DPA eDisplay srl

2021

Sommario

ACCORDO PRINCIPALE PER IL TRATTAMENTO DI DATI PERSONALI – MASTER DATA PROCESSING AGREEMENT (MDPA) (dal Regolamento UE 2016/679)

Il presente accordo per la Protezione di Dati Personali è concluso tra Edisplay srl e il Cliente, come di seguito meglio individuati, in ottemperanza alle disposizioni di cui all'art. 28 Reg. UE 2016/679 (di seguito anche solo "GDPR"). Le disposizioni qui previste costituiscono appendice e integrano quanto statuito nel/i contratto/i stipulato/i tra le parti ai fini della fornitura di uno o più prodotti e/o servizi da parte di Edisplay. Le parti sono individuate come segue:

- Per "Fornitore" (di seguito anche solo il "Fornitore", il "Responsabile" o "eDisplay") si intende: eDisplay srl, con sede legale in Fonni (NU) nel viale del Lavoro n. 53, P.IVA e C.F 01172340919, in persona del suo legale rappresentante pro tempore Raffaele Serusi;
- Per "Cliente" (di seguito anche solo il "Cliente" o il "Titolare") si intende il soggetto indicato nel/i contratto/i con cui il Cliente ha acquistato uno o più prodotti e/o servizi offerti dal Fornitore e che ne disciplinano termini e condizioni.

Fornitore e Cliente saranno anche di seguito denominati, congiuntamente, le "Parti" e ognuno di essi, disgiuntamente, la "Parte".

PREMESSO CHE

a. Il Cliente ha sottoscritto uno o più contratti (di seguito il "Contratto") con il Fornitore, volti all'acquisto di uno o più prodotti e/o servizi offerti da quest'ultimo, al cui contenuto si rimanda integralmente per ogni aspetto non specificato nel presente accordo;
b. Le Parti intendono disciplinare nel presente "accordo principale per il trattamento dei dati personali – Master Data Processing Agreement" (di seguito "MDPA" o "Accordo") le condizioni e le modalità del trattamento dei dati personali eseguito dal Fornitore nell'ambito del Contratto e della prestazione dei Servizi e le responsabilità connesse al trattamento medesimo, ivi incluso l'impegno assunto dal Fornitore, quale Responsabile del trattamento dei dati personali, ai sensi dell'art. 28 del GDPR. Le disposizioni del presente MDPA sono integrate, ove occorra, da apposito Data Processing Agreement (DPA) specifico per ogni prodotto/servizio che, ove predisposto, viene consegnato al Cliente contestualmente al presente accordo;
c. Il Cliente ha valutato che il Fornitore possiede requisiti di affidabilità, capacità ed esperienza tali da fornire adeguata garanzia di rispetto delle vigenti disposizioni in materia di trattamento dei dati personali;
d. Con la stipula del relativo contratto per la prestazione di uno o più fra i servizi offerti dal Responsabile, il Cliente dichiara di accettare integralmente le condizioni che seguono.

1. DEFINIZIONI E INTERPRETAZIONE

Le premesse costituiscono parte integrante del presente Accordo.
Nell'Accordo i seguenti termini ed espressioni avranno il significato associato ad essi qui di seguito:
"**Data di Decorrenza dell'Accordo"** indica la data in cui il Cliente sottoscrive o accetta il presente accordo;
"Dati Personali" ha il significato di cui alla Legislazione in materia di Protezione dei Dati Personali e include tutti i dati, i quali siano oggetto di trattamento da parte del Fornitore in conseguenza del Contratto. Sono quindi inclusi, ad esempio, tutti i dati forniti, archiviati, inviati, ricevuti o altrimenti elaborati o creati dal Cliente, nonché dall'Utente Finale in relazione alla fruizione dei Servizi.
"Decisione di Adeguatezza" indica una decisione della Commissione Europea sulla base dell'Articolo 45(3) del GDPR in merito al fatto che le leggi di un certo paese garantiscano un adeguato livello di protezione, come previsto dalla Legislazione in materia di Protezione dei Dati Personali;

