APPENDICE AL CONTRATTO IN ESSERE TRA IL TITOLARE DEL TRATTAMENTO ED IL FORNITORE ESTERNO DI SERVIZI IN OUTSOURCING

Il presente Accordo sulla Protezione dei Dati ("**Accordo**"), Release 2020 01, costituisce parte integrante del contratto già esistente ("**Accordo Principale**") tra:

L'ENTE (da qui in avanti denominatO "**Titolare del Trattamento**") che agisce per proprio conto;

e

ICA Systems S.r.l. con sede in Via Albere, 19 – 37135 Verona - P.I 02655940233 (da qui in avanti denominato **"Responsabile del Trattamento**"**)** che agisce per proprio conto.

I termini utilizzati nel presente Accordo avranno i significati indicati nello stesso. I termini non altrimenti definiti nel presente documento avranno il significato loro attribuito nel Contratto di fornitura di servizi già in essere. Salvo quanto modificato di seguito, i termini del Contratto di fornitura di servizi già in essere rimarranno in vigore a tutti gli effetti.

Le parti concordano che i termini e le condizioni di seguito indicati saranno aggiunti come Addendum al Contratto di fornitura di servizi già in essere.

PREMESSO CHE:

- Il Fornitore effettua per conto del Titolare trattamenti di dati personali nell'ambito dei servizi di cui al contratto di fornitura già in essere;
- L'art. 28 del GDPR prescrive che il titolare del trattamento, qualora intenda far eseguire trattamenti di dati personali per proprio conto, debba ricorrere unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato;
- L'art. 28 del GDPR prescrive che i trattamenti da parte dei responsabili del trattamento siano disciplinati da un atto giuridico stipulato in forma scritta che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, natura e finalità del trattamento, tipo di dati personali e categorie di interessati, nonché obblighi e diritti del titolare del trattamento;
- Con la sottoscrizione del presente accordo il Titolare, aisub sensi dell'articolo 28 del GDPR, nomina il Fornitore Responsabile del trattamento;
- Con la sottoscrizione del presente accordo il Fornitore accetta la nomina a Responsabile del trattamento formulata dal Titolare ai sensi dell'articolo 28 del GDPR e dichiara e garantisce – per esperienza, capacità ed affidabilità – il pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
- Il provvedimento del 27 novembre 2008, modificato con provv. del 25 giugno 2009 ("**Provvedimento Amministratori di Sistema**"), prevede una serie di obblighi per il Titolare del Trattamento concernenti l'individuazione e la designazione di Persone Autorizzate che svolgono all'interno della struttura del Titolare il ruolo di amministratore di sistema, così come definito nel provvedimento richiamato;
- deve essere considerato Amministratore di sistema chiunque, in maniera non occasionale, si occupa della gestione e della manutenzione di impianti di elaborazione con cui vengono effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise resource planning) utilizzati in aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire, anche accidentalmente, sui Dati Personali.

le Parti convengono e stipulano quanto segue:

Oggetto dell'Appendice

Con la sottoscrizione della presente Appendice, che costituisce parte integrante e sostanziale dei Contratti principali già stipulati tra le Parti, il Titolare designa ICA Systems S.r.l. quale "Responsabile del trattamento" ai sensi dell'articolo 28 del RGPD, e ICA Systems S.r.l. accetta tale designazione garantendo - per esperienza, capacità ed affidabilità - il pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
Le Parti concordano che i termini e le condizioni di seguito indicati saranno aggiunti come Appendice, a decorrere dalla data di stipula.

Definizioni

Nel presente Accordo, i seguenti termini avranno i significati indicati e i termini affini devono essere interpretati di conseguenza:

"***Sub Responsabile***" indica qualsiasi Responsabile del Trattamento di Dati (incluso qualsiasi terzo) nominato dal Responsabile del Trattamento per elaborare i Dati personali del Titolare del Trattamento per conto del Titolare del Trattamento.

"***Trattare / Trattamento / Trattato", "Titolare del Trattamento di dati", "Responsabile del Trattamento di dati", "Interessato", "Dati personali", "Categorie particolari di dati personali"*** e qualsiasi altra definizione non inclusa nel presente Accordo o nel Contratto di servizi già in essere devono avere lo stesso significato di cui al Regolamento Generale sulla Protezione dei Dati dell'UE 2016/679 del Parlamento Europeo e del Consiglio dell'Unione Europea ("GDPR").

" Norme sulla protezione dei dati" indica il Regolamento Generale sulla Protezione dei Dati dell'UE 2016/679 del Parlamento Europeo e del Consiglio Europeo ("GDPR"), nonché la normativa nazionale sulla protezione dei dati.

