DATA PROCESSING AGREEMENT (DPA)

Accordo sul trattamento dei dati personali ai sensi dell'art. 28 del Regolamento (UE) 2016/679
Versione: 1.00

TRA

Ikonika S.r.l., con sede legale in Via Armando Diaz 59 p.iva 04354060610, quale Responsabile del trattamento (ovvero Sub-Responsabile, a seconda del ruolo in cui opera ai sensi delle Premesse), di seguito "Responsabile";

E

il cliente o committente che, nell'ambito del contratto principale, affida al Responsabile i trattamenti oggetto del presente DPA, agendo quale titolare del trattamento ovvero quale responsabile del trattamento per conto di un terzo titolare, come precisato nelle Premesse, di seguito "Titolare".

Il Titolare e il Responsabile sono congiuntamente indicati come le "Parti" e singolarmente come la "Parte".

PREMESSE

Il titolare del trattamento determina le finalità e i mezzi essenziali dei trattamenti descritti nel presente DPA e (direttamente o per il tramite del Titolare) affida al Responsabile attività di trattamento necessarie all'esecuzione dei servizi contrattuali.

Il Responsabile eroga i propri servizi a clienti che, rispetto ai dati personali trattati mediante tali servizi, possono operare in uno dei due ruoli seguenti, ai quali corrisponde la qualifica assunta dal Responsabile ai sensi del GDPR:

(a) Ruolo di Responsabile: il cliente è titolare del trattamento e nomina Ikonika S.r.l. responsabile del trattamento ai sensi dell'art. 28, paragrafi 1 e 3, del GDPR;

(b) Ruolo di Sub-Responsabile: il cliente è a sua volta responsabile del trattamento per conto di un terzo titolare (il "Titolare Finale") e nomina Ikonika S.r.l. sub-responsabile ai sensi dell'art. 28, paragrafi 2 e 4, del GDPR, sulla base dell'autorizzazione del Titolare Finale.

Il ruolo applicabile è quello indicato nel contratto principale o nel modulo di attivazione dei servizi o, in mancanza, comunicato per iscritto dal cliente prima dell'avvio del trattamento; in assenza di indicazioni, il cliente dichiara e garantisce di agire quale titolare del trattamento. Il presente DPA si applica a entrambi i ruoli. Nel Ruolo di Sub-Responsabile il termine "Titolare" designa il cliente nella sua qualità di soggetto che impartisce le istruzioni al Responsabile, fermo restando quanto previsto dall'Art. 1.5.

Il Responsabile dichiara di possedere garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate e si impegna a trattare i dati personali esclusivamente per conto del Titolare e secondo istruzioni documentate.

I servizi comprendono apposizione di firma elettronica, archiviazione dei dati in cloud, archiviazione documentale, conservazione digitale e backup cloud, nonché, ove il Titolare lo abiliti, l'identificazione del firmatario mediante verifica del documento di identità e dei dati biometrici, anche con l'ausilio di sistemi di intelligenza artificiale forniti da sub-responsabili.

Il presente DPA integra il contratto principale e costituisce il contratto o altro atto giuridico scritto, anche in formato elettronico, richiesto dall'art. 28, paragrafi 3 e 9, del GDPR. Il DPA è pubblicato all'URL indicato nel contratto principale ed è richiamato mediante collegamento ipertestuale, senza necessità di un documento separato o di una sottoscrizione autonoma. In caso di contrasto, prevalgono le disposizioni del presente DPA limitatamente alla materia della protezione dei dati personali, salvo diversa pattuizione documentata e validamente accettata dalle Parti.

Le premesse e gli allegati costituiscono parte integrante del presente DPA.

Art. 1 — Definizioni e ambito

1.1. Ai fini del presente DPA, i termini "dato personale", "trattamento", "violazione dei dati personali", "dati relativi alla salute", "dati biometrici", "categorie particolari di dati" e "autorità di controllo" hanno il significato loro attribuito dal GDPR. I termini "Titolare", "Titolare Finale", "Responsabile", "Ruolo di Responsabile" e "Ruolo di Sub-Responsabile" hanno il significato indicato nell'intestazione e nelle Premesse; il termine "Responsabile" designa Ikonika S.r.l. in entrambi i ruoli, mentre il termine "sub-responsabile" indica i soggetti di cui il Responsabile si avvale per il trattamento ai sensi dell'Art. 7.