“Indirizzo di notifica” si intende l'indirizzo (o gli indirizzi) e-mail e/o PEC fornito/i dal Cliente, all'atto della sottoscrizione del Servizio o fornito/i tramite altro canale ufficiale al Fornitore e a cui il Cliente intende ricevere le notifiche da parte del Fornitore;
“Istruzioni” indica le istruzioni scritte impartite dal Titolare nel presente Accordo e eventualmente, nel Contratto;
“Legislazione in materia di Protezione dei Dati Personali” indica il GDPR, e ogni eventuale ulteriore norma e/o regolamento di attuazione emanati ai sensi del GDPR o comunque vigenti in Italia in materia di protezione dei Dati Personali, nonché ogni provvedimento vincolante che risulti emanato dalle autorità di controllo) competenti in materia di protezione dei Dati Personali (es. Garante per la protezione dei dati personali, e conservi efficacia vincolante (ivi inclusi i requisiti delle Autorizzazioni generali al trattamento dei dati sensibili e giudiziari, se applicabili e ove abbiano mantenuto la propria efficacia vincolante successivamente al 25 maggio 2018).
“Personale del Fornitore” indica i dirigenti, dipendenti, consulenti, e altro personale del fornitore in qualità di soggetti autorizzati, con esclusione del personale dei Responsabili Ulteriori del Trattamento;
“Richiesta” indica qualunque richiesta di un interessato che rientri tra quelle previste nella Legislazione in materia di Protezione dei Dati Personali (es. esercizio dei diritti, reclami);
“Responsabile Ulteriore del Trattamento” indica qualunque soggetto terzo che tratti dati personali per conto del Responsabile, qualora rispetto agli stessi dati il Cliente rivesta la qualità di Titolare o anche ove il Cliente rivesta la qualità di Responsabile e il Fornitore di ulteriore Responsabile rispetto a questi;
“Servizio/i” indica il servizio o i servizi, nonché eventuali prodotti oggetto del/i Contratto/i sottoscritto/i tempo per tempo tra il Cliente e il Fornitore;
“Utente Finale” si intende l'eventuale fruitore finale del Servizio, Titolare del Trattamento; **“Violazione della Sicurezza dei Dati Personali”** o “Data Breach” indica 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 occorsa su sistemi gestiti dal Fornitore o comunque sui quali il Fornitore abbia un controllo.
“Termini e Condizioni” accordo commerciale a cui si fa esplicitamente riferimento (disposizioni contenute nel “Contratto”).

2. RUOLO DELLE PARTI

2.1. Le Parti riconoscono e convengono che, per le finalità di cui al Contratto, il Fornitore agisce quale Responsabile del trattamento (“Responsabile”) ai sensi dell’art. 28 del GDPR e il Cliente agisce quale Titolare del trattamento dei Dati Personali (“Titolare”).
2.2. Qualora il Cliente svolga operazioni di trattamento per conto di altro Titolare, il Cliente potrà agire come Responsabile del trattamento. In tal caso, il Cliente garantisce che le istruzioni impartite e le attività intraprese in relazione al trattamento dei Dati Personali, inclusa la nomina, da parte del Cliente, del Fornitore quale Responsabile ulteriore del Trattamento derivante dalla stipula del presente Accordo è stata autorizzata dal relativo titolare del trattamento e si impegna ad esibire al Fornitore, dietro sua richiesta scritta, la documentazione attestante quanto sopra.
2.3. Ciascuna delle Parti si impegna a conformarsi, nel trattamento dei Dati Personali, ai rispettivi obblighi derivanti dalla Legislazione in materia di Protezione dei Dati Personali applicabile.
2.4. Il Fornitore è espressamente autorizzato a fare ricorso, ove occorra, a Responsabili Ulteriori del Trattamento. Il Fornitore garantisce, il tal caso, che su tali responsabili saranno imposti gli stessi obblighi in materia di protezione dei dati cui è esso stesso assoggettato in base al presente MDPA.
2.5. Il Titolare è tenuto a garantire che il trattamento dei Dati Personali di cui al Contratto sia effettuato conformemente alla Legislazione in materia di Protezione dei Dati Personali.

3. TRATTAMENTO DEI DATI PERSONALI

3.1. Con la stipula del presente Accordo, il Cliente affida al Fornitore l'incarico di trattare i Dati Personali ai soli fini della prestazione dei Servizi così come meglio dettagliati nel Contratto e nel presente Accordo.
3.2. L’accesso ai Dati Personali è finalizzato al perseguimento di un interesse esclusivo del Titolare e i

Dati Personali non saranno in alcun modo utilizzati per il perseguimento di scopi propri del Responsabile. Per ogni trattamento effettuato, il Responsabile si impegna a porre in essere le misure di sicurezza previste dalla Legislazione in materia di Protezione dei Dati Personali e a non agire per finalità illecite.
3.3. Il Fornitore si impegna a conformarsi alle Istruzioni e a rispettare tutti gli obblighi previsti dalla Legislazione in materia di Protezione dei Dati Personali in capo allo stesso, fermo restando che, qualora il Cliente richieda variazioni rispetto alle Istruzioni iniziali, il Fornitore valuterà gli aspetti di fattibilità e concorderà con il Cliente le predette variazioni ed i costi connessi.
3.4. Nei casi di cui all'art. 3.3 e in caso di richieste del Cliente che comportino il trattamento di Dati Personali che siano, ad avviso del Fornitore, in violazione della Legislazione in materia di Protezione dei Dati Personali, il Fornitore è autorizzato ad astenersi dall'eseguire tali Istruzioni e ne informerà prontamente il Cliente. In tali casi il Cliente potrà valutare eventuali variazioni alle Istruzioni impartite o contattare l'Autorità di controllo per verificare la liceità delle richieste avanzate.

4. LIMITAZIONI ALL'UTILIZZO DEI DATI PERSONALI

4.1. Nell'eseguire il trattamento dei Dati Personali ai fini della prestazione dei Servizi, il Fornitore si impegna a eseguire il trattamento dei Dati Personali:

a. soltanto nella misura e con le modalità necessarie per erogare i Servizi o per adempiere opportunamente i propri obblighi, previsti dal Contratto e dal presente Accordo ovvero imposti dalla Legislazione in materia di Protezione dei Dati Personali. In tale ultima circostanza il Fornitore ne informerà il Cliente (salvo il caso in cui ciò sia vietato dalla legge per ragioni di pubblico interesse) mediante comunicazione trasmessa all'Indirizzo di notifica;
b. in conformità alle Istruzioni del Cliente.

