AREU
Sistema Socio Sanitario
Regione Lombardia

DELIBERA DEL DIRETTORE GENERALE

98 / 2021 del 23/03/2021

***Oggetto*: CONTRATTO DI NOMINA RESPONSABILE ESTERNO DEL TRATTAMENTO A FAVORE DI GPI S.P.A.**

Agenzia Regionale Emergenza Urgenza
Via a. Campanini 6, 20124 Milano \ CF e P. Iva 11513540960
T 02.67129001 - F 02.67129002 \ M protocollo@pec.areu.lombardia.it
www.areu.lombardia.it

OGGETTO: CONTRATTO DI NOMINA RESPONSABILE ESTERNO DEL TRATTAMENTO A FAVORE DI GPI S.P.A.

vista la seguente proposta di deliberazione n. 161/2021, avanzata dal Direttore della Struttura Complessa Affari Generali e Legali

IL DIRETTORE GENERALE

VISTI:

- il Regolamento (UE) 2016/679 del 27.04.2016 "Regolamento generale in materia di protezione dati personali";
- il D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali", come modificato dal D.Lgs. 101/2018 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);

CONSIDERATO che, ai sensi della citata normativa in materia di protezione dati personali, qualora un trattamento dati debba essere effettuato per conto del Titolare del trattamento, quest'ultimo, ai sensi dell'art. 28 del GDPR, deve nominare un Responsabile del trattamento che presenti garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale da soddisfare i requisiti previsti dal Regolamento stesso;

ATTESO CHE:

- con provvedimento deliberativo n. 90/2020, AREU ha aderito alla "Convenzione per il "Servizio di gestione informatizzata delle risorse umane in SaaS - Enti SSR - GPI - ARCA_2016_109", con conseguente predisposizione di ordinativo di fornitura per il servizio predetto e, successivamente, ha richiesto l'estensione del servizio con acquisizione del pacchetto platinum (delibera n. 315/2020) e con il pacchetto di correzione dei flussi inviati all'INPS ed eventuali squadrature (delibera n. 326/2020);
- GPI S.p.A. è, altresì, titolare della APP SIGMA I BADGE, finalizzata a consentire ai dipendenti di inserire le timbrature, in entrata e in uscita, registrando la posizione GPS senza vincolare la timbratura ad un terminale di rilevazione presenze, ma attraverso "timbratori virtuali" come individuati dall'Agenzia;
- con il predetto contratto, AREU ha assicurato la gestione dei servizi e degli adempimenti amministrativi connessi al rapporto di lavoro per i propri dipendenti e per il personale funzionalmente assegnato alla stessa per le attività di competenza come previste dalla LR 33/2009, successivamente modificata dalla LR 22/2019 con istituzione dell'Agenzia Regionale Emergenza Urgenza e attivazione di quest'ultima con DGR 2701/2019 e DGR 4078/2020;

CONSIDERATO CHE:

- AREU, nella propria qualità di datore di lavoro è Titolare del Trattamento per le operazioni che interessano i dati del proprio personale, con conseguente responsabilità di provvedere alla nomina del Responsabile Esterno del trattamento;

- l'esecuzione delle pratiche connesse alla gestione del rapporto di lavoro del personale AREU comporta il trattamento di dati personali e/o appartenenti a categorie particolari da parte di GPI S.p.A.;

PRESO ATTO che, in ottemperanza alla vigente normativa in materia di protezione dei dati personali GPI S.p.A., con sede legale a Trento in via Ragazzi del '99 n. 13, Codice Fiscale e P.Iva n. 01944260221 deve essere nominato Responsabile esterno del trattamento ai sensi dell'art. 28 Regolamento (UE) 2016/679;

DATO ATTO che la durata del contratto di nomina di Responsabile esterno del trattamento ha durata dalla data di sottoscrizione dei contratti per "Convenzione per il "Servizio di gestione informatizzata delle risorse umane in SaaS - Enti SSR - GPI - ARCA_2016_109"" e delle relative estensioni, aggiudicate, rispettivamente con delibera 90/2020, n. 315/2020 e n. 326/2020 e sino alla conclusione degli stessi;

DATO ATTO che dall'adozione del presente provvedimento non derivano oneri a carico del bilancio aziendale;

PRESO ATTO che il Proponente del procedimento attesta la completezza, la regolarità tecnica e la legittimità del presente provvedimento;

ACQUISITI i pareri favorevoli del Direttore Amministrativo e del Direttore Sanitario, resi per quanto di specifica competenza ai sensi dell'art. 3 del D.Lgs. n. 502/1992 e s.m.i.;

DELIBERA

Per tutti i motivi in premessa indicati e integralmente richiamati:

1. di approvare il testo del contratto di nomina di Responsabile esterno del trattamento dei dati connessi alla gestione informatizzata delle informazioni relative al personale dipendente, giuridiche-economiche-previdenziali, allegato al presente provvedimento quale parte integrante e sostanziale, ai sensi dell'art. 28 del Regolamento (UE) 2016/679 a favore di GPI S.p.A. e di autorizzarne la sottoscrizione;
2. di dare atto che dall'adozione del presente provvedimento non derivano oneri economici a carico del Bilancio aziendale;
3. di dare mandato alla SC Affari generali e legali di comunicare l'adozione del presente provvedimento alle competenti Strutture aziendali ed ai referenti GPI S.p.A. per la "Convenzione per il "Servizio di gestione informatizzata delle risorse umane in SaaS - Enti SSR - GPI - ARCA_2016_109" e per la APP SIGMA I BADGE
4. di dare atto che, ai sensi della L. n. 241/1990, responsabile del presente procedimento è la Dott.ssa Domenica De Giorgio, Dirigente della S.C. Affari Generali e Legali;
5. di disporre che vengano rispettate tutte le prescrizioni inerenti alla pubblicazione sul portale web aziendale di tutte le informazioni e i documenti richiesti e necessari ai sensi del D.Lgs. n. 33/2013 e s.m.i., c.d. Amministrazione Trasparente;
6. di disporre la pubblicazione del presente provvedimento all'Albo Pretorio on line dell'Agenzia, dando atto che lo stesso è immediatamente esecutivo (ex art. 32 comma 5 L. n. 69/2009 s.m.i. e art. 17 comma 6 L.R. n. 33/2009).