"Cancellazione" indica la rimozione o la distruzione dei Dati Personali in modo che questi non possano essere recuperati o ricostruiti.

"SEE" indica lo Spazio Economico Europeo.

"Paese terzo" indica qualsiasi paese al di fuori dell'UE/SEE, tranne nei casi in cui tale paese sia oggetto di una valida decisione di adeguatezza da parte della Commissione Europea sulla Protezione dei Dati Personali nei Paesi Terzi.

"Dati personali del Titolare del Trattamento" indica i dati descritti nell'Allegato 1 e qualsiasi altro Dato Personale trattato dal Responsabile del Trattamento per conto del Titolare del Trattamento in conformità o in connessione con il Contratto di servizi già in essere.

"Violazione dei dati personali" la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali del Titolare del Trattamento trasmessi, conservati o comunque trattati.

"Servizi" indica i servizi che devono essere forniti dal Responsabile del Trattamento al Titolare del Trattamento in conformità al Contratto di servizi già in essere.

"Prodotti" indica i prodotti che devono essere forniti dal Responsabile del Trattamento al Titolare del Trattamento in conformità al Contratto di servizi già in essere.

"Clausole contrattuali tipo": le clausole contrattuali tipo per il trasferimento di dati personali ai Responsabili stabiliti in paesi terzi, quali approvate dalla decisione della Commissione Europea 2010/87/UE, o qualsiasi serie di clausole approvate dalla Commissione Europea che le modifica, sostituisce o annulla.

1. Termini relativi al Trattamento dei Dati

1.1 Nel corso della fornitura dei Servizi e/o dei Prodotti al Titolare del Trattamento in conformità al Contratto di servizi già in essere, il Responsabile del Trattamento può trattare i dati personali del Titolare del Trattamento per conto del Titolare del Trattamento secondo i termini del presente Addendum. Il Responsabile del Trattamento si impegna a rispettare le seguenti disposizioni in relazione ai dati personali del Titolare del Trattamento.

1.2 Il Responsabile del Trattamento dovrà ottenere e mantenere tutte le licenze, autorizzazioni e permessi necessari per il trattamento dei dati personali, compresi i dati personali di cui all'Allegato 1, nella misura richiesta dalle Norme sulla protezione dei Dati applicabili.

Il Responsabile del Trattamento costruirà e/o manterrà tutte le misure tecniche e organizzative necessarie a soddisfare i requisiti stabiliti nell'addendum e nei suoi allegati.

2. Trattamento dei Dati personali del Titolare del Trattamento

2.1 Il Responsabile del Trattamento tratta i Dati personali del Titolare del Trattamento solo ai fini del rispetto del Contratto di servizi già in essere. Il Responsabile del Trattamento non deve trattare, trasferire, modificare, correggere o alterare i Dati personali del Titolare del Trattamento o divulgare o consentire la divulgazione dei dati personali del Titolare del Trattamento a terzi se non in conformità alle istruzioni documentate del Titolare del Trattamento, a meno che il trattamento non sia richiesto dall'UE o dalle leggi dello Stato Membro a cui è soggetto il Responsabile del Trattamento. Il Responsabile del Trattamento dovrà, nella misura consentita da tali leggi, informare il Titolare del Trattamento di tali requisiti legali prima di trattare i Dati Personali e attenersi alle istruzioni del Titolare del Trattamento per ridurre al minimo, per quanto possibile, l'ambito della divulgazione.

2.2 Ai fini illustrati nella sezione precedente, il Titolare del Trattamento con la presente incarica il Responsabile del Trattamento di trasferire i Dati personali del Titolare del Trattamento ai destinatari nei Paesi della Comunità Europea sempre a condizione che il Responsabile del Trattamento soddisfi la sezione “6. Sub-trattamento”

3. Affidabilità e Non–Divulgazione

3.1 Il Responsabile del Trattamento adotterà misure ragionevoli per garantire l'affidabilità di qualsiasi dipendente, agente o collaboratore che possa avere accesso ai dati personali del Titolare del Trattamento, assicurando in ogni caso che l'accesso sia strettamente limitato alle persone che, per il loro ruolo, hanno la necessità di accedere ai Dati personali del Titolare.