4.2. Il Personale del Fornitore che accede, o comunque tratta i Dati Personali, è preposto al trattamento di tali dati sulla base di idonee autorizzazioni e ha ricevuto la necessaria formazione anche in merito al trattamento dei Dati Personali. Tale personale è altresì vincolato da obblighi di riservatezza e dal Codice Etico aziendale e deve attenersi alle policy di riservatezza e di protezione dei dati personali adottate dal Fornitore ("Soggetti Autorizzati").

5. DISPOSIZIONI IN MATERIA DI SICUREZZA DEL FORNITORE E DIRITTI DEGLI INTERESSATI

5.1. Nell'eseguire il trattamento dei Dati Personali, il Fornitore, ai fini della prestazione dei Servizi adotta misure tecnico-organizzative adeguate al fine di minimizzare i rischi di trattamento illecito o non autorizzato, distruzione accidentale o illecita, danneggiamento, perdita accidentale, alterazione o divulgazione non autorizzata di, o accesso ai, Dati Personali, come descritte nell'Allegato 1 al presente Accordo ("Misure di Sicurezza TECNICO ORGANIZZATIVE" o "Allegato 1").
5.2. L'Allegato 1 all'Accordo contiene misure di protezione degli archivi dati commisurate al livello dei rischi presenti con riferimento ai Dati Personali per consentire la riservatezza, integrità, disponibilità e resilienza dei sistemi e dei Servizi del Fornitore, nonché misure per consentire il tempestivo ripristino degli accessi ai Dati Personali in caso di Violazione della Sicurezza dei Dati Personali, e misure per testare l'efficacia nel tempo di dette misure. Il Cliente dà atto ed accetta che, tenuto conto dello stato dell'arte, dei costi di implementazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità di trattamento dei Dati Personali, le procedure e i criteri di sicurezza implementati dal Fornitore garantiscono un livello di protezione adeguato al rischio per quanto riguarda i suoi Dati Personali.
5.3. Il Fornitore potrà aggiornare e modificare nel tempo le Misure di Sicurezza sopra indicate, fermo restando che tali aggiornamenti e modifiche non potranno comportare una riduzione del livello di sicurezza complessivo dei Servizi.
5.4. Qualora il Cliente richieda di adottare misure di sicurezza aggiuntive rispetto alle Misure di Sicurezza, il Fornitore si riserva il diritto di valutarne la fattibilità e, prima dell'eventuale implementazione delle stesse, concorderà in buona fede con il Titolare eventuali costi aggiuntivi. 5.5. Il Fornitore, tenuto conto della natura del trattamento e delle informazioni a sua disposizione, assiste il Cliente nel garantire il rispetto degli obblighi di sicurezza di cui agli artt. 32- 36 del GDPR nei modi definiti

nel presente accordo;
5.6. Il Fornitore garantisce che saranno poste in essere tutte le necessarie misure tecnico organizzative volte ad assicurare un adeguato livello di sicurezza commisurato al grado di rischio.
5.7. Qualora il prodotto/servizio oggetto del Contratto consenta l'operatività con applicativi di terze parti (es. fogli di Google, prodotti per l'eCommerce) che il Cliente può liberamente scegliere di utilizzare, la responsabilità circa tale scelta resta in capo al Cliente e il Fornitore non potrà essere ritenuto responsabile dell'applicazione di idonee Misure di Sicurezza nelle componenti delle terze parti o delle modalità di funzionamento delle stesse e del rispetto, in generale, del GDPR da parte della terza parte.
5.8. Il Responsabile, tendendo conto della natura del trattamento assiste il Titolare con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo di quest'ultimo di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III GDPR. Il Titolare riconosce e accetta che la gestione dei rapporti con gli interessati resta a suo carico ed è quindi lo stesso Titolare a dover dare riscontro a tali richieste o eventuali reclami. Ove venga contattato direttamente da un interessato, il Responsabile raccoglie le richieste, raccomandando all'interessato di rivolgersi direttamente al Cliente, in quanto Titolare del trattamento. Contestualmente, il fornitore comunica tramite mail la richiesta/il reclamo ricevuto al Titolare, corredandolo di eventuali informazioni che non siano già nella disponibilità del Titolare e che si rendano necessarie per l'evasione della richiesta/del reclamo."
5.9. Qualora il Cliente abbia necessità di ricevere informazioni dal Responsabile (che non siano già in suo possesso) al fine di dimostrare il rispetto degli obblighi di cui all'art. 28 GDPR, in conseguenza di una richiesta ricevuta da parte dell'Autorità di Controllo, il Fornitore provvederà a rendere disponibili tali informazioni entro il termine imposto dall'Autorità. Resta inteso che, perché tale termine sia rispettato, la richiesta dovrà essere notificata tempestivamente al Responsabile della Protezione dei Dati (contattabile all'indirizzo mail sopra indicato) e allo stesso Fornitore.