La presente delibera è sottoscritta digitalmente, ai sensi dell'art. 21 D.Lgs. n. 82/2005 e s.m.i., da:

Il Direttore Amministrativo Luca Filippo Maria Stucchi

Il Direttore Sanitario Giuseppe Maria Sechi

Il Direttore Generale Alberto Zoli

CONTRATTO DI TRATTAMENTO DEI DATI
NOMINA DEL RESPONSABILE DEL TRATTAMENTO

Il presente contratto (il "**Contratto**") è stipulato

t r a

AGENZIA REGIONALE EMRGENZA URGENZA DELLA LOMBARDIA (di seguito, per brevità, AREU) con sede legale in Milano (MI), Viale Monza n. 223, C.F./P.Iva 11513540960, in persona del legale rappresentante *pro tempore*, Direttore Generale, Dott. Alberto Zoli ("**Titolare del Trattamento**")

e

GPI S.p.A., con sede legale a Trento in via Ragazzi del '99 n. 13, Codice Fiscale e P.Iva n. 01944260221, n. di iscrizione al Registro delle Imprese di Trento 01944260221, nella persona del Procuratore Speciale, Oscar FRUET (il "**Responsabile del Trattamento**").

Congiuntamente definite "**Parti**",

Premesso che

(A) AREU è un'Azienda (ora Agenzia) Sanitaria attivata con DGR VIII/6994 del 02.04.2008, con il compito di promuovere l'evoluzione del sistema di emergenza e urgenza sanitaria territoriale, e, inoltre, di implementare e rendere omogeneo nel territorio della Regione, il soccorso sanitario di emergenza urgenza extraospedaliera (rif. LR 33/2009 come modificata dalla LR 23/2015 e dalla LR 22/2019 con costituzione dell'Agenzia Regionale Emergenza Urgenza e attivazione della stessa con DGR 2701/2019 e DGR 4078/2020);

(B) GPI S.p.A., Società che dal 1988 opera nel mercato della sanità;

(C) GPI S.p.A. è soggetto assegnatario della Convenzione per il "Servizio di gestione informatizzata delle risorse umane in SaaS - Enti SSR - GPI - ARCA_2016_109, cui AREU ha aderito con conseguente predisposizione di ordinativo di fornitura per il servizio predetto, come da provvedimenti deliberativi AREU n. 90/2020 (adesione), n. 315/2020 estensione del servizio platinum) e n. 326/2020 (estensione servizio correzione dei flussi inviati all'INPS ed eventuali squadrature).

(D) GPI S.p.A. è, altresì, titolare della APP SIGMA I BADGE, finalizzata a consentire ai dipendenti di inserire le timbrature, in entrata e in uscita, registrando la posizione GPS senza vincolare la timbratura ad un terminale di rilevazione presenze, ma attraverso "timbratori virtuali" come individuati dall'Agenzia;

(E) Nel contesto illustrato ed, ai sensi e per gli effetti dell'attuale normativa vigente in materia di protezione dei dati, AREU è "Titolare del Trattamento" ai sensi e per gli effetti dell'articolo 4.7 del Regolamento (UE) n. 679/2016 ("Regolamento Generale sulla protezione dei dati", di seguito, per brevità, "RGPD") in quanto determina le finalità e i mezzi del trattamento stesso di dati personali e particolari con cui GIP S.p.A., mediante

i propri dipendenti/collaboratori, viene in contatto in forza delle attività che la stessa deve svolgere in esecuzione del contratto di fornitura sottoscritto con AREU;

(F) AREU intende incaricare GPI spa dello svolgimento di talune attività di raccolta/trasmissione e registrazione che implicano il trattamento di dati personali - e nominarla "Responsabile del Trattamento" ai sensi e per gli effetti dell'articolo 28 del RGPD;

(G) GPI S.p.A. dichiara di avere competenze e conoscenze tecniche in relazione alle finalità e modalità del trattamento ai sensi del Codice Privacy e del RGPD, alle relative misure di sicurezza da adottare a garanzia della riservatezza, completezza ed integrità dei dati personali;

(H) il presente Contratto è stipulato per garantire le opportune salvaguardie per la protezione della riservatezza e della sicurezza dei dati personali trasmessi dal Titolare del Trattamento al Responsabile del Trattamento (o appresi dal Responsabile del Trattamento durante lo svolgimento delle attività *sub* (C) dell'Allegato 1) al presente contratto) per essere trattati, previa autorizzazione del Titolare del Trattamento;

(I) il Responsabile della protezione dei dati del Titolare del Trattamento è contattabile ai seguenti recapiti:

- e-mail: dpo@areu.lombardia.it
- raccomandata A/R: alla c.a. Responsabile Protezione dati personali AREU, presso la sede operativa AREU sita in Via Alfredo Campanini 6, 20124 Milano (MI)

Il Responsabile della protezione dei dati del Responsabile del Trattamento è contattabile ai seguenti recapiti:

- email dpo@gpi.it.

Tutto ciò premesso, le Parti convengono quanto segue

PREMESSE

Le premesse costituiscono parte integrante e sostanziale del presente contratto.

DEFINIZIONI

Nel presente Contratto, salvo diversa esigenza richiesta dal contesto, le espressioni seguenti avranno i significati qui indicati:

"Allegato":	indica un allegato al Contratto, di cui costituisce parte integrante;
"Addetto Autorizzato al Trattamento":	si riferisce a chiunque agisca sotto l'autorità del Titolare del Trattamento o del

	Responsabile del Trattamento e che abbia accesso a dati personali (Art. 29 RGPD);
"Istruzioni":	si riferiscono alle istruzioni che sono o saranno impartite dal Titolare al Trattamento al Responsabile del Trattamento per il Trattamento (Art. 28 RGPD);
"Violazione dei Dati Personali":	indica una violazione della sicurezza che causi accidentalmente o illecitamente la distruzione, la perdita, l'alterazione, la divulgazione o l'apprendimento non autorizzati di dati personali trasmessi, archiviati o in qualsiasi modo elaborati.

Le espressioni "Titolare del Trattamento", "Responsabile del Trattamento", "*Sub* Responsabile", "Interessato", "Dati Personali" e "Trattamento" avranno il significato attribuito dal RGPD.

Salvo diversamente disposto, i riferimenti a premesse, allegati ed articoli si intendono alle premesse, agli allegati e agli articoli del Contratto e negli allegati, salvo diversamente specificato, i riferimenti a paragrafi si intendono ai paragrafi di quegli stessi allegati.

Nel Contratto i riferimenti a statuti, disposizioni di legge o leggi si intendono come riferimenti agli statuti, articoli alle disposizioni di legge o alle leggi come di volta in volta modificati, prorogati o promulgati. Salvo diversamente disposto, ogni riferimento alle espressioni "per iscritto" o "scritto" comprenderà i fax e tutte le forme tangibili di riproduzione visibile delle parole (quali a mero titolo esemplificato: e-mail, posta elettronica certificata etc.).