3.2 Il Responsabile del Trattamento deve garantire che tutte le persone che hanno il compito di trattare i dati personali del Titolare del Trattamento:

3.2.1 siano informate della natura confidenziale dei Dati personali del Titolare del Trattamento e siano a conoscenza degli obblighi del Responsabile del Trattamento ai sensi del presente Addendum e del contratto di Servizi già in essere in relazione ai Dati personali del Titolare del Trattamento;

3.2.2 siano in possesso di formazione/certificazioni appropriate in relazione alle Norme sulla protezione dei Dati o qualsiasi altra formazione/certificazione richiesta dal Titolare del Trattamento;

3.2.3 siano soggetti a impegni di riservatezza e/o obblighi professionali e/o normativi di riservatezza;

3.2.4 qualora svolgano il trattamento con sistemi informatici, siano soggetti all'autenticazione dell'utente e alle procedure di accesso quando accedono ai Dati personali del Titolare del Trattamento in conformità al presente Accordo, al Contratto di servizi già in essere e alle Norme sulla protezione dei Dati applicabili.

4. Sicurezza dei Dati Personali

4.1 Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il Responsabile del Trattamento mette in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

4.1.1. la pseudonimizzazione e la cifratura dei dati personali;

4.1.2. La capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

4.1.3. la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali del Titolare del Trattamento in caso di incidente fisico o tecnico; e

4.1.4. una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

4.2. Nel valutare l'adeguato livello di sicurezza, il Responsabile del Trattamento tiene conto, in special modo, dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

5. Sub-Trattamento

5.1. A partire dalla Data di Validità dell'Addendum, il Titolare del Trattamento autorizza il Responsabile del Trattamento a coinvolgere i Sub Responsabili (TRASFERIMENTI AUTORIZZATI DEI DATI PERSONALI DEL TITOLARE DEL TRATTAMENTO). Il Responsabile del Trattamento non ricorre a un Sub Responsabile, per il trattamento dei dati, senza previa autorizzazione scritta, specifica o generale, del Titolare del trattamento. Inoltre, quest'ultimo può rifiutare a sua assoluta discrezione esercitando il potere di opposizione.

5.2. **Il Responsabile del Trattamento, al fine di permettere al Titolare del Trattamento un correto esercizio del potere di opposizione, deve tenere sempre informato il Titolare stesso** di **ogni modifica che determini l'aggiunta o la sostituzione di altri Sub Responsabili;** Per quanto riguarda ciascun Sub Responsabile, il Responsabile del Trattamento dovrà:

5.2.1. fornire al Titolare del Trattamento i dettagli completi sul trattamento dei dati ad opera di ciascun Sub Responsabile;

5.2.2. effettuare un'adeguata *due diligence* su ciascun Sub Responsabile per garantire che possa fornire il livello di protezione dei Dati personali del Titolare del Trattamento, incluse, ma non limitatamente a, sufficienti garanzie per mettere in atto misure tecniche e organizzative appropriate in modo tale che il Trattamento soddisfi i requisiti del GDPR, il presente Accordo, il contratto di fornitura di servizi già in essere e le Norme sulla protezione dei Dati applicabili;

5.2.3. includere i termini nell'accordo tra il Responsabile del Trattamento e ciascun Sub Responsabile che siano gli stessi indicati nel presente Addendum. Su richiesta, il Responsabile del Trattamento dovrà fornire al Titolare del Trattamento una copia dei suoi accordi con i Sub Responsabili, per la sua revisione;

5.2.4. se e quando tale contratto comporti il trasferimento dei Dati Personali del Titolare del Trattamento al di fuori del SEE, incorporare le Clausole Contrattuali Tipo o qualsiasi altro meccanismo, come pre indicato dal Titolare del Trattamento nel contratto tra il Responsabile del Trattamento e ciascun Sub Responsabile per garantire l'adeguata protezione dei Dati personali del Titolare del Trattamento trasferiti;

5.2.5. rimanere pienamente responsabile nei confronti del Titolare del Trattamento per qualsiasi mancanza da parte di ciascun Sub Responsabile nell'adempiere ai propri obblighi in relazione al trattamento dei Dati personali del Titolare del Trattamento.

5.3. A partire dalla Data di validità del presente addendum, il Titolare del Trattamento autorizza il Responsabile del Trattamento a coinvolgere i Sub Responsabili (Trasferimenti Autorizzati dei Dati Personali del Titolare del Trattamento).

6. I Diritti degli Interessati

6.1. Tenuto conto della natura del Trattamento, il Responsabile del Trattamento assisterà il Titolare del Trattamento implementando le misure tecniche e organizzative appropriate, se e quando possibile, per l'adempimento dell'obbligo del Titolare del Trattamento di rispondere alle richieste degli interessati di esercitare i propri diritti, come stabilito nel GDPR.

6.2. Il Responsabile del Trattamento dovrà informare tempestivamente il Titolare del Trattamento se riceve una richiesta da un interessato, dall'Autorità di controllo e/o altra autorità competente ai sensi delle Norme sulla protezione dei dati applicabili in relazione ai Dati Personali del Titolare del Trattamento.