6. MISURE DI SICUREZZA DEL CLIENTE

6.1. Fermi restando gli obblighi di cui al precedente punto 5 in capo al Fornitore, il Cliente riconosce e accetta che, nella fruizione dei Servizi, rimane responsabilità esclusiva del Cliente l'adozione di adeguate misure di sicurezza da parte del proprio personale e di coloro che sono autorizzati ad accedere a detti Servizi.
6.2. A tal fine, il Cliente si impegna ad utilizzare i Servizi e le funzionalità relative in modo da garantire un livello di protezione adeguato al rischio effettivo
6.3. Il Cliente si impegna altresì ad adottare tutte le misure idonee per proteggere le credenziali di autenticazione, i sistemi e i dispositivi utilizzati dal Cliente stesso o dai fruitori presso l'Utente Finale per accedere ai Servizi, e per effettuare i salvataggi e backup dei Dati Personali al fine di garantire il ripristino dei Dati Personali nel rispetto delle norme di legge.
6.4. Resta escluso qualsiasi obbligo o responsabilità in capo al Fornitore circa la protezione dei Dati Personali che il Cliente o l'Utente Finale, se applicabile, conservino o trasferiscano fuori dai sistemi utilizzati dal Fornitore e dai suoi Responsabili ulteriori del Trattamento (ad esempio, in archivi cartacei, o presso propri data center, come nel caso di Contratti aventi ad oggetto prodotti installati presso il Cliente o presso fornitori del Cliente).

7. VIOLAZIONI DI SICUREZZA

Il Fornitore, qualora venga a conoscenza di una Violazione di Sicurezza dei Dati Personali:
7.1. Informa senza ingiustificato ritardo e comunque non oltre 24 ore dalla conoscenza della violazione il Cliente mediante comunicazione inoltrata all'Indirizzo di notifica;
7.2. Adotta misure ragionevoli per limitare i prevedibili danni a carico degli interessati e la sicurezza dei Dati Personali;
7.3. Fornisce al Cliente una descrizione della Violazione di Sicurezza dei Dati Personali avvenuta e lo informa:

- della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati in questione);
- delle probabili conseguenze della violazione dei dati personali e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione, anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, il Responsabile comunica al Titolare le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo."

7.4. Considera come confidenziali le informazioni attinenti alle eventuali Violazioni della Sicurezza, i relativi documenti, comunicati e avvisi e non comunica a terzi dati o informazioni alle stesse attinenti senza il previo consenso scritto del Titolare, fuori dai casi strettamente necessari all'assolvimento di obblighi normativi (di qualunque genere) a carico del Cliente o dello stesso Fornitore, a richieste delle autorità competenti, all'assolvimento di obblighi contrattuali, alla mitigazione dei rischi ipotizzabili a carico degli interessati o ad attività strumentali relativamente alle predette finalità.

7.5. Il Cliente riconosce e accetta che è sua responsabilità esclusiva adempiere, in qualità di Titolare, nei casi previsti dalla Legislazione in materia di Trattamento di Dati Personali, agli eventuali obblighi di notificazione della Violazione di Sicurezza all'Autorità di controllo e agli interessati.

7.6. Resta inteso che la notificazione di una Violazione di Sicurezza o l'adozione di misure volte a gestire una Violazione di Sicurezza non costituisce riconoscimento di inadempimento o di responsabilità da parte del Fornitore in relazione a detta Violazione di Sicurezza

7.7. Il Cliente, in caso di Violazione di Sicurezza, dovrà comunicare tempestivamente al Fornitore eventuali utilizzi impropri degli account o delle credenziali di autenticazione, nonché eventuali usi non autorizzati riguardanti i Servizi da esso utilizzati e di cui abbia avuto conoscenza.

8. NOMINA ULTERIORI RESPONSABILI

8.1. Con il presente accordo il Titolare conferisce al Fornitore autorizzazione generale a ricorrere ad ulteriori responsabili del trattamento (c.d. Sub-Responsabili), nel rispetto di quanto prescritto dall'art. 28, par. 2 e 4 GDPR. Resta fermo che tale autorizzazione non si estende ai casi in cui il ricorso ad ulteriori responsabili comporti trasferimento dei dati al di fuori dell'Unione Europea o a organizzazioni internazionali, trasferimento che potrà avvenire solo al realizzarsi delle condizioni di cui al successivo paragrafo 9.

Il Responsabile si impegna espressamente ad informare il Titolare di eventuali modifiche riguardanti l'aggiunta o la sostituzione di eventuali Sub- responsabili del trattamento, dandogli così l'opportunità di opporsi a tali modifiche, e il Responsabile del Trattamento non potrà ricorrere ai Sub-responsabili in riferimento ai quali il Titolare abbia manifestato la sua opposizione.

8.2. Nel caso in cui il Responsabile utilizzi un Sub-responsabile per specifiche attività, a tale Sub-responsabile saranno imposte le medesime obbligazioni di cui al presente MDPA attraverso la stipula di un contratto o altro atto giuridico di valore equivalente nell'ordinamento italiano, assicurando sufficienti garanzie nell'adozione delle necessarie misure tecniche ed organizzative atte a garantire che il trattamento sia conforme alle disposizioni del GDPR.

8.3. Gli Ulteriori Responsabili sono conservati dal Responsabile in un apposito registro in formato digitale e consultabile dal Titolare anche da remoto su richiesta.

