Ufficio d'Ambito di Lodi

azienda speciale provinciale per la regolazione e il controllo della gestione
del servizio idrico integrato

il Presidente

Decreto del Presidente	numero 9	del 10 ottobre 2018

OGGETTO: Nomina a Responsabile esterno del Trattamento dei dati. Provincia di Lodi.

IL PRESIDENTE

PREMESSO che:

- il sottoscritto è, in quanto Legale Rappresentante pro-tempore dell'Ufficio d'Ambito di Lodi, "Titolare del trattamento" come definito all'art. 4 del Regolamento UE 679/2016 in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali (RGPD);
- l'art. 4 comma 7 del RGPD definisce:
  - ✓ «Titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
  - ✓ «Responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- l'art. 28 del RGPD dispone che:
  a) qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto adeguate misure tecniche e organizzative in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato;
  b) il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche;
  c) i trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da

altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

1) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
2) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
3) adotti tutte le adeguate misure richieste ai sensi dell'articolo 32 del RGPD;

RICHIAMATA la Convenzione per la regolazione dei rapporti tra la Provincia di Lodi e l'Ufficio d'Ambito di Lodi stipulata il 20 maggio 2010 con scadenza al 31 dicembre 2012, prorogata dapprima al 31 dicembre 2013 e successivamente al 31 dicembre 2014, al 31 dicembre 2015 e al 31 dicembre 2018 con deliberazioni assunte dal CdA rispettivamente il 6 novembre 2012, il 12 novembre 2013, il 9 dicembre 2014 e il 5 novembre 2015;

CONSIDERATO che:

- tra i servizi erogati dalla Provincia all'Ufficio vi sono anche servizi che comportano il trattamento di dati personali, quali i servizi informatici, ivi compresa la gestione del programma di rilevazione delle presenze del personale, e, a fronte di specifica richiesta dell'Ufficio: corsi di formazione e aggiornamento a favore del personale dell'Ufficio, consulenza in materia di gestione delle risorse umane, condivisione di graduatorie di concorsi banditi dalla Provincia;
- l'Ufficio, in quanto fruitore dei servizi, riveste il ruolo di Titolare del trattamento dei dati personali di propria pertinenza, ospitati sui server provinciali, in relazione ai quali la Provincia di Lodi assume il ruolo di Responsabile del trattamento dei dati;
- in relazione ai medesimi dati personali di persone fisiche, la Provincia di Lodi assume, altresì, il compito di amministratore dei sistemi;

RITENUTO necessario integrare la Convenzione in essere definendo le modalità e le condizioni alle quali il Responsabile del trattamento si impegna ad effettuare, per conto del Titolare del trattamento, le operazioni di trattamento dei dati personali implicati dalla Convenzione;

VISTO lo Statuto aziendale;

DECRETA

1. di nominare la Provincia di Lodi quale *Responsabile esterno del trattamento*, ai sensi dell'art. 28 del Regolamento UE 2016/679, per i compiti ad essa affidati nell'ambito della Convenzione per la regolazione dei rapporti tra la Provincia di Lodi e l'Ufficio d'Ambito di Lodi stipulata il 20 maggio 2010 e rinnovata fino al 31 dicembre 2018;

2. di comunicare la presente nomina alla dott.ssa Donata Fraschini, Responsabile della Protezione dei Dati personali;
3. di specificare che il trattamento dei dati personali nel contesto dei servizi resi dalla Provincia di Lodi avverrà con le modalità definite nell'atto integrativo alla Convenzione, come concordato con la Provincia, che nel seguito si riporta:

PREMESSO che:

a. tra l'Ufficio d'Ambito di Lodi e la Provincia di Lodi è in essere una Convenzione per la regolazione dei rapporti tra la Provincia di Lodi e l'Ufficio d'Ambito di Lodi che contempla l'erogazione di servizi, anche informatici, di cui la presente è parte integrante;
b. nella presente Convenzione le parti concordano di definire:
   - con il termine "*Convenzione*" la Convenzione per la regolazione dei rapporti tra la Provincia di Lodi e l'Ufficio d'Ambito di Lodi stipulata tra le parti il 20 maggio 2010 e rinnovata fino al 31 dicembre 2018;
   - con il termine "*RGPD"* il 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;
   - con il termine *"Circolare"* la circolare AGID del 18 aprile 2017, n. 2/2017 avente oggetto "Misure Minime di Sicurezza ICT per le Pubbliche Amministrazioni";
   - con il termine "*Normativa Privacy*" le disposizioni del RGPD nonché tutte le altre disposizioni delle leggi dell'Unione o delle leggi degli Stati membri relative alla protezione dei dati personali e alla loro libera circolazione;
c. nello svolgimento del servizio, il Titolare del trattamento dei dati personali, ai sensi e per gli effetti dell'art. 4, comma 1, numero 7), del RGPD, è l'Ufficio d'Ambito di Lodi e incombe sul Titolare il compimento di tutti gli atti previsti dal RGPD e dalla Normativa Privacy per il trattamento dei dati personali, vale a dire l'informativa, la raccolta del consenso, l'adozione di tutte le misure autorizzative, di incarico e di conservazione e di altro tipo anche per realizzare il Sistema sicurezza, ivi comprese le relative misure minime incluse nella Circolare;

Ciò premesso, tra le parti

SI CONVIENE E SI STIPULA

quanto di seguito riportato:

Art. 1. Designazione del Responsabile del trattamento

1. Per i compiti che, in base alla Convenzione, sono affidati alla Provincia di Lodi, quest'ultima ai sensi dell'Art. 4, c. 1, n. 8), del RGPD è designata *Responsabile del trattamento*.
2. Il *Responsabile del trattamento* precisa di essere in grado di offrire garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti RGPD e garantisca la tutela dei diritti degli interessati.

Art. 2. Oggetto e durata della presente regolamentazione

1. Oggetto delle presenti condizioni è definire le modalità e le condizioni contrattuali alle quali il *Responsabile del trattamento* si impegna ad effettuare, per conto del *Titolare del trattamento*, le operazioni di trattamento dei dati personali quali definiti dalla Convenzione.
2. Nel quadro delle loro relazioni convenzionali, le parti si impegnano a rispettare la regolamentazione in vigore applicabile al trattamento dei dati a carattere personale (dati personali) e, in particolare, il "*RGPD*" e la "*Normativa Privacy*".
3. Il presente allegato avrà la durata della Convenzione a cui si riferisce.

Art. 3. Descrizione delle prestazioni del Responsabile del trattamento

1. Il *Responsabile del trattamento* è autorizzato a trattare, per conto del *Titolare del trattamento*, dati a carattere personale necessari per fornire i servizi previsti dalla Convenzione. I dati che il *Titolare del trattamento* ha già fornito e che fornirà avranno già acquisito il consenso degli interessati al loro trattamento ai sensi dell'art. 6, comma 1, lett. a), del RGPD, salvi i casi indicati nel predetto art. 6 di trattamento consentito anche in assenza di consenso.
2. Il *Titolare del trattamento* garantisce il *Responsabile del trattamento* di disporre legittimamente di tutte le informazioni (testi, dati, notizie, segni, immagini, suoni e quant'altro) che affiderà al *Responsabile del trattamento* per il loro trattamento, assicurando altresì che dette informazioni non violano in alcun modo diritti di terzi.
3. Il *Titolare del trattamento* mantiene la titolarità delle informazioni che saranno comunicate al *Responsabile del trattamento* per il servizio ed assume espressamente ogni più ampia responsabilità in ordine al contenuto dei relativi dati personali e manleva il *Responsabile del trattamento* da ogni obbligo e/o onere di accertamento e/o di controllo diretto e indiretto al riguardo.
4. La natura delle operazioni realizzate sui dati da parte del *Responsabile* è la messa in esercizio, manutenzione e aggiornamento del sistema informativo utilizzato dal *Titolare*.
5. La finalità del trattamento è di fornire un servizio di manutenzione e assistenza al *Titolare*. Il *Titolare del trattamento* dichiara che il trattamento è affidato al *Responsabile del trattamento* per lo svolgimento del servizio come meglio descritto nella Convenzione.
6. Per quanto di sua competenza, il *Responsabile del trattamento*, nel trattare i dati per l'erogazione del servizio, effettuerà il trattamento in osservanza:
   - dell'Art. 5 del RGPD relativo ai "Principi applicabili al trattamento dei dati personali";
   - delle misure elencate alla colonna 'Misure Minime' delle tabelle ABSC1, ABSC2, ABSC3, ABSC4, ABSC5, ABSC8, ABSC10 e ABSC13 della Circolare, ivi di seguito esplicitate:

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.

1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione
2	1	1	M	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

ABSC_ID			Livello	Descrizione
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.
3	4	1	M	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

ABSC_ID			Livello	Descrizione
4	1	1	M	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia

				per il sistema operativo sia per le applicazioni.
4	5	2	M	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.
4	7	1	M	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.
4	8	1	M	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).
4	8	2	M	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC_ID			Livello	Descrizione
5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.
5	7	1	M	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.
5	10	3	M	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le

				situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Livello	Descrizione
8	1	1	M	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.
8	9	1	M	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.
8	9	2	M	Filtrare il contenuto del traffico web.
8	9	3	M	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.

10	3	1	M	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.
10	4	1	M	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Livello	Descrizione
13	1	1	M	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.

7. La natura dei dati trattati dal *Responsabile del trattamento* varia in funzione del servizio fruito dal *Titolare*. Il trattamento potrebbe estendersi anche ai dati particolari di cui all'Art. 9 del RGPD per i quali il *Titolare del trattamento* e il *Responsabile del trattamento* rilasceranno ai propri Addetti l'autorizzazione.
8. Le categorie di persone interessate sono essenzialmente fruitori delle funzioni pubbliche proprie del *Titolare del trattamento* e dipendenti che, incaricati dal *Titolare*, trattano i dati del servizio informativo.
9. Per l'esecuzione dell'incarico oggetto della presente Convenzione, il *Titolare del trattamento* mette a disposizione del *Responsabile del trattamento* le informazioni necessarie all'esecuzione delle attività di assistenza e manutenzione e indirizzate all'utilizzo appropriato del sistema informativo.
10. Gli Incaricati al trattamento della Provincia di Lodi ricopriranno la figura di Incaricati al trattamento designati dal *Responsabile del trattamento* ai sensi dell'art. 28, comma 3, lett. B, del RGPD.
11. Poiché il trattamento dei dati è fatto anche direttamente dall'Ufficio d'Ambito, *Titolare del trattamento*, questi, per il trattamento diretto, provvederà a designare tali Addetti con l'osservanza di tutti gli obblighi della Normativa Privacy e con esonero del *Responsabile del trattamento*, in relazione a ciò, da ogni sorta di responsabilità. Gli addetti al trattamento per il *Titolare*, quindi, saranno designati dal *Titolare del trattamento* e gli addetti al trattamento per il *Responsabile del trattamento* saranno designati dal *Responsabile del trattamento* in ottemperanza ed osservanza delle disposizioni in merito dettate dal RGPD.
12. Le operazioni di trattamento saranno quindi effettuate per la Provincia di Lodi da Addetti che opereranno sotto la diretta autorità del *Responsabile del trattamento*, attenendosi alle istruzioni da questi impartite. La designazione sarà effettuata per iscritto e individuerà puntualmente l'ambito del trattamento consentito e autorizzato. Si considererà tale anche la documentata

preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito ed autorizzato agli addetti all'unità medesima.

13. Il *Responsabile del trattamento* si dichiara edotto che chiunque agisca sotto la sua autorità e abbia accesso a dati personali non può trattare tali dati se non è stato istruito in tal senso.