6.3. Il Responsabile del Trattamento dovrà cooperare, senza alcun onere aggiuntivo, col Titolare del Trattamento, come dallo stesso richiesto, per consentirgli di conformarsi a qualsiasi esercizio di diritti da parte di un Interessato ai sensi delle Norme sulla protezione dei Dati in relazione ai dati personali del Titolare del Trattamento e conformarsi a qualsiasi valutazione, richiesta, avviso o indagine, in base alle Norme sulla Protezione dei dati o al presente Accordo, in riferimento ai Dati Personali del Titolare del Trattamento. Tra le richieste a cui il Responsabile del Trattamento deve rispondere efficacemente e velocemente si devono menzionare:

6.3.1 la fornitura di tutti i dati richiesti dal Titolare entro un ragionevole periodo di tempo specificato dal Titolare in ciascun caso, comprese le informazioni complete e le copie del reclamo, della comunicazione o della richiesta e qualsiasi Dato Personali che il Responsabile del Trattamento conserva relativo a un Interessato;

6.3.2 ove applicabile, fornire l'assistenza richiesta dal Titolare del Trattamento per consentirgli di soddisfare la relativa richiesta entro i termini prescritti dalle Norme sulla Protezione dei Dati;

6.3.3 l'implementazione di eventuali misure tecniche e organizzative aggiuntive che possano essere ragionevolmente richieste dal Titolare del Trattamento per consentire al Titolare del Trattamento di rispondere in modo efficace a reclami, comunicazioni o richieste pertinenti.

7. Violazione dei Dati Personali

7.1. Il Responsabile del Trattamento dovrà inviare una notifica al Titolare del Trattamento senza indebito ritardo e, in ogni caso, entro ventiquattro (24) ore da quando è venuto a conoscenza di una violazione di dati o di elmenti che inducano il ragionevole sospetto che abbia avuto luogo una violazione di dati personali. Il Responsabile del Trattamento fornirà al Titolare del Trattamento informazioni sufficienti per consentire al Titolare del Trattamento di adempiere a qualsiasi obbligo di segnalare una violazione dei Dati Personali ai sensi delle Norme sulla protezione dei Dati. Tale notificadeve come minimo:

7.1.1. descrivere la natura della violazione dei dati personali, le categorie e il numero dei soggetti interessati, nonché le categorie e il numero di registrazioni di dati personali colpite dalla violazione;

7.1.2. comunicare il nome e le informazioni di contatto del Responsabile della protezione dei dati, del Responsabile della privacy o di altri contatti rilevanti dai quali possono essere ottenute ulteriori informazioni;

7.1.3. descrivere il rischio stimato e le probabili conseguenze della Violazione dei Dati Personali;

7.1.4. descrivere le misure adottate o proposte per gestire la Violazione dei Dati Personali.

7.2. Il Responsabile del Trattamento dovrà cooperare con il Titolare del Trattamento e intraprendere le misure ragionevoli, come indicate dal Titolare del Trattamento, per assistere nelle indagini, nella mitigazione e risoluzione di ogni Violazione dei Dati Personali.

7.3. In caso di violazione dei dati personali, il Responsabile del Trattamento non deve informare terzi senza prima ottenere il consenso scritto del Titolare del Trattamento, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il Responsabile del Trattamento. In tal caso, il Responsabile del Trattamento dovrà informare il Titolare del Trattamento circa tale obbligo giuridico, fornire una copia della notifica proposta e considerare eventuali commenti formulati dal Titolare del Trattamento prima di notificare la Violazione dei dati personali**.**

8. Valutazione d'Impatto sulla Protezione dei Dati e Consultazione Preventiva

Il Responsabile del Trattamento fornirà al Titolare del Trattamento un'assistenza ragionevole con qualsiasi valutazione d'impatto sulla protezione dei dati richiesta dall'articolo 35 del GDPR e previa consultazione con qualsiasi autorità di controllo da parte del Titolare del Trattamento che sia richiesta ai sensi dell'articolo 36 del GDPR, in ogni caso unicamente in relazione al trattamento dei dati personali del Titolare del Trattamento da parte del Responsabile del

Trattamento per conto del Titolare del Trattamento e considerate la natura del trattamento e delle informazioni disponibili al Responsabile del Trattamento.