9. LIMITAZIONI AL TRASFERIMENTO DEI DATI PERSONALI AL DI FUORI DELLO SPAZIO ECONOMICO EUROPEO (SEE)

9.1. Il Fornitore custodisce e tratta i Dati Personali per i quali il Cliente riveste la qualità di Titolare all'interno dell'Unione Europea e non trasferisce i Dati personali al di fuori dello SEE salvo ricorrano le condizioni precisate all'art. 9.2.

9.2. Ove il Fornitore abbia intenzione di trasferire, anche ai fini della sola conservazione, i dati personali oggetto del presente accordo al di fuori dell'Unione Europea o ad Organizzazioni Internazionali, ne dà notizia al Cliente almeno 60 giorni prima. Il Cliente potrà, ove non acconsenta al trasferimento, recedere

dal contratto entro 15 giorni da tale comunicazione. Ove il Cliente non eserciti il proprio diritto di recesso nel suddetto termine, il Responsabile potrà effettuare il trasferimento dei dati di cui sopra nel rispetto delle condizioni di cui agli artt. 44 e ss. GDPR.

10. VERIFICHE E CONTROLLI

10.1. Il Fornitore sottopone ad audit periodici la sicurezza dei sistemi e degli ambienti di elaborazione dei Dati Personali dallo stesso utilizzati per l'erogazione dei Servizi e le sedi in cui avviene tale trattamento. Il Fornitore avrà la facoltà di incaricare dei professionisti indipendenti selezionati dal Fornitore stesso per lo svolgimento di audit secondo standard internazionali e/o best practice, i cui esiti saranno riportati in specifici report ("Report"). Tali Report, che costituiscono informazioni confidenziali del Fornitore, potranno essere resi disponibili al Cliente che ne faccia richiesta per consentirgli di verificare la conformità del Fornitore agli obblighi di sicurezza di cui al presente Accordo.
10.2. Il Cliente concorda che, nei casi di cui al punto 10.1, il proprio diritto di verifica sarà esercitato attraverso la verifica dei Report messi a disposizione dal Fornitore.
10.3. Il Fornitore riconosce il diritto del Cliente, con le modalità e nei limiti di seguito indicati, di effettuare audit indipendenti per valutare periodicamente le misure organizzative, tecniche e di sicurezza adottate dal Responsabile del trattamento nonché per verificare la conformità del Fornitore agli obblighi previsti nel presente Accordo nonché dalla normativa vigente in materia di trattamento di dati personali. Il Cliente potrà avvalersi per tali attività di proprio personale specializzato o di revisori esterni, purché tali soggetti siano previamente vincolati da idonei impegni alla riservatezza.
Con il presente accordo, il Cliente garantisce il rispetto della riservatezza da parte degli auditor incaricati.
10.4. Il Cliente dovrà previamente inviare richiesta scritta di verifica (audit) al Responsabile della Protezione dei Dati (DPO) del Fornitore tramite il recapito indicato nel presente accordo o, eventualmente, successivamente in sostituzione e contestualmente allo stesso Fornitore (ai recapiti indicati nel Contratto o successivamente comunicati in sostituzione degli stessi).
10.5. Il Fornitore potrà opporsi per iscritto alla nomina da parte del Cliente di eventuali revisori esterni che reputi non adeguatamente qualificati o indipendenti, che siano concorrenti del Fornitore o siano evidentemente inadeguati. Il fornitore dovrà sempre poter assistere, anche tramite proprio personale qualificato o revisori esterni dallo stesso nominati, alla conduzione delle attività di audit.
10.6. Resta inteso che gli audit di cui al presente punto potranno essere condotti solo relativamente agli ambiti coinvolti nei processi di trattamento dei dati per i quali il Cliente riveste la qualità di Titolare.
10.7. Il Cliente si impegna a tenere indenne il fornitore da eventuali costi che possano derivare dallo svolgimento dell'audit. Tali eventuali costi dovranno essere esaminati congiuntamente dalle parti in fase di pianificazione dell'audit stesso." Restano a carico esclusivo del Cliente i costi delle attività di verifica dallo stesso commissionate a terzi.
10.8. Il Fornitore ha nominato un Responsabile della Protezione dei Dati, che può essere contattato all'indirizzo mail: dpo@edisplay.it.
Il fornitore avrà cura di comunicare al Cliente l'eventuale variazione del dato di contatto indicato.

11. ASSISTENZA A FINI DI CONFORMITÀ

11.1. Il Fornitore, tenuto conto della natura dei Dati Personali trattati, si impegna ad assistere il Cliente nel garantire il rispetto degli obblighi di cui agli artt. 32-36 GDPR. In particolare, presterà assistenza al Cliente e coopererà nei modi di seguito indicati al fine di consentire al Cliente il rispetto degli obblighi previsti dalla Legislazione in materia di Protezione dei Dati Personali.
11.2. Il Fornitore provvederà a informare tempestivamente il Cliente, salvo il caso in cui ciò sia vietato dalla legge, con avviso all'Email di notifica di eventuali ispezioni o richieste di informazioni presentate da autorità di controllo e forze di polizia rispetto a profili che riguardano il trattamento dei Dati Personali.
11.3. Qualora, ai fini dell'evasione delle Richieste di cui ai precedenti punti, il Cliente abbia necessità di ricevere informazioni dal Fornitore circa il trattamento dei Dati Personali, il Fornitore presterà la necessaria assistenza fornendo le informazioni nella propria disponibilità.
11.4. Il Fornitore, tenuto conto della natura dei Dati Personali e delle informazioni ad esso disponibili,