Art. 4. Obblighi del Responsabile del trattamento di fronte al *Titolare del trattamento*

1. Il *Responsabile del trattamento*, nello svolgimento delle sue funzioni, si impegna ad assolvere ed osservare i seguenti obblighi:

   a) Osservanza, nel trattamento dei dati personali, delle istruzioni date dal Titolare

   1) Il *Responsabile del trattamento* dovrà trattare i dati solo per le finalità specificate dal *Titolare* e per l'esecuzione delle prestazioni contrattuali.

   2) Il *Responsabile del trattamento* dovrà trattare i dati in conformità a quanto previsto nel Registro dei trattamenti per il Servizio ed il *Titolare* ritiene adeguate le misure di sicurezza ivi previste.

   3) I dati saranno trattati dal *Responsabile del trattamento* su territorio Italiano. Qualora in futuro il trattamento dovrà essere eseguito anche all'estero sia in paesi UE che Extra UE, il *Responsabile* ne darà immediata comunicazione al *Titolare* per convenire le garanzie che lo stesso richiederà in funzione del luogo in cui il trattamento sarà svolto.

   b) Garantire la riservatezza

   1) Il *Responsabile del trattamento* garantisce l'osservanza della riservatezza dei dati a carattere personale (dati personali) trattati nell'ambito della presente Convenzione.

   2) Il *Responsabile del trattamento* garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza e che esse ricevano e che venga loro data la formazione necessaria in materia di trattamenti dei dati personali e di protezione dei dati a carattere personale.

   c) Adozione delle misure di sicurezza del trattamento

   1) Il *Responsabile del trattamento* deve procedere al trattamento dei dati personali in presenza delle misure richieste ai sensi dell'art. 32 (Sicurezza del trattamento) del RGPD. Le misure di sicurezza adottate sono quelle dichiarate nel Registro dei trattamenti relative al servizio. Il *Titolare* prende atto che in alcuni casi il *Responsabile del trattamento*, procederà al trattamento attraverso gli strumenti predisposti e configurati dallo stesso e pertanto dovrà adottare ogni cautela necessaria solo qualora il trattamento sia effettuato fuori dal controllo dello strumento impostato e configurato dal *Titolare*.

   2) Se il *Responsabile del trattamento* ha aderito ad un codice di comportamento, o ha esibito una certificazione, deve operare in presenza delle misure di sicurezza previste dal codice di comportamento o dai protocolli di cui alla certificazione. In questo caso il *Titolare* accetterà la certificazione come prova del fatto che il *Responsabile del trattamento* ha adottato misure adeguate rispetto al trattamento effettuato. In questo caso il *Titolare* rinuncia ad effettuare attività di *audit* sui sistemi e sulle procedure del *Responsabile*.

   3) Il *Responsabile del trattamento*, per i casi contemplati all'art. 37 del RGPD, conformemente a detta disposizione opera avvalendosi del proprio Responsabile della

protezione dei dati (in seguito RPD) e comunica al *Titolare del trattamento* il nome e i dati del RPD designato.

4) In conformità dell'Art. 30 del RGPD ogni *Responsabile del trattamento* e, ove applicabile, il suo rappresentante, se non rientrante nei casi di esonero di cui al paragrafo 5 di tale articolo, devono tenere un registro di tutte le categorie di attività relative al trattamento svolte per conto del *Titolare del trattamento*, contenente quanto indicato nel comma 2 di detto articolo.

5) I registri indicati devono essere tenuti in forma scritta, anche in formato elettronico.

d) Nomina di altro Responsabile da parte del Responsabile del trattamento

1) La Provincia di Lodi può affidare il servizio di gestione dei servizi a terzi responsabili del trattamento in qualsiasi momento, previa comunicazione scritta al *Titolare*, il quale potrà opporsi entro 15 giorni dal ricevimento di tale comunicazione.