9. Cancellazione o restituzione dei Dati Personali del Titolare del Trattamento

9.1. Il Responsabile del Trattamento dovrà prontamente e, in ogni caso, entro e non oltre 90 (novanta) giorni solari: (i) cessare il Trattamento dei Dati Personali del Titolare del Trattamento, documentandone la cessazione; o (ii) risolvere il Contratto di servizi già in essere, a scelta del Titolare del Trattamento (tale scelta deve essere notificata al Responsabile del Trattamento per iscritto). Dovrà inoltre:

9.1.1. restituire una copia completa di tutti i Dati personali del Titolare del Trattamento al Titolare stesso mediante trasferimento sicuro di file nel formato indicato dal Titolare del Trattamento al Responsabile del Trattamento e cancellare in modo sicuro tutte le altre copie dei Dati personali del Titolare del Trattamento elaborati dal Responsabile del Trattamento o da qualsiasi Sub Responsabile Autorizzato; o

9.1.2. cancellare in modo sicuro tutte le copie dei dati personali del Titolare del Trattamento trattati dal Responsabile del Trattamento o da qualsiasi Sub Responsabile autorizzato e, in ogni caso, fornire una certificazione scritta al Titolare del Trattamento attestante che ha rispettato pienamente i requisiti della sezione Cancellazione o Restituzione dei Dati Personali del Titolare del Trattamento.

9.2. Il Responsabile del Trattamento può conservare i Dati personali del Titolare del Trattamento nellamisura richiesta dalle leggi dell'Unione o dello Stato Membro, e solo nella misura e per il periodo richiesto dalla legge dell'Unione o dello Stato Membro, e sempre a condizione che il Responsabile del Trattamento garantisca la riservatezza di tutti i Dati personali del Titolare del Trattamento e garantisca che i Dati personali del Titolare del Trattamento siano trattati esclusivamente secondo le necessità per gli scopi specificati nelle leggi dell'Unione o degli Stati membri che richiedono la sua conservazione e per nessun'altra finalità.

10. Diritti di audit

Il Responsabile del Trattamento dovrà mettere a disposizione del Titolare del Trattamento, su richiesta, tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del Trattamento o da un altro soggetto da questi incaricato di qualsiasi sede in cui il Trattamento di Dati Personali del Titolare del Trattamento abbia luogo. Il Responsabile del Trattamento consentirà al Titolare del Trattamento o ad altro auditor incaricato dal Titolare del Trattamento di ispezionare, verificare e copiare tutte le registrazioni, processi e sistemi pertinenti in modo che il Titolare del Trattamento possa accertarsi che le disposizioni del presente Addendum siano rispettate. Il Responsabile del Trattamento dovrà fornire piena collaborazione al Titolare del Trattamento in relazione a tali audit e fornirà, su richiesta del Titolare del Trattamento, evidenza del rispetto degli obblighi previsti dal presente Addendum. Il Responsabile del Trattamento dovrà immediatamente informare il Titolare qualora, a suo parere, un'istruzione ai sensi della presente sezione "Diritti di Audit" violi il presente regolamento o altre disposizioni, nazionali o dell'Unione Europea, relative alla protezione dei dati.

11. Trasferimento dei Dati Personali del Titolare del Trattamento

11.1. Il Responsabile del Trattamento non tratterà i Dati Personali del Titolare del Trattamento né consentirà a nessun Sub-Responsabile Autorizzato di trattare i Dati Personali del Titolare del Trattamento in un Paese terzo, e solo se sia stato preventivamente autorizzato per iscritto dal Titolare del Trattamento, mediante un emendamento al presente Addendum.

11.2. Quando richiesto dal Titolare del Trattamento, il Responsabile del Trattamento dovrà prontamente stipulare (o provvedere che qualsiasi pertinente Sub Responsabile del Responsabile del Trattamento stipuli) un accordo con il Titolare del Trattamento che includa le Clausole Contrattuali Tipo e/o una variante come potrebbe essere richiesto dalle Norme sulla Protezione dei Dati, in relazione a qualsiasi trattamento di Dati Personali del Titolare del Trattamento in un Paese terzo, i quali termini avranno la precedenza su quelli del presente Addendum.

12. Codici di Condotta e Certificazione

Su richiesta del Titolare del Trattamento, il Responsabile del Trattamento dovrà rispettare qualsiasi Codice di condotta approvato ai sensi dell'articolo 40 del GDPR e ottenere qualsiasi certificazione approvata dall'articolo 42 del GDPR dell'UE, per quanto riguarda il trattamento dei Dati personali del Titolare del Trattamento.

13. Condizioni generali

13.1. In base a questa sezione, le parti concordano che il presente Accordo e le clausole contrattuali tipo terminano automaticamente in caso di risoluzione del Contratto di servizi già in essere o alla scadenza o alla risoluzione di tutti i contratti di servizio stipulati dal Responsabile del Trattamento con il Titolare del Trattamento, ai sensi del Contratto di servizi già in essere, qualunque venga dopo.