fornirà assistenza al Cliente nel rendere disponibili informazioni utili per consentire al Cliente l'effettuazione di valutazioni di impatto sulla protezione dei Dati Personali nei casi previsti dalla legge. In tal caso il Fornitore renderà disponibili tutte le informazioni necessarie in base al Servizio e chiaramente richieste dal Cliente, quali le informazioni contenute nel Contratto, nel presente Accordo e in eventuali ulteriori DPA.
Eventuali richieste di assistenza personalizzate potranno essere soggette al pagamento di un corrispettivo da parte del Cliente. Resta inteso che è responsabilità e onere esclusivo del Cliente, o dell'Utente Finale se Titolare del trattamento, procedere ad eventuali necessarie/opportune Valutazioni d'Impatto (DPIA) relative al trattamento dei Dati Personali dallo stesso posto in essere nel contesto dei Servizi.

12. OBBLIGHI DEL CLIENTE E LIMITAZIONI

12.1. Il Cliente si impegna a impartire Istruzioni conformi alla normativa e a utilizzare i Servizi in modo conforme alla Legislazione in materia di Protezione dei Dati Personali e solo per trattare Dati Personali che siano stati raccolti in conformità alla Legislazione in materia di Protezione dei Dati Personali.
12.2. Il Cliente si impegna ad assolvere a tutti gli obblighi posti in capo al Titolare del Trattamento 12.3. È onere del Cliente mantenere l'account collegato all'Email di notifica attivo ed aggiornato.

13. DURATA, RESTITUZIONE CANCELLAZIONE DEI DATI PERSONALI

13.1. Il presente Accordo ha validità a partire dalla data di sottoscrizione del Contratto cui si riferisce e fino al momento in cui tutti i Dati Personali saranno cancellati dal Responsabile, sulla base delle statuizioni di cui al successivo punto 13.2
13.2. Al termine di scadenza del Contratto e/o in caso di scioglimento dello stesso, i Dati Personali di titolarità del Titolare detenuti dal Responsabile e le eventuali copie dei Dati stessi, comprensivi di quelli forniti dal Titolare tramite inserimento diretto nella piattaforma online del Fornitore, saranno conservati per un periodo di 6 mesi, in modo da essere ancora disponibili ove venga riattivato lo stesso Servizio nel periodo successivo alla scadenza e al fine di garantire l'esercizio del diritto di portabilità, salvo la sussistenza di un obbligo di legge o di regolamento nazionale e/o europeo che preveda la conservazione di tali Dati. Il Titolare potrà in ogni caso chiederne la cancellazione anticipata al termine o allo scioglimento del contratto nonché procedere personalmente alla cancellazione ove il servizio ne preveda la possibilità (es: Emailchef).
13.3. La conservazione per i 6 mesi successivi alla conclusione del rapporto non viene garantita e non forma oggetto di pretesa alcuna da parte del Titolare, una volta che sia stato esercitato il diritto di portabilità. Decorso tale termine i dati saranno cancellati e non ne sarà conservata copia, salvo che la conservazione si renda necessaria in base ad un obbligo normativo. In tal caso, i dati verranno conservati per il periodo prescritto dalla singola disposizione. Saranno inoltre conservati, fino alla decorrenza del relativo termine di prescrizione, eventuali dati necessari all'accertamento, esercizio o difesa di un diritto in sede giudiziaria.

14. RESPONSABILITA'

14.1. Ciascuna Parte è responsabile per l'adempimento dei propri obblighi previsti dal presente Accordo

15. CATEGORIE DI DATI INTERESSATI

15.1. Possono essere trattati dati personali che il Cliente abbia fornito al Responsabile, anche tramite archiviazione, ad opera del Cliente, direttamente su portale del Fornitore ai fini della fruizione dei servizi prescelti.
15.2. Tipicamente, vengono trattati dati personali comuni come: dati anagrafici, dati di contatto o indicanti l'attività lavorativa svolta, dati bancari.
15.3. I suddetti dati fanno riferimento, principalmente, alle seguenti categorie di interessati: clienti e

potenziali clienti, fornitori, personale impiegato e collaboratori.
15.4. Possono essere trattati dati ulteriori e finanche dati particolari (es. dati relativi alla salute), anche riferiti ad altri soggetti individuati dal Titolare il quale abbia verificato la sussistenza di idonea base giuridica e delle altre condizioni necessarie per la liceità del trattamento e la sua conformità al GDPR
15.5. Il Cliente si impegna a non comunicare in alcun modo al Fornitore dati personali rispetto ai quali non possa garantire che il trattamento sia lecito e, in generale, conforme al GDPR in ottemperanza al principio di Accountability e alle responsabilità che, in base a tale principio, sono a carico del Titolare.

16. CORRISPETTIVO

16.1. Il corrispettivo pattuito nel Contratto include le prestazioni inerenti alla qualifica di Responsabile.

17. LEGGE APPLICABILE E FORO COMPETENTE

17.1. Il presente Accordo è regolato dalla legge italiana.
17.2. Qualunque controversia dovesse insorgere con riferimento all'esecuzione, interpretazione e/o applicazione del presente Accordo, sarà di esclusiva competenza del foro di Nuoro.