2) La Provincia di Lodi dichiara e garantisce che tali ulteriori responsabili presentano garanzie sufficienti per mettere in atto misure tecniche e organizzative idonee a garantire il rispetto delle disposizioni della vigente normativa sulla privacy e si impegna a vincolare contrattualmente gli ulteriori responsabili al rispetto degli stessi obblighi in materia di protezione dei dati personali assunti dal *Responsabile* nei confronti del *Titolare*.

3) Spetta al *Responsabile del trattamento* iniziale assicurare che l'ulteriore *Responsabile del trattamento* presenti le stesse garanzie sufficienti alla messa in opera di misure tecniche ed organizzative appropriate di modo che il trattamento risponda alle esigenze del regolamento europeo sulla protezione dei dati.

4) Qualora l'ulteriore *Responsabile del trattamento* ometta di adempiere ai propri obblighi in materia di protezione dei dati, il *Responsabile* iniziale conserva, nei confronti del *Titolare del trattamento*, l'intera responsabilità dell'adempimento degli obblighi dell'ulteriore *Responsabile*.

e) Assistenza al Titolare per l'esercizio dei diritti degli interessati

1) Per quanto possibile, il *Responsabile del trattamento*, tenendo conto della natura del trattamento, deve assistere il *Titolare del trattamento* al fine dell'adempimento dell'obbligo del *Titolare del trattamento* di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al *Capo III (Diritti dell'interessato):* di far seguito alle domande di esercizio dei diritti di accesso, di rettifica, di cancellazione e di opposizione, alla limitazione del trattamento, a trasportare i dati, di non essere oggetto di una decisione individuale automatizzata (compreso il profilo).

2) Il *Responsabile del trattamento*, nella misura in cui ciò sia possibile, assisterà il *Titolare* con misure tecniche e organizzative adeguate.

Art. 5. In relazione al diritto di informazione degli interessati

1. Spetta al *Titolare del trattamento* fornire l'informativa di cui agli art. 13-14 alle persone interessate per le operazioni del trattamento al momento della raccolta dei dati.

2. Il *Responsabile del trattamento*, tenendo conto della natura del trattamento e delle informazioni a disposizione del *Responsabile del trattamento*, deve assistere il *Titolare del trattamento* nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del *RGPD*, vale a dire:
   - l'articolo 32. *Sicurezza del trattamento*;
   - l'articolo 33. *Notifica di una violazione dei dati personali all'autorità di controllo*;
   - l'articolo 34. *Comunicazione di una violazione dei dati personali all'interessato*;
   - l'articolo 35. *Valutazione d'impatto sulla protezione dei dati*;
   - l'articolo 36. *Consultazione preventiva*.

Art. 6. Assistenza per la "*Sicurezza del trattamento*"

1. Il *Responsabile del trattamento* ha l'obbligo di assistere il *Titolare del trattamento* nella realizzazione della *Sicurezza del trattamento*, conformemente all'articolo 32 del RGPD.
2. Il *Responsabile del trattamento*, in caso di situazioni anomale o di emergenze, provvederà a relazionare periodicamente sulle misure di sicurezza adottate – anche mediante eventuali questionari e liste di controllo - e ad informare immediatamente il *Titolare del trattamento.*

Art. 7. Particolari misure di sicurezza del *Responsabile del trattamento* già in atto