OGGETTO E AMBITO APPLICAZIONE DEL PRESENTE CONTRATTO

L'oggetto, le modalità e la finalità, nonché le categorie dei Dati Personali e gli Interessati, sono descritti nell'Allegato 1 ("*Descrizione del Trattamento*") qui accluso.

In relazione ai Servizi, il presente Contratto si applicherà **a tutti i Dati Personali e particolari/sensibili** che il Titolare del trattamento:

- Invia, in proprio, o per suo conto, al Responsabile del Trattamento per il Trattamento;
- Appresi dal Responsabile del trattamento durante lo svolgimento della propria attività, per essere trattati, previa autorizzazione del Titolare del Trattamento;
- comunque pervenuti al Responsabile del Trattamento, per conto del Titolare del Trattamento, per essere Trattati.

TRATTAMENTO DEI DATI

In adempimento dell'articolo 2 che precede, il Responsabile del Trattamento si impegna a trattare i Dati Personali oggetto del presente Contratto attenendosi ai termini e alle condizioni ivi inclusi; in particolare, il Responsabile del **Trattamento dichiara e garantisce**:

a) di Trattare i Dati Personali esclusivamente per conto del Titolare del Trattamento, attenendosi sempre alle Istruzioni impartite dal Titolare del Trattamento nell'ambito del presente Contratto, nonché a tutte le leggi vigenti di protezione dei dati personali e unicamente ai fini (attinenti alla prestazione dei Servizi da parte del Responsabile del Trattamento) e con le modalità indicate, di volta in volta e per iscritto, dal Titolare del Trattamento e per nessun'altra finalità e in nessun altro modo, salvo che con il preventivo ed espresso consenso scritto del Titolare del Trattamento. Le Istruzioni impartite verbalmente dovranno essere immediatamente confermate per iscritto. Se per qualsiasi motivo il Responsabile del Trattamento non potrà ottemperare a questa disposizione, lo stesso si impegna a informare immediatamente il Titolare del Trattamento circa tale impossibilità. Qualora il Responsabile del Trattamento ritenga che attenendosi alle Istruzioni dei Titolare del Trattamento violerebbe una legge vigente sulla protezione dei dati, il Responsabile del Trattamento dovrà comunicarlo senza indugio e per iscritto al Titolare del Trattamento;

b) che nella propria area di responsabilità, articolerà la propria organizzazione aziendale interna in modo da garantire il rispetto degli obblighi specifici di protezione dei Dati Personali così come previsti dall'articolo 32 del RGPD. Il Responsabile del Trattamento adotterà i provvedimenti tecnici e organizzativi necessari al fine di proteggere adeguatamente i Dati Personali trasferiti dal Titolare del Trattamento contro usi impropri e perdite, come stabilito dalla legge vigente in materia di protezione dei dati. L'Allegato 2 ("*Descrizione dei Provvedimenti Tecnici e Organizzativi*") qui accluso contiene una descrizione generale di tali provvedimenti tecnici e organizzativi. Il Responsabile del Trattamento vigila costantemente sul rispetto di questi provvedimenti e, se del caso, si prodigherà nell'aggiornamento/adeguamento degli stessi e ne darà pronta comunicazione al Titolare del Trattamento;

c) che assisterà il Titolare del Trattamento con misure tecniche e organizzative adeguate per soddisfare l'obbligo del Titolare del Trattamento di dare seguito alle richieste che potranno essergli avanzate dagli Interessati per l'esercizio del propri diritti ai sensi del capo III ("*Diritti dell'interessato*") del RGPD;

d) che assisterà il Titolare del Trattamento nel rispetto degli obblighi di cui agli articoli nn. 32 ("*Sicurezza del trattamento*"), 33 ("*Notifica di una violazione dei dati personali all'autorità di controllo*") 34 ("*Comunicazione di una violazione de dati personali all'interessato*)" 35 ("*Valutazione d'impatto sulla protezione dei dati*") e 36 ("*Consultazione preventiva*") del RGPD, tenendo conto della natura del trattamento e delle informazioni a sua disposizione;

e) che ciascuno dei suoi dipendenti/collaboratori/professionisti è informato degli obblighi di cui al presente Contratto relativamente alla sicurezza e alla protezione dei Dati Personali;

f) di assicurare che ciascuno dei propri Addetti Autorizzati al Trattamento (cfr. articolo 7 che segue) e Sub Responsabili (cfr. articolo 8 che segue), che sono o che verranno a conoscenza dei Dati Personali, si impegni(no) a mantenerne la riservatezza o vi sia(no) già vincolato(i) da un'opportuna e specifica disposizione di legge. L'obbligo di mantenere la segretezza dei Dati Personali resterà in vigore anche dopo la

risoluzione dei rispettivi rapporti di lavoro o professionali;

g) di non divulgare i Dati Personali direttamente o indirettamente a persone, aziende, società o altri soggetti senza l'esplicito consenso scritto del Titolare del Trattamento, eccettuati quei dipendenti incaricati al Trattamento, Addetti Autorizzati al Trattamento e Sub Responsabili e vincolati dagli obblighi descritti negli articoli 3.5 o 3.6, salvo diversa disposizione di legge o di regolamento;

h) di avvertire, senza ingiustificato ritardo, il Titolare del Trattamento inviando una comunicazione ai seguenti recapiti: dpo@areu.lombardia.it e affari.generalilegali@areu.lombardia.it delle seguenti circostanze:

- richieste giuridicamente vincolanti di comunicazione dei Dati Personali inviate da un'autorità giudiziaria, salvo qualora la comunicazione sia vietata, ad esempio, da norme di diritto penale per salvaguardare il segreto di indagini giudiziarie;

- violazioni di leggi vigenti per la protezione dei dati o del presente Contratto, commesse dal Responsabile del Trattamento o da suoi dipendenti durante il Trattamento dei Dati Personali soggetti al trattamento del Titolare del Trattamento;

- una Violazione dei Dati Personali. Tale notifica dovrà avvenire tempestivamente e non altre 24 ore da quando si è venuti a conoscenza dall'avvenimento; la stessa dovrà specificare, tenuto conto della natura del Trattamento e delle informazioni a disposizione del Responsabile del Trattamento, qualsiasi informazione utile al fine di agevolare il Titolare del Trattamento nel rispetto degli obblighi di comunicazione stabiliti dalla legge vigente. Qualora non fosse possibile comunicare contemporaneamente tutte le informazioni pertinenti, il Responsabile del Trattamento potrà inviarle a scaglioni, ma senza ingiustificati ritardi;