1.2. Il DPA si applica a ogni trattamento effettuato dal Responsabile per conto del Titolare nell'ambito dei servizi indicati nell'Allegato 1, compresi i trattamenti eseguiti mediante infrastrutture cloud, sistemi di firma, sistemi di conservazione, copie di sicurezza, assistenza tecnica e gestione degli accessi.

1.3. Il DPA non attribuisce al Responsabile alcun diritto di utilizzare i dati per finalità proprie, di marketing, profilazione, analisi commerciale, addestramento di modelli o sviluppo di prodotti, salvo previa istruzione documentata e separata del Titolare che individui la diversa titolarità o base giuridica.

1.4. Il Responsabile opera, a seconda del cliente e del servizio, nel Ruolo di Responsabile o nel Ruolo di Sub-Responsabile indicati nelle Premesse. In entrambi i ruoli il Responsabile tratta i dati esclusivamente per conto e secondo le istruzioni documentate del titolare del trattamento, trasmesse direttamente o per il tramite del Titolare, e non determina finalità e mezzi essenziali del trattamento.

1.5. Nel Ruolo di Sub-Responsabile valgono inoltre le seguenti regole:

(a) il Titolare dichiara e garantisce di agire sulla base di un valido atto di nomina del Titolare Finale, di essere stato autorizzato da quest'ultimo a ricorrere al Responsabile e ai sub-responsabili di cui all'Art. 7, anche con riguardo ai trasferimenti di cui all'Art. 12, e di impartire istruzioni conformi a quelle del Titolare Finale;

(b) eventuali obblighi ulteriori o più gravosi imposti al Titolare dal Titolare Finale vincolano il Responsabile solo se comunicati per iscritto prima dell'avvio del trattamento e da questo accettati;

(c) le comunicazioni, le richieste e gli adempimenti previsti dal presente DPA (istruzioni, richieste degli interessati, violazioni dei dati personali, sub-responsabili, audit, restituzione e cancellazione) sono indirizzati al Titolare, che li inoltra senza ritardo al Titolare Finale; i termini a carico del Titolare per opporsi o rispondere sono commisurati ai tempi di tale inoltro; i diritti di istruzione, opposizione e verifica del Titolare Finale sono esercitati per il tramite del Titolare, fermo restando che il Responsabile può interagire direttamente con il Titolare Finale quando richiesto dalla legge o dal Titolare;

(d) il Titolare risponde verso il Titolare Finale ai sensi dell'art. 28, paragrafo 4, del GDPR, senza pregiudizio per la responsabilità del Responsabile verso il Titolare ai sensi dell'Art. 14.

1.6. Il Responsabile agisce quale autonomo titolare del trattamento, secondo la propria informativa, limitatamente ai dati personali del Titolare e dei suoi referenti necessari alla gestione del rapporto contrattuale, alla fatturazione, alla sicurezza dei propri sistemi e all'adempimento di obblighi di legge, che non rientrano nell'oggetto del presente DPA.

Art. 2 — Oggetto, durata e documentazione del trattamento

2.1. Il Responsabile tratta i dati esclusivamente per fornire i servizi contrattuali e per le operazioni descritte nell'Allegato 1. L'oggetto, la durata, la natura e la finalità del trattamento, le categorie di dati e le categorie di interessati sono specificati nell'Allegato 1.

2.2. Il DPA produce effetti dalla data di efficacia del contratto principale o dall'attivazione dei servizi, secondo quanto previsto dal contratto principale, e resta efficace per tutta la durata del rapporto e, comunque, fino alla restituzione o cancellazione dei dati, salvo il periodo durante il quale il Responsabile sia tenuto a conservarli per legge. La conservazione obbligatoria non autorizza ulteriori trattamenti per finalità diverse da quelle imposte dalla legge.