13.2. Qualsiasi obbligo imposto al Responsabile del Trattamento ai sensi del presente Addendum in relazione al Trattamento dei Dati personali sopravviverà a qualsiasi risoluzione o scadenza di questo Addendum.

13.3. Il presente Addendum, ad esclusione delle clausole contrattuali tipo, è regolato dagli articoli di legge previsti nel Contratto di servizi già in essere per tutto il tempo in cui tali articoli facciano parte della legislazione di uno Stato membro dell'Unione Europea.

13.4. Qualsiasi violazione di questo Addendum costituirà una violazione sostanziale del Contratto di servizi già in essere.

13.5. Per quanto riguarda l'oggetto del presente Addendum, in caso di incongruenze tra le disposizioni del presente Addendum e qualsiasi altro accordo tra le parti, incluso ma non limitato al Contratto di servizi già in essere, le disposizioni del presente Addendum prevarranno per quanto riguarda gli obblighi delle parti di protezione dei dati personali di un interessato di uno Stato membro dell'Unione Europea.

13.6. Qualora una qualsiasi disposizione di questo Addendum fosse non valida o inapplicabile, il resto di questo Addendum rimarrà valido e in vigore. La clausola non valida o inapplicabile sarà (i) emendata se necessario per garantirne la validità e l'applicabilità, preservando nel contempo il più strettamente possibile le intenzioni delle parti o, se ciò non fosse possibile, (ii) interpretata in modo tale che la parte non valida o inapplicabile non sia mai stata contenuta in esso.

IN FEDE questo Addendum è stata sottoscritto e diventa una parte vincolante del Contratto di servizi già in essere con effetto dalla Data dell'entrata in vigore dell'Addendum sopra riportata**.**

Titolare del trattamento

_____

Responsabile del trattamento

Francessco Russo

francesco russo
23.06.2023 15:23:44 GMT+00:00

ALLEGATO 1: INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI DEL TITOLARE DEL TRATTAMENTO

Il presente Allegato 1 include alcune informazioni specifiche sul trattamento dei dati personali del Titolare del Trattamento ai sensi dell'articolo 28, paragrafo 3, del GDPR.

Oggetto e durata del Trattamento dei Dati Personali del Titolare del Trattamento

1. La durata del Trattamento dei Dati Personali è correlata alla durata del rapporto contrattuale definita dal contratto di servizi in essere.
2. *L'oggetto del Trattamento dei Dati Personali del Titolare del Trattamento:* Supporto assistenza su incarico dei clienti clienti/Comuni
3. *.I tipi di Dati Personali del Titolare del Trattamento da trattare:* potenzialmente tutti i dati personali contenuti nei moduli oggetto di acquisto nel presente contratto
4. *Le categorie di Interessati cui si riferiscono i Dati Personali del Titolare del Trattamento:* potenzialmente tutti gli interessati i cui dati personali sono contenuti nei moduli oggetto di acquisto nel presente contratto

ALLEGATO 1: INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI DEL TITOLARE DEL TRATTAMENTO

L'informazine sul trattamento dei dati personali saà parte integrante dell'offerta di software e servizi

ALLEGATO 2: MISURE TECNICHE E ORGANIZZATIVE

1. Misure organizzative di sicurezza

1.1. Gestione della sicurezza

a. Politica e procedure di sicurezza: il Responsabile del Trattamento deve documentare una politica di sicurezza in merito al trattamento dei dati personali.

b. Ruoli e responsabilità:

i. I ruoli e le responsabilità relativi al trattamento dei dati personali sono chiaramente definiti e assegnati in conformità con la politica di sicurezza.

ii. Durante le riorganizzazioni interne o le cessazioni e il cambio di lavoro, la revoca dei diritti e delle responsabilità con le rispettive procedure di trasferimento sono chiaramente definite.

c. Politica di controllo dell'accesso: specifici diritti di controllo dell'accesso sono assegnati a ciascun ruolo coinvolto nel trattamento dei dati personali, seguendo il principio della necessità di sapere.

d. Gestione delle risorse/dei beni: il Responsabile del Trattamento dispone di un registro delle risorse IT utilizzate per il trattamento dei dati personali (hardware, software e rete). Ad una persona specifica è assegnato il compito di mantenere e aggiornare il registro (ad esempio, il responsabile IT).

e. Gestione delle modifiche: il Responsabile del Trattamento si assicura che tutte le modifiche al sistema IT siano registrate e monitorate da una persona specifica (ad esempio, il responsabile IT o della sicurezza). Ha luogo Il monitoraggio regolare di questo processo.