- tutte le richieste pervenute direttamente dagli Interessati e rimaste senza risposta, salvo autorizzazione scritta del Titolare del Trattamento in tal senso;

Nel caso di mancata comunicazione, il Responsabile del trattamento risponde e tiene indenne il Titolare del trattamento dalle eventuali conseguenze che, sul piano civile, penale e amministrativo potranno derivare dalla mancata notifica all'Autorità Garante ed all'interessato e quindi dalla mancata tempestiva gestione della violazione e delle sue conseguenze;

i) tenuto conto della natura del Trattamento, di collaborare con il Titolare del Trattamento attuando per quanto possibile gli opportuni provvedimenti tecnici ed organizzativi per l'adempimento dell'obbligo del Titolare del Trattamento di rispondere alle richieste di esercitare i diritti conferiti agli Interessati dalla legge vigente;

j) di mettere a disposizione del Titolare del Trattamento tutte le informazioni necessarie per dimostrare l'adempimento degli obblighi previsti dal presente Contratto e consentire, contribuendovi, i controlli, tra cui ispezioni, eseguiti dal Titolare del Trattamento o da un altro revisore incaricato dal Titolare del Trattamento, come descritto nell'articolo 6 che segue;

k) che tutti i Trattamenti effettuati da un *Sub* Responsabile saranno eseguiti conformemente all'articolo "Nomina dei sub-responsabili" che segue;

l) che, ove ciò sia richiesto dalla legge vigente, il Responsabile del Trattamento ha nominato un addetto alla protezione dei dati ("**DPO**"). Il Responsabile del Trattamento comunicherà al Titolare del Trattamento i dettagli di contatto della persona nominata quale DPO;

m) di collaborare con il Titolare del Trattamento per garantire l'adempimento dell'obbligo di eseguire stime dell'impatto sulla protezione dei dati e di consultarsi con le autorità di vigilanza, tenendo conto della natura del Trattamento e delle informazioni a disposizione del Responsabile del Trattamento.

n) su scelta del Titolare del Trattamento, di cancellare o restituire tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e di cancellare le copie esistenti, salvo che il Diritto dell'Unione o della normativa vigente preveda la conservazione dei dati;

o) Il Responsabile del trattamento si obbliga a tenere manlevato ed indenne il Titolare da ogni responsabilità e/o danno, anche nei confronti di terzi, nonché degli Interessati al trattamento, per azioni ed omissioni, inadempimenti di qualunque natura, imputabili allo stesso Responsabile, ai soggetti/operatori da esso autorizzati e dai Sub Responsabili. Tale responsabilità in materia di protezione dei dati personali e di cui agli artt. 28 c.10, 82, 83 e 84 del Regolamento Ue 2016/679, che si richiamano espressamente, rientra nel quadro della responsabilità contrattuale derivante dalla sottoscrizione del contratto di fornitura del servizio in oggetto e del presente atto di nomina.

OBBLIGHI DEL TITOLARE DEL TRATTAMENTO DATI

Il Titolare del Trattamento garantisce che (i) i Dati Personali che sono stati o saranno comunicati al Responsabile del Trattamento sono stati raccolti in conformità alla legge applicabile e (ii) che le comunicazioni di Dati Personali al Responsabile del Trattamento sono state o saranno eseguite in conformità alle disposizioni di legge applicabili e, se del caso, anche autorizzate dai relativi Interessati.

DURATA

Il presente atto di nomina a Responsabile del trattamento ha durata pari a quella del contratto di fornitura del "Servizio di gestione informatizzata delle risorse umane in SaaS - Enti SSR - GPI - ARCA_2016_109", come da Delibere AREU n. 92/2020 (60 mesi iniziali prorogabili di ulteriori 24 mesi), n. 315/2020 (estensione servizio platinum) e n. 326/2020 (Estensione servizio correzione flussi INPS ed eventuali squadrature), nonché del tempo di utilizzo dell'applicazione SIGMA I BADGE da parte del personale dipendente, comandato, distaccato e qualsiasi altro titolo presente in AREU.

RISOLUZIONE

Il presente Contratto dovrà intendersi risolto automaticamente e di diritto alla data in cui il Titolare del Trattamento revocherà la nomina al Responsabile del Trattamento e, pertanto, quest'ultimo sarà sciolto dagli obblighi relativi ai Servizi.
Il presente contratto dovrà intendersi risolto anche in caso di contestazione di inadempienze contrattuali che portino alla risoluzione del contratto principale in essere tra le parti.
In ogni caso, l'obbligo di mantenere la segretezza dei Dati Personali resterà in vigore in capo al Responsabile del Trattamento anche dopo la risoluzione del presente Contratto.
Immediatamente dopo la risoluzione del presente Contratto, il Responsabile del Trattamento dovrà consegnare al Titolare del Trattamento tutti i Dati Personali di quest'ultimi in proprio possesso oppure distruggerli, a scelta dei Titolari del Trattamento.
Su richiesta del Titolare del Trattamento, il Responsabile del Trattamento dovrà confermare per iscritto di avere adempiuto a tali obblighi e di aver cancellato tutte le copie esistenti, salvo qualora la conservazione dei Dati Personali sia imposta dalla legge vigente.

CONTROLLI E RICHIESTE DI INFORMAZIONI

Il Titolare del Trattamento potrà, durante il normale orario di lavoro, senza ragionevolmente interferire con le attività aziendali/professionali del Responsabile del Trattamento, e dopo averne dato ragionevole preavviso, svolgere direttamente i controlli presso il Responsabile del Trattamento o affidare tali controlli a un *auditor* esterno, che sarà soggetto agli stessi obblighi di riservatezza.
Prima dell'inizio dei controlli nel sito, il Titolare del Trattamento e il Responsabile del Trattamento concorderanno l'ambito, gli orari e la durata dei controlli. Se ne riceverà richiesta, il Responsabile del Trattamento dovrà comunicare in tempi ragionevoli al Titolare del Trattamento tutte le informazioni necessarie per eseguire il controllo dei Trattamenti.
Il Responsabile del Trattamento informerà il Titolare del Trattamento circa le relative richieste di informazioni. Il quale deciderò in merito alle predette istanze.
L'evasione delle richieste di informazioni poste in ottemperanza delle normative vigenti e non ridondanti, pervenute al Responsabile del trattamento, non comporta oneri economici per il Titolare del trattamento.