2.3. Le Parti completano e aggiornano l'Allegato 1 prima dell'avvio di ogni nuovo trattamento o servizio che modifichi in modo sostanziale l'oggetto, le categorie di dati, gli interessati, i destinatari o la localizzazione dei dati.

Art. 3 — Istruzioni documentate e limiti del trattamento

3.1. Il Responsabile tratta i dati soltanto sulla base delle istruzioni documentate del Titolare, contenute nel presente DPA, negli Allegati, nel contratto principale e nelle successive istruzioni scritte trasmesse tramite i recapiti concordati.

3.2. Le istruzioni comprendono: raccolta o ricezione, registrazione, organizzazione, conservazione, consultazione, confronto, aggiornamento, rettifica, recupero, backup, restituzione e cancellazione, nei limiti necessari per i servizi affidati.

3.3. Il Responsabile non vende, comunica, diffonde, combina, arricchisce o riutilizza i dati per finalità proprie. Non può determinare autonomamente finalità o mezzi essenziali del trattamento; può scegliere i mezzi tecnici non essenziali più idonei, purché coerenti con le istruzioni e con il livello di sicurezza concordato.

3.4. Se ritiene che un'istruzione violi il GDPR o altra disposizione applicabile in materia di protezione dei dati, il Responsabile informa immediatamente il Titolare e sospende l'esecuzione dell'istruzione contestata, salvo diverso obbligo di legge.

3.5. Il presente DPA è pubblicato in una pagina identificata da un codice di versione e da una data di pubblicazione. Il contratto principale rinvia al collegamento della versione applicabile; il Responsabile conserva uno storico delle versioni pubblicate. La mera pubblicazione sul sito di una modifica sostanziale non sostituisce la comunicazione al Titolare né determina, da sola, l'applicazione della modifica ai rapporti già in essere. Le modifiche sostanziali diventano applicabili solo secondo le modalità previste dal contratto principale o mediante accordo documentato tra le Parti.

3.6. Qualora i servizi o le funzionalità abilitate dal Titolare comprendano sistemi di intelligenza artificiale (ad esempio per l'acquisizione e la verifica del documento di identità, il confronto biometrico uno-a-uno e la verifica di presenza dal vivo del firmatario), il Responsabile: (a) non utilizza i dati, né consente ai sub-responsabili di utilizzarli, per addestrare, affinare, validare o migliorare modelli propri o di terzi; (b) non impiega funzionalità di riconoscimento delle emozioni né di categorizzazione biometrica degli interessati; (c) non adotta decisioni fondate unicamente sul trattamento automatizzato che producano effetti giuridici o incidano in modo analogo significativamente sugli interessati, e rende possibile l'intervento umano su richiesta del Titolare; (d) fornisce al Titolare, su richiesta, le informazioni ragionevolmente necessarie per l'informativa agli interessati, per la valutazione d'impatto e per gli adempimenti del Regolamento (UE) 2024/1689 che gli competono; (e) informa il Titolare con congruo preavviso delle modifiche sostanziali dei modelli o dei fornitori di tali sistemi che possano incidere sui rischi per gli interessati.

Art. 4 — Obblighi del Titolare

- determinare finalità, basi giuridiche, categorie di dati e tempi di conservazione dei trattamenti;
- fornire istruzioni lecite, documentate e sufficientemente determinate;
- fornire al Responsabile i dati necessari e assicurare, per quanto di propria competenza, la correttezza, pertinenza e liceità dei dati e delle istruzioni;
- informare gli interessati e gestire i rapporti con gli interessati e con l'autorità di controllo, con l'assistenza del Responsabile quando necessaria;
- valutare, ove applicabile, la necessità di una valutazione d'impatto e consultare preventivamente l'autorità di controllo nei casi previsti;
- indicare nell'Allegato 1 le categorie effettive di dati e interessati, le localizzazioni autorizzate e le regole di conservazione.;
- ove operi nel Ruolo di Sub-Responsabile, assicurare le garanzie e le autorizzazioni del Titolare Finale previste dall'Art. 1.5;
- individuare la base giuridica e, per le categorie particolari di dati (compresi i dati biometrici trattati mediante la funzionalità di identificazione del firmatario), la condizione prevista dall'art. 9, paragrafo 2, del GDPR, e fornire agli interessati l'informativa, anche in merito all'uso di sistemi di verifica biometrica e di intelligenza artificiale, ove abilitati.