18. VALIDITA' DEL PRESENTE ACCORDO E MODIFICHE

18.1. Le disposizioni di cui al presente accordo sostituiscono e prevalgono su qualsiasi disposizione contrattuale o di altro genere eventualmente stipulata tra le parti sulla stessa materia.
Ove il Fornitore ritenga di apportare una o più modifiche al presente accordo, ne darà al Cliente comunicazione in forma scritta, anche con strumenti elettronici (e-mail, PEC). Il Cliente potrà, in tal caso, ove non ritenga di accettare le modifiche apportate, recedere dal Contratto entro 60 giorni dal ricevimento di tale comunicazione. Il recesso dovrà essere comunicato in forma scritta a mezzo raccomandata A/R o tramite PEC. In mancanza, le modifiche apportate si intenderanno accettate e vincolanti per entrambe le parti.

19. COMUNICAZIONI E NOTIFICHE

19.1. Ogni comunicazione fra le parti inerente al Trattamento dei dati Personali dovrà avvenire agli indirizzi comunicati in sede di stipula del contratto o eventualmente successivamente comunicati in sostituzione.

Fonni, 27.05.2021

IL RESPONSABILE DEL TRATTAMENTO
eDisplay srl

IL LEGALE RAPPRESENTANTE
Raffaele Serusi

MISURE TECNICO-ORGANIZZATIVE (allegato 1)

In aggiunta alle misure di sicurezza previste nel Contratto e nel MDPA il Responsabile del Trattamento applica le seguenti misure di sicurezza organizzative a seconda della tipologia di Servizio con cui viene erogato o licenziato il prodotto:
A – Cloud SaaS

Misure di sicurezza organizzative	**Policy e Disciplinari utenti** – Il Fornitore applica dettagliate policy e disciplinari, ai quali tutta l'utenza con accesso ai sistemi informativi ha l'obbligo di conformarsi e che sono finalizzate a garantire comportamenti idonei ad assicurare il rispetto dei principi di riservatezza, disponibilità ed integrità dei dati nell'utilizzo delle risorse informatiche. **Autorizzazione accessi logici –** il Fornitore definisce i profili di accesso nel rispetto del least privilege necessari all'esecuzione delle mansioni assegnate. I profili di autorizzazione sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. Tali profili sono oggetto di controlli periodici finalizzati alla verifica della sussistenza delle condizioni per la conservazione dei profili attribuiti. **Gestione interventi di assistenza** – Gli interventi di assistenza sono regolamentati allo scopo di garantire l'esecuzione delle sole attività previste contrattualmente e impedire il trattamento eccessivo di dati personali la cui titolarità è in capo al Cliente o all'Utente Finale. **Valutazione d'impatto sulla protezione dei dati (DPIA)** – In conformità agli artt. 35 e 36 del GDPR e sulla base del documento WP248 – Linee guida sulla valutazione d'impatto nella protezione dei dati adottate dal Gruppo di lavoro ex art. 29, il Fornitore ha predisposto una propria metodologia per l'analisi e la valutazione dei trattamenti che, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, presentino un rischio elevato per i diritti e le libertà delle persone fisiche allo scopo di procedere con la valutazione dell'impatto sulla protezione dei dati personali prima di iniziare il trattamento. **Incident Management** – Il Fornitore ha realizzato una specifica procedura di Incident Management allo scopo di garantire il ripristino delle normali operazioni di servizio nel più breve tempo possibile, garantendo il mantenimento dei livelli migliori di servizio. **Data Breach** – Il Fornitore ha implementato un'apposita procedura finalizzata alla gestione degli eventi e degli incidenti con un potenziale impatto sui dati personali che definisce ruoli e responsabilità, il processo di rilevazione (presunto o accertato), l'applicazione delle azioni di contrasto, la risposta e il contenimento dell'incidente / violazione nonché le modalità attraverso le quali effettuare le comunicazioni delle violazioni di dati personali al Cliente. **Formazione**: Il Fornitore eroga periodicamente ai propri dipendenti coinvolti nelle attività di trattamento corsi di formazione sulla corretta gestione dei dati personali
Misure di sicurezza tecniche	**Firewall, IDPS** - I dati personali sono protetti contro il rischio d'intrusione di cui all'art. 615-quinquies del codice penale mediante sistemi di Intrusion Detection & Prevention, mantenuti aggiornati in relazione alle migliori tecnologie disponibili. **Sicurezza linee di comunicazione**- Per quanto di propria competenza, sono adottati dal Fornitore protocolli di comunicazione sicuri e in linea con quanto la tecnologia rende disponibile. **Protection from malware**– I sistemi sono protetti contro il rischio di intrusione