1. Il *Titolare del trattamento* prende atto che, per il servizio, il *Responsabile del trattamento* ha in essere misure di sicurezza adeguate in osservanza del RGPD.
2. Per i dati personali trattati nell'infrastruttura informatica del *Responsabile del trattamento* rimane comunque l'obbligo, per lo stesso, di caratterizzare il sistema di trattamento dati in conformità ai prerequisiti di sicurezza e, su richiesta del *Titolare del trattamento*, a servizio cessato, di cancellare i dati comunicati dal *Titolare del trattamento* per lo svolgimento del servizio; nel qual caso, il *Responsabile del trattamento* provvederà a cancellarli quando non siano più necessari per lo svolgimento del servizio o per gli atti conseguenti.
3. In particolare, per i servizi erogati dal Data center i dati saranno restituiti al *Titolare* sotto forma di backup e cancellati dal data Center entro 60 giorni dalla data di cessazione della Convenzione. Si precisa che i dati del *Titolare* comunque risiederanno per i 12 mesi successivi su supporti di backup che saranno sovrascritti al termine del periodo menzionato.
4. In relazione alle attività svolte dal *Responsabile del trattamento* riferite alla conservazione dei dati personali e alle attività sistemistiche dirette alla manutenzione della rete e all'aggiornamento dei relativi data base e sistemi operativi, gli operatori del *Responsabile del trattamento* avranno la funzione di *Amministratori di sistema*.
5. Gli adempimenti previsti dal Garante per la privacy nel provvedimento del 27 novembre 2008 saranno gestiti dal *Responsabile del trattamento*; in particolare, sarà il *Responsabile del trattamento* a valutare le caratteristiche soggettive degli amministratori di sistema, ad effettuare le designazioni individuali, a verificare le attività dagli stessi svolte ed a provvedere alla registrazione dei relativi accessi. In relazione a quanto previsto dal provvedimento stesso il *Responsabile del trattamento* si obbliga a comunicare al *Titolare del trattamento* l'elenco aggiornato degli Amministratori di sistema; la comunicazione di tali dati potrà avvenire in formato elettronico o cartaceo e il *Titolare* del trattamento considera evaso tale adempimento

anche con la semplice messa a disposizione dell'elenco aggiornato dei nominativi degli stessi Amministratori di sistema in un'area internet a ciò dedicata.

Art. 8. Assistenza in caso di violazione dei dati personali

1. Il *Responsabile del trattamento* ha l'obbligo di assistere il *Titolare del trattamento* nell'adempimento degli obblighi di "Notifica di una violazione dei dati personali all'autorità di controllo", conformemente all'articolo 33 del RGPD. Il *Responsabile del trattamento* notifica al *Titolare del trattamento* ogni violazione di dati a carattere personale nel tempo massimo di 24 ore dopo esserne venuto a conoscenza tramite PEC. Tale notifica è accompagnata da quanto espressamente indicato nel 3° comma dell'articolo 33, utile per permettere al *Titolare del trattamento*, se necessario, di notificare questa violazione all'autorità di controllo competente.
2. Il *Responsabile del trattamento* ha l'obbligo di assistere il *Titolare del trattamento* nell'adempimento degli obblighi di "*Comunicazione di una violazione dei dati personali all'interessato"*, conformemente all'articolo 34 del RGPD; tale comunicazione andrà comunque sempre fatta da parte del *Titolare del trattamento*.
3. Il *Responsabile del trattamento* assisterà il *Titolare del trattamento* nell'adempimento degli obblighi della "*Valutazione d'impatto sulla protezione dei dati"*, conformemente all'articolo 35 del RGPD, fornendo al *titolare* ogni informazione utile in suo possesso.

Art. 9. Assistenza in caso di controlli

1. Il *Responsabile del trattamento* assiste il *Titolare del trattamento* nella consultazione preventiva dell'autorità di controllo, prevista dall'articolo 36 del RGPD, fornendo al *titolare* ogni informazione utile in suo possesso.
2. Il *Responsabile del trattamento* metterà a disposizione del *Titolare del trattamento* tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 del RGPD e deve consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal *Titolare del trattamento* o da un altro soggetto da questi incaricato o dalle autorità. Qualora tali attività comportino un costo per il *Responsabile del trattamento*, tali attività andranno valutate a livello progettuale con la definizione di una valutazione economica.

Art. 10. Altri obblighi del *Responsabile del Trattamento*

1. I compiti del *Responsabile del trattamento* sono quelli indicati nella Convenzione che regola il servizio e qualificati quali obblighi o attività dovute dal *Responsabile*.
2. Qualora il *Responsabile del trattamento* ritenga a suo parere che un'istruzione del *Titolare del trattamento* violi il RGPD o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati dovrà informare immediatamente il *Titolare del trattamento*.
3. Nello svolgimento dell'incarico, il *Responsabile del trattamento* dovrà operare in osservanza dei principi di protezione dei dati a partire da quando questi vengono progettati (privacy by design) e della protezione dei dati di default (privacy by default).