NOMINA DEGLI ADDETTI AUTORIZZATI AL TRATTAMENTO

Ai sensi e per gli effetti dell'art. 29 RGPD, con il presente Contratto il Titolare del Trattamento autorizza il Responsabile del Trattamento ad avvalersi, tramite designazione formale, di propri Addetti Autorizzati al Trattamento per l'esecuzione dei Servizi e le finalità del Contratto.
La nomina degli Addetti Autorizzati da parte del Responsabile del Trattamento *sub* 7.1. dovrà:

(i) essere eseguita per iscritto;
(ii) indicare l'ambito di Trattamento consentito;
(iii) specificare le istruzioni del Trattamento che saranno impartite tenendo in considerazione i termini del presente Contratto nonché le Istruzioni.

Su richiesta del Titolare del Trattamento, il Responsabile del Trattamento metterà a disposizione del Titolare del Trattamento un elenco aggiornato degli Addetti Autorizzati al Trattamento per l'esecuzione dei Servizi.

Nessun Trattamento eseguito da un Addetto Autorizzato al Trattamento incaricato dal Responsabile del Trattamento libererà quest'ultimo dalle responsabilità legate agli obblighi impostigli dal presente Contratto e/o dalla legge, ma sarà da considerarsi interamente responsabile del lavoro e dell'operato svolto da ciascun proprio Addetto Autorizzato al Trattamento.

NOMINA DEI *SUB* RESPONSABILI [Inserire a seconda del caso]

La nomina di soggetti sub Responsabili del trattamento ad opera del Responsabile del trattamento è possibile soltanto previa comunicazione ed espressione di parare favorevole alla stessa rilasciato dal Titolare del trattamento.

Su richiesta del Titolare del Trattamento, il Responsabile del Trattamento metterà a disposizione del Titolare del Trattamento un elenco aggiornato dei *Sub* Responsabili ai fini della prestazione dei Servizi.
Il Titolare del Trattamento potrà esercitare il diritto di obiettare l'utilizzo di un nuovo *Sub* Responsabile da parte del Responsabile del Trattamento avvisandone tempestivamente e per iscritto il Responsabile del Trattamento entro dieci (10) giorni lavorativi dalla ricezione della comunicazione del Responsabile del Trattamento.
Tutti i Trattamenti eseguiti da un *Sub* Responsabile dovranno esser condotti secondo i termini e condizioni inclusi in uno specifico contratto scritto concluso tra le parti che non sia meno restrittivo del presente Contratto. Nessun Trattamento eseguito da un *Sub* Responsabile libererà il Responsabile del Trattamento dalle responsabilità legate agli obblighi impostigli dal presente Contratto ma sarà da considerarsi interamente responsabile del lavoro e dell'operato svolto da ciascun suo *Sub* Responsabile.

DISPOSIZIONI VARIE

Le variazioni del, o le integrazioni al, presente Contratto saranno valide esclusivamente se stipulate per iscritto.

L'eventuale invalidità originaria o sopravvenuta di una clausola del presente Contratto non influirà sulla validità delle altre clausole. In tale caso le Parti saranno tenute a collaborare ai fini della redazione di altre clausole che esprimano un risultato giuridicamente valido e commercialmente il più simile possibile a quello della clausola invalida. Si applicherà la suddetta regola anche per colmare eventuali lacune del Contratto.

Tutti gli obblighi imposti al Responsabile del Trattamento da disposizioni di legge o da decisioni delle autorità giudiziarie o di vigilanza non saranno modificati dal presente Contratto.

Il presente Contratto è regolato dalla legge italiana e il Tribunale di Milano avrà la competenza esclusiva per dirimere qualsivoglia controversia dovesse insorgere tra le Parti in relazione all'esecuzione del Contratto.

La presente designazione non comporta alcun diritto per il Responsabile ad uno specifico compenso o indennità o rimborso per l'attività svolta.

Per tutto quanto non previsto dal presente atto di designazione si rinvia alle disposizioni generali vigenti ed applicabili in materia di protezione dei dati personali.

* * *

Si accludono i seguenti documenti:

- Allegato 1 "*Descrizione del Trattamento*"
- Allegato 2 "*Descrizione dei Provvedimenti Tecnici e Organizzativi*"

Milano data e luogo della sottoscrizione digitale

Per AGENZIA REGIONALE EMERGENZA URGENZA DELLA LOMBARDIA
Titolare del Trattamento
Legale Rappresentante p.t, Direttore Generale, Dott. Alberto Zoli

Per GIP S.P.A.
Responsabile del Trattamento
Procuratore Speciale p.t, _____

Allegato 1

Descrizione del Trattamento

A. **Oggetto (**Oggetto del Trattamento**) e base giuridica del Trattamento**

Il presente contratto ha ad oggetto il trattamento dei dati personali del personale dipendente, comandato, distaccato e qualsiasi altro titolo presente in AREU, determinato dallo svolgimento delle attività previste dal contratto per la fornitura del servizio Servizio di gestione informatizzata delle risorse umane in SaaS - Enti SSR - GPI - ARCA_2016_109", come da come da Delibere AREU n. 92/2020 (60 mesi iniziali prorogabili di ulteriori 24 mesi), n. 315/2020 (estensione servizio platinum) e n. 326/2020 (Estensione servizio correzione flussi INPS ed eventuali squadrature), nonché dei dati personali dei predetti interessati derivati dall'utilizzo da parte degli stessi dell'applicazione SIGMA I BADGE di GPI S.p.A..

B. Durata

Il Responsabile del trattamento può compiere le operazioni di trattamento nel periodo di validità del predetto contratto.

Si precisa che tale nomina avrà validità per il tempo necessario ad eseguire le operazioni affidate dal titolare e si considererà revocata a completamento dell'incarico affidato a GPI SPA, rimanendo gli obblighi di segretezza rispetto a tutti di dati trattati nel periodo di riferimento.

C. Categorie di interessati

Interessato al trattamento è il personale dipendente, comandato, distaccato e qualsiasi altro titolo presente in AREU;

D. Oggetto, Tipo e Finalità del Trattamento:

Oggetto del trattamento

A fronte delle attività svolte da GPI SPA, si evidenzia che, oggetto del trattamento saranno i seguenti dati:

- Nome e cognome;
- Codice fiscale;
- Residenza fiscale e domicilio se diverso dalla residenza;
- Recapito telefonico;
- Dati reddituali;
- Dato di geolocalizzazione;
- Dati appartenenti a categorie particolari di dati (es. dati relativi allo stato di salute, dati giudiziar, dati di appartenenza sindacale);
- Altri dati quali:
    - Informazioni relative alla assunzione
    - Informazioni relative alla qualifica
    - Informazioni relative alle aspettative

- Informazioni relative alle detrazioni fiscali
- Eredi
- Informazioni relative all'ANF
- Addizionali rateizzate
- Sedi lavoro / Organigramma
- Accantonamento TFR
- Storico cedolini
- Ulteriori dati economici personali (ad personam)
- Cessioni, riscatti assicurazioni
- File storico assenze
- Residui ferie
- Dati maternità e congedi parentali
- Abbinamenti badge dipendente
- Credito/debito orario iniziale
- Dati part-time verticale
- Dati part-time orizzontale

Le attività di trascodifica, richiedono invece la predisposizione di abbinamenti puntuali tra le informazioni storicamente gestite da AREU e le corrispondenti codifiche GPI riferite a:

- qualifiche contrattuali,
- tipologie di assunzione,
- motivi di dimissione,
- aspettative,
- discipline,
- voci retributive,
- codici di assenza

Tipologia del trattamento

I dati personali acquisiti da GIP S.p.A. nell'ambito dell'attività contrattualmente in essere con AREU, sono trattati mediante operazioni di raccolta (cartacea/informatizzata), raccolta, registrazione, utilizzo, elaborazione, estrazione, raffronto, consultazione, conservazione, comunicazione, cancellazione.