Misure di sicurezza tecniche	e dell'azione di programmi mediante l'attivazione di idonei strumenti elettronici aggiornati con cadenza periodica. Sono in uso strumenti antivirus mantenuti costantemente aggiornati. **Credenziali di autenticazione** – I sistemi sono configurati con modalità idonee a consentirne l'accesso unicamente a soggetti dotati di credenziali di autenticazione che ne consentono la loro univoca identificazione. Fra questi, codice associato a una parola chiave, riservata e conosciuta unicamente dallo stesso; dispositivo di autenticazione in possesso e uso esclusivo dell'utente, eventualmente associato a un codice identificativo o a una parola chiave. **Parola chiave** – Relativamente alle caratteristiche di base ovvero obbligo di modifica al primo accesso, lunghezza minima, assenza di elementi riconducibili agevolmente al soggetto, regole di complessità, scadenza, history, valutazione contestuale della robustezza, visualizzazione e archiviazione, la parola chiave è gestita conformemente alle best practice. Ai soggetti ai quali sono attribuite le credenziali sono fornite puntuali istruzioni in relazione alle modalità da adottare per assicurarne la segretezza. **Logging –** I sistemi sono configurabili con modalità che consentono il tracciamento degli accessi e, ove appropriato, delle attività svolte in capo alle diverse tipologie di utenze (Amministratore, Super Utente, etc.) protetti da adeguate misure di sicurezza che ne garantiscono l'integrità. **Backup & Restore** – Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati. Ove gli accordi contrattuali lo prevedono è posto in uso un piano di continuità operativo integrato, ove necessario, con il piano di disaster recovery; essi garantiscono la disponibilità e l'accesso ai sistemi anche nel caso di eventi negativi di portata rilevante che dovessero perdurare nel tempo. **Vulnerability Assessment & Penetration Test** – Il Fornitore effettua periodicamente attività di analisi delle vulnerabilità finalizzate a rilevare lo stato di esposizione alle vulnerabilità note, sia in relazione agli ambiti infrastrutturali sia a quelli applicativi, considerando i sistemi in esercizio o in fase di sviluppo. Ove ritenuto appropriato in relazione ai potenziali rischi identificati, tali verifiche sono integrate periodicamente con apposite tecniche di Penetration Test, mediante simulazioni di intrusione che utilizzano diversi scenari di attacco, con l'obiettivo di verificare il livello di sicurezza di applicazioni/sistemi/reti attraverso attività che mirano a sfruttare le vulnerabilità rilevate per eludere i meccanismi di sicurezza fisica/logica ed avere accesso agli stessi. I risultati delle verifiche sono puntualmente e dettagliatamente esaminati per identificare e porre in essere i punti di miglioramento necessari a garantire l'elevato livello di sicurezza richiesto. **Amministratori di Sistema** – Relativamente a tutti gli utenti che operano in qualità di Amministratori di Sistema, il cui elenco è mantenuto aggiornato e le cui funzioni attribuite sono opportunamente definite in appositi atti di nomina, è gestito un sistema di log management finalizzato al puntuale tracciamento delle attività svolte ed alla conservazione di tali dati con modalità inalterabili idonee a consentirne ex post il monitoraggio. L'operato degli Amministratori di Sistema è sottoposto ad attività di verifica in modo da controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previsti dalle norme vigenti. **Data Center** – L'accesso fisico al Data Center è limitato ai soli soggetti autorizzati. Per il dettaglio delle misure di sicurezza adottate con riferimento ai servizi di data center erogati dai Responsabili Ulteriori del Trattamento, così come individuati nei MDPA Condizioni Speciali, si fa rinvio alle misure di sicurezza indicate descritte dai medesimi Responsabili Ulteriori e rese disponibili nei

Misure di sicurezza tecniche	relativi siti istituzionali ai seguenti indirizzi (o a quelli che saranno successivamente resi disponibili dai Responsabili Ulteriori): **Per i servizi di Data Center erogati da Amazon Web Services**: https://aws.amazon.com/it/compliance/data-center/controls/ Per i servizi di Data Center erogati da Microsoft: https://www.microsoft.com/en-us/trustcenter **Protection from malware VM** – Le VM sono protette contro il rischio di intrusione e dell'azione di programmi mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza periodica. Tutte le VM sono gestite tramite funzionalità antivirus (sia a livello hypervisor che infrastrutturale). **Backup & Restore** – Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati.
	Alta affidabilità – il Fornitore garantisce l'alta affidabilità nei seguenti termini: • L'architettura Server è basata sull'utilizzo della soluzione di virtualizzazione VMWare applicata mediante duplicazione fisica e virtuale dei singoli sistemi, al fine di garantire la tolleranza ai guasti e l'eliminazione dei single point of failure. In particolare in caso di failure di un sistema, il software di gestione dell'ambiente virtuale è in grado di ridistribuire le attività in corso verso gli altri sistemi (high availabilty e load balancing), riducendo al minimo i disservizi e garantendo la persistenza delle connessioni esistenti. • Ciascun Server è attestato su una SAN mediante connessione iSCSI ad alta velocità. • Tutte le componenti dell'infrastruttura, sono completamente ridondate per eliminare ogni single point of failure. • L'architettura di rete è progettata per proteggere i sistemi di frontend da Internet e dalle reti interne mediante l'utilizzo di una DMZ protetta da due livelli di firewalling distinti (defense-in-depth): un firewall di frontiera connesso ad Internet ed un secondo firewall, che integra anche funzionalità di Intrusion Prevention e antimalware, di proprietà dell'organizzazione, è messo a protezione della DMZ e dei sistemi di backend. Tutti gli allarmi sono remotizzati al presidio di vigilanza.