1.2. Risposta agli incidenti e continuità operativa

a. Gestione degli incidenti/Violazione dei dati personali:

i. Viene definito, a cura del Responsabile del Trattamento, un piano di risposta agli incidenti con procedure dettagliata, da inviare senza ritardo al Titolare del Trattamento, per garantire una risposta efficace e ordinata agli incidenti relativi ai dati personali.

ii. Il Responsabile del Trattamento segnalerà senza indebito ritardo al Titolare del Trattamento qualsiasi incidente di sicurezza che abbia comportato una perdita, un uso improprio o l'acquisizione non autorizzata di dati personali.

b. Continuità operativa: il Responsabile del Trattamento stabilisce le principali procedure e i controlli da seguire al fine di garantire il livello richiesto di continuità e disponibilità del sistema informatico che elabora i dati personali (in caso di incidente /violazione dei dati personali).

1.3. Risorse umane

a. Riservatezza del personale: il responsabile del trattamento garantisce che tutti i dipendenti comprendano le proprie responsabilità e gli obblighi relativi al trattamento dei dati personali. I ruoli e le responsabilità sono chiaramente comunicati durante il processo di pre-assunzione e/o di inserimento.

b. Formazione: il Responsabile del Trattamento garantisce che tutti i dipendenti siano adeguatamente informati e formati sui controlli di sicurezza del sistema IT relativi al lavoro quotidiano. I dipendenti coinvolti nel trattamento dei dati personali sono adeguatamente informati e formati in merito ai requisiti di protezione dei dati e agli obblighi legali attraverso regolari campagne di sensibilizzazione e progetti di formazione

2. Misure tecniche di sicurezza

2.1. Controllo degli accessi e autenticazione

a. Viene implementato un sistema di controllo degli accessi applicabile a tutti gli utenti che accedono al sistema IT. Il sistema consente di creare, approvare, rivedere ed eliminare gli account utente.

b. Viene evitato l'uso di account utente comuni. Nei casi in cui ciò fosse necessario, è garantito che tutti gli utenti dell'account comune abbiano gli stessi ruoli e responsabilità.

c. Quando si concede l'accesso o si assegnano ruoli utente, si deve osservare il "principio della necessità di sapere" al fine di limitare il numero di utenti che hanno accesso ai dati personali solo a coloro che lo richiedono per il raggiungimento delle finalità di trattamento del Responsabile del Trattamento.

d. Laddove i meccanismi di autenticazione sono basati su password, il Responsabile del Trattamento richiede che la password sia lunga almeno otto caratteri e sia conforme a parametri di controllo di password molto forti, tra cui lunghezza, complessità dei caratteri e la non ripetibilità.

e. Le credenziali di autenticazione (come l'ID utente e la password) non devono mai essere trasmesse non protette sulla rete.

2.2. Registrazione e monitoraggio: i file di registro vengono attivati per ogni sistema/applicazione utilizzata per il trattamento dei dati personali. Includono tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione).

2.3. Sicurezza dei dati a riposo

a. Sicurezza del server / database

i. I server di database e applicazioni sono configurati per funzionare utilizzando un account separato, con i privilegi minimi del sistema operativo per funzionare correttamente.

ii. I server di database e applicazioni trattano solo i dati personali che è effettivamente necessario trattare al fine di raggiungere le proprie finalità di trattamento.

b. Sicurezza della postazione:

i. Gli utenti non sono in grado di disattivare o bypassare le impostazioni di sicurezza.
ii. Le applicazioni antivirus e le firme di rilevamento sono configurate su base regolare.
iii. Gli utenti non hanno i privilegi per installare o disattivare applicazioni software.
iv. il sistema ha timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo.
v. Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo sono installati regolarmente.

2.4. Sicurezza di rete / comunicazione:

a. Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione viene crittografata tramite protocolli di cifratura.
b. Il traffico da e verso il sistema IT viene monitorato e controllato tramite firewall e sistemi di rilevamento delle intrusioni.

2.5. Back-up:

a. Le procedure di backup e ripristino dei dati sono definite, documentate e chiaramente collegate a ruoli e responsabilità.
b. Ai backup viene fornito un livello appropriato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.
c. L'esecuzione dei backup viene monitorata per garantirne la completezza.

2.6. Dispositivi mobili / portatili:

a. Le procedure di gestione dei dispositivi mobili e portatili sono definite e documentate stabilendo regole chiare per il loro corretto utilizzo.
b. I dispositivi mobili ai quali è consentito accedere al sistema informativo sono pre-registrati e pre-autorizzati.