GIP S.p.A si serve di infrastrutture e sistemi forniti da Elemec Informatica SPA di Brunello-Varese. Le facility di infrastruttura Emelec sono composte da diversi Data Center, localizzati, rispettivamente, nelle località di Gazzada (VA) e Brunello (VA). Inoltre dispone di una facility localizzata a Sinziano (PV) per la gestione del Dister Recovery.

Finalità del trattamento

I dati personali sono trattati per le seguenti finalità:

a) Gestione delle codifiche a 2 caratteri nella sezione Programmazione;
b) Assegnazione attività giornaliere (turno, reperibilità, etichette, ecc.);
c) Estrazione dei dati di qualifica su fogli excel e report;

d) Nodo Assenze - Contatori di Copertura: gestione degli assenti per giorno e tipologia di assenza;
e) Gestione delle Note per giorno/dipendente,
f) Ordinamenti personalizzati dei contatori di copertura giornaliera;
g) Ordinamenti personalizzati dei dipendenti sul mese;
h) Gestione dei dipendenti per Gruppi di Qualifica;
i) Gestione del Turno da ambiente timbrature;
j) Gestione della "Stimbratura";
k) Modalità di Visualizzazione "zoom";
l) Visualizzazione e report con Fasce Orarie in alternativa alle codifiche (orari e reperibilità);
m) Funzioni di copia e incolla su Etichette, Orario di Servizio e Reperibilità;
n) Filtri su codifiche per verifica Coperture del servizio;
o) Gestione dipendenti aggiuntivi;
p) Storicizzazione della Programmazione: Funzione di Archiviazione;
q) Funzioni avanzate di ricerca;
r) Prospetti timbrature per reparto: report ed estrazione file excel;
s) Reportistica ed estrazione saldi orari (programmato e progressivi mensili);
t) Adeguamento dei dati dell'attuale applicativo utilizzato in AREU ai tracciati record previsti dalla convenzione ARIA; l'export dei dati sarà effettuato dai Sistemi Informativi AREU e GPI, disponendo delle necessarie competenze, predisporrà il suddetto tracciato;
U) Attività di transcodifica, che richiedono la predisposizione di abbinamenti puntuali tra le informazioni gestite dell'attuale applicativo e le corrispondenti codifiche GPI";
V) Attività di gestione dei cartellini previste dal sistema platinum
- ✓ permettere a responsabili e coordinatori di:
  - produrre, in formato pdf, il cartellino di uno o più mesi preselezionati riferiti a ciascuno dei propri collaboratori;
  - visualizzare l'elenco delle timbrature, i giustificativi di presenza e assenza, il saldo ferie e permessi, il saldo ore - credito e debito orario dei propri collaboratori al fine di un adeguato governo delle risorse umane assegnate;
- ✓ permettere ai dipendenti di:
  - annullare le timbrature doppie/errate;
  - invertire il verso entrata/uscita delle timbrature;
  - visualizzare per singoli giustificativi di presenza/assenza le disponibilità residue;
  - visualizzare la pianificazione delle ferie;

Z) Servizio di assistenza dedicato alla correzione dei flussi DMA trasmessi all'INPS e riconciliazione di squadrature (ECA) tra versamenti e denunce inviate;

E. Periodo di conservazione dei dati

I dati personali vengono trattati per il tempo necessario per adempiere alle finalità di cui sopra e, comunque, conservati secondo le indicazioni contenute nel Massimario di Scarto della Regione Lombardia (Rev. 03, punto 1.4.13, Risorse Umane).

Per quanto attiene i dati trattati mediante l'utilizzo della APP SIGMA IBADGE, si precisa che tutte le attività riguardanti la gestione dell'applicazione sono registrate in apposito file di log conservato per almeno 24 mesi, messo a disposizione di AREU qualora richiesto; la conservazione avviene per 6 mesi on line e per 24 mesi off line. La conservazione dei dati è la stessa delle timbrature ordinarie.

F. Categorie di destinatari dei dati

I dati vengono comunicati al personale di AREU preposto alla gestione delle pratiche amministrative legate ai rapporti di lavoro instaurati dall'Agenzia, al personale di ASST GRANDE OSPEDALE METROPOLITANO NIGUARDA in forza della convenzione per l'acquisizione di supporto giuridico-amministrativo-economico del personale dipendente, comandato, distaccato e qualsiasi altro titolo presente in AREU.

I dati saranno, altresì, comunicati a soggetti legittimati e secondo le modalità di evasione delle istanze di accesso agli atti definite di concerto con AREU, nonché agli Organismi di vigilanza, Autorità giudiziarie nonché a tutti gli altri soggetti ai quali la comunicazione sia obbligatoria per legge per l'espletamento delle finalità dette e per i casi di ricezione di comunicazioni di dati personali al di fuori dell'ambito di una specifica indagine (cfr. art. 4 GDPR "destinatari" e (C31) GDPR).

G. Trasferimento dei dati

La gestione e la conservazione dei dati personali avverrà su server, ubicati all'interno dell'Unione Europea, appartenenti al Titolare e/o di società terze incaricate e debitamente nominate quali Responsabili del trattamento. Resta inteso, in ogni caso, che il Titolare, ove si rendesse necessario, avrà facoltà di spostare l'ubicazione dei server in Italia e/o Unione Europea e/o Paesi extra-UE. In tal caso, il Titolare assicura sin d'ora che il trasferimento dei dati extra-UE avverrà in conformità alle disposizioni di legge applicabili stipulando, se necessario, accordi che garantiscano un livello di protezione adeguato e/o adottando le clausole contrattuali standard previste dalla Commissione Europea.

