolare.
Ogni ulteriore istruzione dovrà essere previamente accettata da Finlombarda, salvo il caso in cui tali istruzioni siano previste come necessarie da nuovi obblighi normativi. In tale ultimo caso, sarà sufficiente una comunicazione da parte del Titolare.