Art. 11. Restituzione dei dati personali al termine della Convenzione

1. Dopo che è terminata la prestazione dei servizi relativi al trattamento, il *Responsabile del trattamento*, su scelta del *Titolare del trattamento*, dovrà restituire o cancellare tutti i dati personali e cancellare le copie esistenti.
2. I dati in possesso del *Responsabile del trattamento* dovranno essere restituiti al *Titolare del trattamento* attraverso la consegna del backup del data base o dei files su cui risiedono i dati personali; entro 90 gg dalla data di risoluzione della Convenzione, dovranno essere distrutti.
3. Alla cessazione del rapporto, eventuali ulteriori copie dei dati stessi di backup, salvo diversi accordi che potranno intervenire tra il *Titolare* e il *Responsabile* dovranno essere distrutte dal *Responsabile del trattamento* entro tempi compatibili con le ulteriori necessità che possono prospettarsi anche alla cessazione del servizio e comunque per un tempo non superiore a 12 mesi. Decorsi i 90 gg dalla data di cessazione suddetta e nel periodo intermedio tra la fine del rapporto e detto termine i dati saranno conservati dal *Responsabile del trattamento* per fini esclusivamente di sicurezza e non destinati alla comunicazione e alla diffusione.
4. In deroga a quanto indicato ai punti precedenti, il *Responsabile del trattamento* dovrà conservare detti dati, nel caso in cui il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati e dovrà conservarli fino al termine imposto da detta normativa o da detti provvedimenti.

Art. 12. Obblighi del *Titolare del trattamento* di fronte al *Responsabile del trattamento*

1. Il *Titolare del trattamento* deve:
   a. fornire al *Responsabile del trattamento* i dati previsti all'art. 3 delle presenti clausole;
   b. documentare per iscritto tutte le istruzioni riguardanti il trattamento dei dati da parte del *Responsabile del trattamento*;
   c. vigilare, in anticipo e durante la durata di tutto il trattamento, sul rispetto degli obblighi previsti dal regolamento europeo sulla protezione dei dati da parte del *Responsabile del trattamento*.

Art. 13. Luoghi ove sono e saranno custoditi i dati

1. Per i servizi comportanti il trattamento dei dati in banche dati create dal *Responsabile del trattamento* per il servizio, i dati personali saranno custoditi presso la sede del *Responsabile* e nel luogo o nei luoghi indicati nella Convenzione regolante il servizio e saranno ivi trattati e conservati. I servizi saranno erogati dall'Italia. Qualora ci fosse la necessità di erogare i servizi da territori Ue o Extra UE ne sarà data immediata notizia al *Titolare* che deciderà se continuare o risolvere la Convenzione.

Art. 14. Controlli

1. Il *Titolare del trattamento* si riserva, anche tramite verifiche periodiche, di vigilare sulla puntuale osservanza delle disposizioni di legge sul trattamento dei dati stessi e sul rispetto delle proprie istruzioni indicate nel presente documento. Il *Responsabile del trattamento* dovrà consentire al *Titolare del trattamento*, dandogli piena collaborazione, periodiche verifiche circa l'adeguatezza delle misure di sicurezza adottate e il rispetto della Normativa Privacy e delle disposizioni del *Titolare del trattamento* stesso.

2. Ogni attività di *audit* da parte del *Titolare* dovrà essere convenuta con il *Responsabile del trattamento*. Qualora tali attività comportino oneri e spese non previste dalla presente Convenzione, tutte le richieste del *Titolare* dovranno essere gestite a livello progettuale con una stima dei costi necessari per la loro attuazione (siano esse attività di *penetration test, vulnerability assessment*, altro).

IL PRESIDENTE
ing. arch. Nicola Buonsante

Documento informatico sottoscritto con firma digitale
(art. 24 del D.Lgs. n. 82/2005)