H. Divieti di trattamento.

In nessun caso il Responsabile del trattamento o il personale da questo autorizzato al trattamento dei dati conferiti dal Titolare del Trattamento può comunicare a soggetti terzi estranei al rapporto contrattuale di fornitura del servizio di gestione informatizzata delle risorse umane in SaaS - Enti SSR - GPI - ARCA_2016_109, con le estensioni platinum e correzione dei flussi inviati all'INPS ed eventuali squadrature e dalla messa a disposizione della APP SIGMA I BADGE, i dati personali e/o particolari/sensibili appresi e trattati nell'ambito dell'esecuzione del rapporto stesso né può in alcun modo ed in qualunque forma diffondere gli stessi.

Ogni violazione alla normativa vigente verrà prontamente segnalata all'autorità competente.

Allegato 2

Descrizione dei Provvedimenti Tecnici e Organizzativi adottati da GPI SPA anche per la APP SIGMA I BADGE

Vedasi documento "Privacy e protezione dati personali" redatto da G.P.I. S.p.A. che segue

PRIVACY E PROTEZIONE DI DATI PERSONALI

Tale documento ha il preciso scopo di descrivere come vengono protetti i dati personali e le relative risorse informatiche comprese le misure di sicurezza adeguate al rischio dirette a respingere tutte le eventuali minacce o intrusioni di terzi.

1. GPI si impegna ad adottare quanto previsto dalla normativa in materia di Protezione dei dati personali, più nello specifico: D. Lgs. 196 del 2003 novellato dal D. Lgs. 101 del 2018; Regolamento (UE) 2016/679 (di seguito indicato anche come "GDPR"); oltre a quanto previsto dalla normativa ISO/IEC 27001 e dalle Linee Guida ISO/IEC 27017 e 27018.
2. GPI si impegna ad attuare le misure tecniche e organizzative adeguate al rischio ex art. 32 GDPR personalizzate per ogni servizio offerto.
3. GPI si impegna a predisporre le procedure in materia di gestione dei diritti degli interessati ai sensi degli artt. da 15 a 22 GDPR.
4. GPI si impegna a formalizzare in modo chiaro e specifico l'obbligo di non divulgazione e riservatezza di tutto il personale dipendente.
5. GPI si impegna ad autorizzare per mezzo dell'atto di nomina ed istruire tramite le istruzioni tutto il personale dipendente, ai sensi dell'art. 29 GDPR.
6. GPI si impegna a formare in materia di Protezione di dati personali tutto il personale dipendente ai sensi degli artt. 29 e 39 del GDPR.
7. GPI adotta una corretta politica di gestione delle postazioni interne all'azienda per ridurre la possibilità che le caratteristiche del software (sistemi operativi, applicazioni aziendali, software per ufficio, impostazioni) vengano sfruttate per danneggiare i dati personali. Per tutelare tale aspetto, GPI applica una serie di misure, come ad esempio: aggiornamento continuo di tutto il personale sulla normativa di riferimento, protezione fisica e degli accessi nei luoghi aziendali, lavoro su uno spazio di rete protetto, controlli di integrità, logging. Inoltre, GPI adotta misure volte a ridurre il rischio che le caratteristiche delle apparecchiature (server, postazioni fisse, portatili, periferiche, dispositivi di comunicazione, supporti rimovibili) siano utilizzate per danneggiare i dati personali, quali, ad esempio, l'inventario, la compartimentalizzazione, la ridondanza, i limiti per l'accesso.

8. GPI assicura la presenza di tutte le misure di sicurezza fisiche che hanno il preciso scopo di rafforzare la sicurezza dei locali che ospitano le infrastrutture IT e le apparecchiature di rete, come di seguito riportato (a titolo esemplificativo e non esaustivo):

I. l'accesso ai locali di GPI è controllato;
II. sono stati installati sistemi di allarme antintrusione che vengono controllati periodicamente;
III. sono stati installati rilevatori di fumo e strumenti antincendio che vengono controllati periodicamente;
IV. è garantita la sicurezza delle chiavi e dei codici di allarme che permettono l'accesso ai locali;
V. sono state separate le aree degli edifici di GPI in base ai rischi;
VI. è presente un elenco aggiornato delle persone o dei dipendenti specificamente autorizzati ad accedere a ciascuna area;
VII. sono state stabilite delle regole e dei metodi specifici per controllare l'accesso dei visitatori;
VIII. vengono protette fisicamente le apparecchiature IT tramite metodi specifici (sistema di prevenzione incendi dedicato, attrezzatura di sollevamento contro possibili alluvioni, alimentazione elettrica e/o ridondanza del condizionamento d'aria, ecc…).

9. GPI si è dotata di una assicurazione a copertura di eventuali danni da violazione o perdita di dati.

10. GPI consente al Titolare del trattamento di poter stabilire, contrattualmente, il periodo di data retention al termine del quale i dati verranno cancellati, anonimizzati o pseudonimizzati. Il Titolare del trattamento potrà scegliere:

I. in caso di Cancellazione: prima di attivare la cancellazione GPI ha la possibilità di attivare un warning per evitare che ci siano cancellazioni accidentali. Inoltre, il Titolare del trattamento ha la possibilità di programmare la cancellazione di dati impostando la scadenza.
II. in caso di Anonimizzazione: nel momento in cui i dati non devono più essere conservati, GPI permette al Titolare del trattamento (in alternativa alla cancellazione), di poterli rendere anonimi eliminando gli identificativi in modo irrecuperabile ed in modo che non siano più collegabili ad altri elementi di identificazione.
III. in caso di Pseudonimizzazione: i dati personali trattati non potranno più essere attribuiti ad un interessato specifico senza l'utilizzo di informazioni aggiuntive. Tali informazioni aggiuntive, inoltre, devono essere conservate separatamente e soggette a misure tecniche e organizzative tali da garantire che i dati personali non siano attribuiti ad una persona fisica identificata o identificabile.

11. GPI ha nominato un Responsabile della protezione dei dati personali (RDP/DPO) in conformità con quanto previsto dalla vigente normativa in materia di Privacy e Protezione dei dati personali. Tale figura può essere contattata al seguente indirizzo e-mail: dpo@gpi.it.

12. GPI rispetta le Linee Guida AGID per lo sviluppo del software sicuro e del Garante per la Protezione dei dati personali, garantendo quindi la conformità alle best practice.

13. Se previsto da contratto, GPI effettua i vulnerability assessment (VA) ed i penetration test (PT), i quali saranno pianificati ed eseguiti almeno una volta l'anno.