Art. 5 — Persone autorizzate e riservatezza

5.1. Il Responsabile autorizza al trattamento soltanto persone che abbiano effettiva necessità di accedere ai dati per svolgere le attività affidate, siano state adeguatamente istruite e siano vincolate alla riservatezza mediante obbligo contrattuale o legale.

5.2. Il Responsabile mantiene evidenza delle autorizzazioni e degli ambiti di accesso, revoca o modifica tempestivamente gli accessi non più necessari e assicura una formazione proporzionata alle mansioni e ai rischi del trattamento.

5.3. Gli obblighi di riservatezza restano efficaci anche dopo la cessazione del rapporto, senza pregiudizio per gli obblighi di conservazione imposti dalla legge.

Art. 6 — Misure tecniche e organizzative

6.1. Il Responsabile adotta e mantiene misure tecniche e organizzative adeguate al rischio, tenendo conto dello stato dell'arte, dei costi, della natura, dell'oggetto, del contesto e delle finalità del trattamento. Le misure minime concordate sono descritte nell'Allegato 2.

6.2. Le misure comprendono, in funzione del rischio e della natura dei servizi: controllo degli accessi secondo il principio del minimo privilegio; autenticazione robusta e, ove disponibile, autenticazione a più fattori per accessi amministrativi o remoti; segregazione degli ambienti; cifratura in transito e a riposo ove appropriata; registrazione e monitoraggio degli accessi; gestione

delle vulnerabilità; backup e ripristino; continuità operativa; gestione degli incidenti; test periodici; formazione e gestione sicura della cancellazione.

6.3. Per i servizi di firma elettronica e conservazione digitale, il Responsabile applica anche i requisiti tecnici e organizzativi applicabili al servizio fiduciario o di conservazione concretamente prestato, senza che tali requisiti sostituiscano gli obblighi del GDPR.

6.4. Il Responsabile documenta le misure adottate e comunica al Titolare ogni modifica sostanziale che possa ridurre il livello di protezione o incidere sulle localizzazioni e sui sub-responsabili.

Art. 7 — Sub-responsabili

7.1. Il Titolare autorizza in via generale il ricorso ai sub-responsabili. L'elenco aggiornato dei sub-responsabili e le relative informazioni devono essere mantenuti disponibili dal Responsabile e comunicati secondo quanto previsto dal presente articolo. L'elenco non è reso pubblico sul sito web per ragioni di riservatezza, ma è disponibile per il Titolare su richiesta scritta (e, in ogni caso, trasmesso al Titolare all'attivazione dei servizi e ad ogni suo aggiornamento) da inviare tramite pec all'indirizzo ikonika.srl@legalmail.it

7.2. Il Responsabile informa il Titolare per iscritto con almeno 15 giorni lavorativi di preavviso dell'aggiunta o sostituzione di un sub-responsabile, indicando identità, sede, attività affidata, localizzazione dei dati e garanzie tecniche e organizzative. Il Titolare può opporsi per motivi documentati connessi alla protezione dei dati. In caso di opposizione le Parti si confrontano in buona fede per individuare una soluzione alternativa; se questa non è possibile entro un termine ragionevole, il Titolare può recedere dal solo servizio interessato senza penali, con rimborso pro rata di quanto eventualmente prepagato per il periodo successivo. Il Responsabile può sostituire un sub-responsabile con preavviso ridotto o successivo, informandone immediatamente il Titolare, quando ciò sia necessario per ragioni urgenti di sicurezza o di continuità del servizio; resta fermo il diritto di opposizione.