2.7. Sicurezza del ciclo di vita delle applicazioni: durante il ciclo di vita dello sviluppo, vengono seguite le best practice, lo stato dell'arte e pratiche o standard di sviluppo sicuro ben noti.

2.8. Cancellazione / eliminazione dei dati:

a. La sovrascrittura basata sul software verrà eseguita sui supporti prima del loro smaltimento. Nei casi in cui ciò non fosse possibile (CD, DVD, ecc.) verrà eseguita la distruzione fisica.
b. Viene effettuata la triturazione di carta e supporti portatili utilizzati per registrate i dati personali.

2.9. Sicurezza fisica: il perimetro fisico dell'infrastruttura del sistema IT non è accessibile al personale non autorizzato. Devono essere adottate misure tecniche adeguate (ad es. sistema di rilevamento delle intrusioni, tornello azionato da tessere munite di chip, sistema di ingresso di sicurezza per singola persona, sistema di chiusura) o misure organizzative (ad es. guardiania) per proteggere le aree di sicurezza e i loro punti di accesso dall'ingresso di persone non autorizzate.

2.10. Sviluppo di sistemi web based: qualora il Responsabile del Trattamento si occupi dello sviluppo, della gestione e della manutenzione di piattaforme web, così come definito nel contratto di servizi esistente, esso si impegna a:

a. Accertarsi che tutti i form di raccolta dati, anche nel caso siano forniti dal Titolare del Trattamento con un servizio esterno, rispettino le formule di acquisizione del consenso in base alle finalità del Trattamento definite con il Titolare del Trattamento. Qualora i form di raccolta dati siano sviluppati e/o implementati dal Reponsabile del Trattamento, essi dovranno rispettare i requisiti di registrazione dei consensi, salvando almeno la data, il nominativo e la tipologia di essi.
b. Garantire che il codice di sviluppo utilizzato rispetti i requisiti previsti dalle linee guida secondo la norma ISO/IEC 9126 soprattutto in termini di affidabilità e sicurezza, nonché i principi di sicurezza secondo lo standard ISO/IEC 27001.
c. Garantire al Titolare del Trattamento l'adeguatezza e la sicurezza delle piattaforme software specifiche adottate: a titolo esemplificativo ma non esaustivo qualora si utilizzino piattaforme di gestione dei contenuti come Wordpress e/o Joomla, il Responsabile del Trattamento dovrà provvedere al regolare aggiornamento sia della base del software (core) sia degli eventuali plug-in installati. Lo stesso principio deve intendersi applicato per eventuali database server come NOSql, MySql, MS SQL, Postgres, Oracle, ElasticSearch, MariaDB, etc e application server come Apache, Tocat, IIS.
d. Eventuali integrazioni e/o scambi di dati con altri servizi esterni, sempre autorizzati preventivamente dal Titolare del Trattamento, dovranno rispettare la crittografia delle comunicazioni, dovranno garantire che tutte le operazioni sui dati personali (a titolo esemplificativo ma non esaustivo l'accesso, l'interpolazione, la modifica, la cancellazione) avvengano rispettando i requisiti di autenticazione e profilazione in base alle effettive necessità di accesso, dovranno prevedere l'utilizzo di protocolli e/o sistemi riconosciuti dal mercato internazionale e/o da enti certificatori (a titolo esemplificativo ma non esasutivo: servizi SOAP e/o REST per API via HTTPS).

2.11. Amministratori di sistema: Il Responsabile si impegna ad adottare tutte le misure ed accorgimenti prescritti ai titolari del trattamento effettuato con strumenti elettronici, relativamente alle attribuzioni delle funzioni di amministratore

di sistema – **(Provvedimento a carattere generale del Garante per la protezione dei dati personali del 27 novembre 2008 e successive integrazioni, in G.U. n. 300 del 24 dicembre 2008)**, comunicando tempestivamente al Titolare del Trattamento dati anagrafici degli stessi dal Responsabile nominati.

2.12. **Cookies e sistemi di tracciamento della navigazione:** Qualora il Responsabile adotti e/o fornisca una piattaforma web si impegna ad adottare tutte le misure ed accorgimenti prescritti ai titolari del trattamento riguardanti l'individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie – (provvedimento Garante Privacy del 8 maggio 2014 Pubblicato sulla Gazzetta Ufficiale n. 126 del 3 giugno 2014), condividendo la tipologia di cookies (cookie "tecnici" e/o cookie "di profilazione ma anonimizzati") e comunicando tempestivamente al Titolare del Trattamento le tecnologie adottate al fine di rendere regolare informativa e richiedere l'eventuale consenso ai visitatori dei propri siti web.