14. GPI supporta il Titolare del trattamento ad effettuare le Valutazione d'impatto sulla protezione dei dati (DPIA) ai sensi dell'art. 35 GDPR e dell'ALLEGATO 1 AL PROVVEDIMENTO N. 467 DELL'11 OTTOBRE 2018, Pubblicato sulla Gazzetta Ufficiale n. 269 del 19 novembre 2018 denominato "Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto".

15. Se previsto da contratto, GPI si impegna ad adottare un sistema di Disaster Recovery, cioè un insieme di misure e di strutture, anche a livello organizzativo, che permettono agli apparati informatici di superare situazioni di emergenza, ovvero di impedire che imprevisti accidentali o incidenti possano compromettere il funzionamento delle strutture. Il Disaster Recovery attiene alla capacità di "recuperare" dati e funzionalità operative in presenza di "disastri".

16. GPI consente di poter utilizzare il servizio "accesso da remoto", in occasione del quale il Titolare del trattamento potrà attivare o disattivare la possibilità che un operatore remoto possa prendere il controllo della macchina locale per finalità di assistenza e intervento esplicito. Tale trattamento di dati, come gli altri offerti da GPI, rispetterà i principi di correttezza, trasparenza e liceità.

17. GPI si impegna, dove contrattualizzato, ad attuare delle misure specifiche che possano rilevare i malware, tramite il monitoraggio costante delle vulnerabilità.

18. GPI si impegna ad attuare un'adeguata politica di gestione di eventuali incidenti di sicurezza e violazioni dei dati personali, gestendo eventi che potrebbero influire sulle libertà e sulla riservatezza degli interessati. GPI adotta una procedura operativa per rilevare e gestire eventuali eventi di personal data breach.

19. GPI possiede un adeguato sistema di tracciabilità, per rilevare tempestivamente incidenti relativi a dati personali e disporre di elementi utilizzabili per studiarli o per fornire prove nel contesto di indagini. Infatti, GPI adotta una politica di registrazione degli eventi di data breach.

20. GPI rispetta il principio di tracciabilità dell'attività, infatti, vengono registrati gli accessi logici all'interno dell'azienda.

21. GPI rispetta i principi di Privacy by design e by default ex art. 25 GDPR, infatti nei servizi offerti che prevedono il trattamento di dati personali, vengono considerati ab origine i requisiti di conformità al GDPR e vengono mantenuti fino alla loro cessazione. Resta in ogni caso inteso che il Titolare del trattamento si impegna a mantenere le Patch dei servizi offerti aggiornate.

22. Se previsto da contratto, GPI dà la possibilità al Titolare del trattamento di scegliere l'infrastruttura dove attivare il proprio servizio nel network di Data Center GPI in Italia ed Europa.

23. Ove previsto dal contratto, si prevede un'adeguata procedura di Backup, per assicurare la disponibilità e/o l'integrità dei dati personali e contro il rischio di perdita accidentale dei dati personali ex art. 5, par. 1, lett. f del GDPR. Tale procedura di Backup prevederà delle funzioni di salvataggio dei dati e sarà strutturata secondo le esigenze del Titolare del trattamento.

24. Per i servizi che prevedono la fornitura di Supporto ed Assistenza Sistemistica si prevede una manutenzione dell'infrastruttura per quanto previsto dal relativo contratto, garantendo la continuità dei sistemi presenti all'interno del data center. GPI in particolare, per quel che riguarda l'Autorizzazione e autenticazione ha predisposto una politica di controllo degli accessi e procedure documentate. Secondo quanto previsto dal provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, "l'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento o dei responsabili, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti". Infatti, GPI individua i soggetti autorizzati a trattare i dati personali, definendo con il supporto tecnico le corrette autorizzazioni di accesso ai dispositivi e alle aree ove i dati sono trattati/conservati. Nel caso in cui un soggetto autorizzato non abbia più alcun motivo di effettuare l'accesso, GPI procederà immediatamente a rimuovere le relative autorizzazioni. GPI garantisce che l'accesso di ciascun amministratore (access log) è registrato e conservato per almeno sei mesi, con caratteristiche di completezza, integrità ed inalterabilità e comprende anche i riferimenti temporali, la descrizione dell'evento e del sistema coinvolto.

25. I servizi di assistenza telefonica, nel caso in cui non vengano attivati i servizi di registrazioni delle conversazioni, non presentano alcuna criticità dal punto di vista del trattamento di dati personali. Infatti, non vengono trasmessi o archiviati dati e le comunicazioni rimangono verbali. Nel caso in cui vengano attivati i servizi di registrazione delle conversazioni, GPI segue le procedure specifiche che ha predisposto.

26. GPI attua il principio di minimizzazione dei dati, poiché tratta i dati personali in modo adeguato, pertinente e limitato rispetto a quelle che sono le finalità. GPI per poter soddisfare il principio di minimizzazione dei dati personali ex art. 5, par. 1, lett. c GDPR, applica le seguenti misure tecniche, se previste dal contratto sottoscritto:

1. Filtraggio e rimozione;
2. Riduzione del potenziale identificativo attraverso trasformazione;
3. Riduzione della natura identificativa del dato;
4. Riduzione dell'accumulazione dei dati;
5. Limitazione dell'accesso ai dati.

27. GPI utilizza un sistema di controllo degli accessi logici, atti ad assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento. Saranno

definite la lunghezza delle password, la tipologia dei caratteri richiesti, la durata della validità, il numero di tentativi prima del blocco dell'account, ecc.), al fine di limitare i rischi di accesso di persone non autorizzate ai dati personali in forma digitale. Per fare ciò, GPI:

I. definisce profili di autorizzazione nei sistemi separando le attività e le aree di responsabilità per limitare l'accesso degli utenti ai soli dati strettamente necessari per portare a termine i rispettivi compiti;
II. rimuove le autorizzazioni di accesso non appena un utente cessi di essere abilitato ad accedere a una risorsa locale o IT, ovvero allo scadere del contratto;
III. realizza una revisione delle abilitazioni per identificare ed eliminare gli account per i dipendenti che cambiano mansione o lavoro e, pertanto, non fanno più parte del gruppo GPI.

Le password sono dotate dei criteri di complessità previsti dalla normativa:

- Non devono contenere il nome account dell'utente.
- Devono essere composte da almeno otto caratteri.
- Devono contenere caratteri di almeno tre delle quattro categorie seguenti:
  - Lettere maiuscole dell'alfabeto latino (dalla A alla Z)
  - Lettere minuscole dell'alfabeto latino (dalla a alla z)
  - Numeri in base 10 (da 0 a 9)
  - Caratteri non alfanumerici, ad esempio punto esclamativo (!), dollaro ($), simbolo di cancelletto (#) o percentuale (%).