7.3. Il Responsabile impone al sub-responsabile, mediante accordo scritto, obblighi in materia di protezione dei dati non meno protettivi di quelli previsti dal presente DPA, in modo da assicurare gli stessi obblighi di cui all'art. 28, paragrafo 4, del GDPR, in particolare su istruzioni, riservatezza, sicurezza, data breach, assistenza, audit, cancellazione e trasferimenti internazionali, nonché il divieto di utilizzare i dati per finalità proprie, incluso l'addestramento di modelli di intelligenza artificiale.

7.4. Il Responsabile resta pienamente responsabile verso il Titolare dell'adempimento degli obblighi del sub-responsabile. Qualora il sub-responsabile non presti più garanzie sufficienti, il Responsabile ne sospende l'utilizzo e propone una soluzione alternativa.

Art. 8 — Richieste degli interessati e assistenza

8.1. Il Responsabile non risponde autonomamente alle richieste degli interessati relative ai dati trattati per conto del Titolare, salvo istruzione espressa o obbligo di legge. Se riceve una richiesta, la inoltra al Titolare senza ingiustificato ritardo e comunque entro 2 giorni lavorativi, senza alterarne il contenuto.

8.2. Tenendo conto della natura del trattamento e delle informazioni disponibili, il Responsabile assiste il Titolare con misure tecniche e organizzative adeguate per rispondere alle richieste di accesso, rettifica, cancellazione, limitazione, portabilità e opposizione.

8.3. Il Responsabile assiste il Titolare, per quanto applicabile, nella sicurezza del trattamento, nella gestione delle violazioni, nelle valutazioni d'impatto, nelle consultazioni preventive e nella dimostrazione della conformità.

Art. 9 — Violazioni dei dati personali e incidenti

9.1. Il Responsabile informa il Titolare di ogni violazione dei dati personali, anche solo sospetta, senza ingiustificato ritardo e, ove tecnicamente possibile, entro 24 ore dalla conoscenza dell'evento. Il termine è un obbligo di comunicazione interna tra le Parti e non sostituisce gli eventuali termini applicabili nei rapporti con l'autorità di controllo o con gli interessati.

9.2. La comunicazione contiene, nella misura delle informazioni disponibili: natura dell'evento; data e ora di rilevazione e, se nota, di accadimento; sistemi e dati coinvolti; categorie e numero approssimativo di interessati e registrazioni; conseguenze probabili; misure adottate o proposte; referente per gli aggiornamenti.

9.3. Se le informazioni non sono disponibili subito, il Responsabile le comunica progressivamente senza ingiustificato ritardo e mantiene un registro degli incidenti e delle decisioni assunte. Il Responsabile collabora con il Titolare nelle analisi, nel contenimento, nel ripristino e nelle comunicazioni eventualmente necessarie.

9.4. Per i servizi fiduciari o di firma elettronica, il Responsabile assicura anche gli adempimenti di sicurezza e comunicazione verso gli organismi competenti che gli siano applicabili in relazione al servizio prestato.

Art. 10 — Registri, autorità e cooperazione

10.1. Il Responsabile tiene, ove applicabile, il registro delle categorie di attività di trattamento svolte per conto del Titolare e lo mette a disposizione nella parte pertinente.

10.2. Il Responsabile informa tempestivamente il Titolare di richieste, ispezioni o provvedimenti dell'autorità di controllo relativi ai trattamenti oggetto del DPA, salvo divieto di legge, e coopera con il Titolare per fornire riscontri accurati.

10.3. Il Responsabile rende disponibili le informazioni necessarie a dimostrare il rispetto degli obblighi del presente DPA e delle disposizioni applicabili, incluse descrizioni aggiornate delle misure, attestazioni o report di audit pertinenti e informazioni sui sub-responsabili.

Art. 11 — Audit e verifiche

11.1. Il Titolare può effettuare verifiche documentali e, ove necessario, ispezioni presso il Responsabile, nei limiti dei diritti di cui il Responsabile dispone nei confronti dei sub-responsabili, presso questi ultimi o mediante i report di audit indipendenti da essi resi disponibili, direttamente o tramite un auditor vincolato alla riservatezza, con preavviso ordinario di almeno 7 giorni lavorativi.

11.2. Il preavviso non è necessario o può essere ridotto in caso di violazione, incidente grave, richiesta dell'autorità o ragionevole rischio per i dati. Le verifiche sono svolte durante l'orario lavorativo, con modalità proporzionate e senza compromettere la sicurezza o la continuità dei servizi.

11.3. Il Responsabile coopera agli audit, mette a disposizione documentazione e personale pertinenti e rimuove tempestivamente le non conformità rilevate. Se una verifica riguarda la conservazione digitale, può comprendere la documentazione e i controlli specifici del servizio di conservazione, nei limiti pertinenti alla protezione dei dati personali.

11.4. I costi ragionevoli di un audit straordinario richiesto dal Titolare per una non conformità imputabile al Responsabile restano a carico del Responsabile; negli altri casi, le Parti concordano preventivamente la ripartizione dei costi.

Art. 12 — Trasferimenti internazionali

12.1. Il Responsabile tratta i dati nelle localizzazioni indicate nell'Allegato 1. Non effettua trasferimenti verso Paesi terzi o organizzazioni internazionali, né consente accessi da tali luoghi, senza previa istruzione documentata del Titolare e senza che siano soddisfatte le condizioni del Capo V GDPR.

12.2. Prima di introdurre un trasferimento extra SEE, il Responsabile comunica al Titolare Paese, destinatario, finalità, categorie di dati, modalità di accesso, meccanismo di trasferimento, valutazione delle garanzie e, ove necessario, misure supplementari. Il trasferimento non può iniziare prima della verifica e documentazione della base giuridica applicabile.

12.3. Il Responsabile informa il Titolare se una disposizione cui è soggetto gli impone di trasferire o divulgare i dati, salvo divieto di legge, e coopera per valutare la legittimità della richiesta e le misure di tutela.

12.4. L'abilitazione da parte del Titolare di funzionalità che, come indicato nell'Allegato 1, comportano il trattamento da parte di un sub-responsabile con sede in un Paese terzo o accessi da un Paese terzo costituisce istruzione documentata ai sensi dell'Art. 12.1, a condizione che il Responsabile abbia comunicato al Titolare le informazioni di cui all'Art. 12.2. Il trasferimento è effettuato sulla base di una decisione di adeguatezza o, in mancanza, delle garanzie adeguate di cui all'art. 46 del GDPR (in particolare le clausole contrattuali tipo adottate con Decisione di esecuzione (UE) 2021/914), previa valutazione d'impatto del trasferimento ed eventuali misure supplementari; il Responsabile non si avvale delle deroghe dell'art. 49 del GDPR e fornisce al Titolare, su richiesta, copia delle clausole applicate e una sintesi della valutazione.

Art. 13 — Restituzione, cancellazione e conservazione

13.1. Alla cessazione dei servizi, il Titolare sceglie se ricevere la restituzione dei dati in formato strutturato e comunemente utilizzato, se tecnicamente applicabile, oppure richiedere la cancellazione. In assenza di istruzione diversa, il Responsabile cancella i dati entro 30 giorni dalla cessazione, previo avviso al Titolare, salvo i tempi tecnici concordati nell'Allegato 1. I dati presenti nelle copie di backup sono cancellati secondo il ciclo di rotazione, entro i termini indicati nell'Allegato 1.

13.2. Il Responsabile cancella le copie esistenti e chiede ai sub-responsabili di fare altrettanto, salvo che la conservazione sia imposta dal diritto dell'Unione o dello Stato membro. In tal caso, i dati sono isolati, protetti e trattati esclusivamente per tale obbligo.

13.3. Su richiesta, il Responsabile rilascia entro 10 giorni lavorativi una dichiarazione di avvenuta restituzione e/o cancellazione, indicando eventuali dati conservati per legge e il relativo termine di cancellazione.

Art. 14 — Responsabilità e rapporto con il contratto principale

14.1. Ciascuna Parte risponde degli obblighi ad essa attribuiti dal GDPR, dal presente DPA e dalla normativa applicabile. Il Responsabile risponde verso il Titolare per i trattamenti effettuati in violazione delle istruzioni lecite o degli obblighi direttamente applicabili al Responsabile, nonché per l'operato dei sub-responsabili nei limiti previsti dal GDPR.

14.2. Le previsioni economiche, le limitazioni di responsabilità, le assicurazioni e le regole di gestione delle controversie restano disciplinate dal contratto principale, salvo disposizioni inderogabili del GDPR o di altra normativa applicabile. Nessuna limitazione di responsabilità è opponibile agli interessati né pregiudica l'art. 82 del GDPR, incluso il diritto di regresso di cui al paragrafo 5.

Art. 15 — Modifiche, prevalenza e cessazione

15.1. Le modifiche al presente DPA e agli Allegati sono identificate mediante codice di versione e data di pubblicazione. La pubblicazione sul sito costituisce modalità di messa a disposizione del testo, ma non produce da sola modifiche sostanziali ai rapporti in essere. Le modifiche sostanziali sono comunicate al Titolare e diventano applicabili secondo le modalità previste dal contratto principale o mediante accordo documentato tra le Parti.

15.2. In caso di contrasto, il presente DPA prevale sulle clausole del contratto principale esclusivamente per la materia del trattamento dei dati personali. Se una clausola è invalida, le restanti clausole rimangono efficaci e le Parti la sostituiscono con una previsione lecita che realizzi il più possibile la stessa funzione.

15.3. La cessazione del contratto principale o del presente DPA non pregiudica gli obblighi che, per loro natura, devono sopravvivere, inclusi riservatezza, cooperazione, audit relativo ai trattamenti pregressi e cancellazione o conservazione limitata per legge.

Art. 16 — Comunicazioni operative

Per le comunicazioni relative a istruzioni, incidenti, data breach, sub-responsabili e audit, le Parti utilizzano i recapiti indicati nel contratto principale e/o i seguenti recapiti operativi:

Funzione	Titolare	Responsabile
Contatto privacy / DPO	Forniti dal Titolare in fase di onboarding ai servizi offerti dal Responsabile.	dpo@ikonika.it
Data breach 24/7		dpo@ikonika.it
PEC		Ikonika.srl@legalmail.it

Art. 17 — Pubblicazione e presa visione

17.1. Il presente DPA è pubblicato sul sito web del Responsabile all'URL indicato nel contratto principale. La pagina del DPA riporta almeno il codice di versione, la data di pubblicazione e, ove previsto, lo storico delle versioni precedenti.

17.2. Il contratto principale contiene il collegamento ipertestuale al DPA e individua, mediante il collegamento alla relativa pagina versionata, il testo applicabile al rapporto. Il DPA è così messo a disposizione in forma scritta elettronica e costituisce parte integrante del rapporto contrattuale nei limiti e secondo le modalità previste dal contratto principale.

17.3. Il Titolare prende visione del DPA mediante il rinvio contenuto nel contratto principale e con le modalità di presa visione ivi previste. Non è richiesta una sottoscrizione separata del presente DPA.

17.4. Il Responsabile conserva evidenza della versione del DPA richiamata nel contratto principale e della data di accettazione e, su richiesta del Titolare, ne rilascia o mette a disposizione copia in formato non modificabile (ad esempio PDF) riferita a tale versione.

ALLEGATO 1 — Descrizione del trattamento

Elemento	Descrizione
Oggetto	Erogazione dei servizi di firma elettronica, archiviazione dati in cloud, archiviazione documentale, conservazione digitale e backup cloud.
Durata	Durata del contratto principale e periodo strettamente necessario a restituzione/cancellazione; eventuale conservazione per legge: 20 anni per documenti firmati elettronicamente e limitatamente alla durata del contratto principale per tutte le altre informazioni.
Finalità	Esecuzione dei servizi richiesti dal Titolare, mantenimento di disponibilità e integrità dei dati, assistenza tecnica e adempimenti documentati del Titolare.
Operazioni	Ricezione/raccolta, registrazione, organizzazione, conservazione, consultazione, confronto, aggiornamento, recupero, backup, restituzione, cancellazione e distruzione sicura.
Sistemi/servizi	Piattaforme di firma; repository documentale; sistemi cloud; sistemi di conservazione; sistemi di backup; strumenti di supporto autorizzati.
Localizzazione	Italia (Spazio Economico Europeo). Per la sola funzionalità opzionale di identificazione del firmatario (FirmaOTP), che il Titolare decida di abilitare: trattamento eseguito su infrastrutture ubicate nel SEE [Germania] da un sub-responsabile con sede in un Paese terzo [Taiwan], con possibilità di accesso da tale Paese per finalità di assistenza e manutenzione, sulla base delle clausole contrattuali tipo di cui alla Decisione di esecuzione (UE) 2021/914 e della relativa valutazione d'impatto del trasferimento, come previsto dall'Art. 12.4.

Categorie di dati personali

- dati identificativi e anagrafici;
- dati di contatto e dati professionali;
- dati contenuti nei documenti caricati, archiviati o conservati;

- dati relativi a firme elettroniche, certificati, marcature temporali e tracciati tecnici, nei limiti del servizio;
- dati di autenticazione, autorizzazione, log e sicurezza;
- dati fiscali, contrattuali e amministrativi eventualmente presenti nei documenti;
- categorie particolari di dati (art. 9 GDPR) e dati relativi a condanne penali e reati (art. 10 GDPR) eventualmente contenuti nei documenti caricati dal Titolare, la cui presenza è determinata esclusivamente dal Titolare e che il Responsabile non ricerca né tratta per finalità proprie;
- Esclusivamente nel caso in cui il Titolare decida di abilitare e utilizzare la funzionalità di identificazione del firmatario legata al prodotto FirmaOTP, il Responsabile tratterà dati biometrici del firmatario (immagine del volto, verifica di presenza dal vivo, immagine del documento di identità ed eventuali sequenze video della sessione di identificazione). Tale trattamento avverrà rigorosamente solo in transito al fine esclusivo di consentire la verifica dell'identità. Tutti i dati biometrici così raccolti saranno definitivamente distrutti in modalità automatica e immediata subito dopo il completamento della procedura di verifica, senza alcuna conservazione o memorizzazione persistente nei sistemi del Responsabile e dei sub-responsabili, fatti salvi i soli log tecnici non biometrici (ad esempio indirizzo IP, user agent e marca temporale) conservati per finalità di sicurezza per non più di 30 giorni. Il trattamento riguarda categorie particolari di dati ai sensi dell'art. 9 del GDPR, la cui condizione di liceità e la cui valutazione d'impatto restano a carico del Titolare (Art. 4).

Categorie di interessati

- clienti, utenti e potenziali clienti del Titolare;
- dipendenti, collaboratori e candidati;
- fornitori, professionisti e partner commerciali;
- legali rappresentanti, referenti e firmatari;
- persone fisiche i cui dati siano contenuti nei documenti affidati;
- personale autorizzato del Titolare e soggetti che esercitano diritti privacy;

ALLEGATO 2 — Misure tecniche e organizzative minime

Il presente allegato descrive il livello minimo concordato. Il Responsabile può adottare misure ulteriori o equivalenti che assicurino un livello di sicurezza non inferiore, documentandone l'equivalenza quando richiesto.

Area	Misure minime
Governance e autorizzazioni	Politiche e procedure privacy/sicurezza; ruoli e responsabilità formalizzati; autorizzazioni per necessità di servizio; riesame periodico degli accessi; vincoli di riservatezza e formazione.
Autenticazione e accesso	Credenziali individuali robuste; gestione di ciclo di vita, revoca e recupero; autenticazione a più fattori per accessi amministrativi o remoti ove tecnicamente disponibile; principio del minimo privilegio.
Sicurezza dei dati	Cifratura in transito e a riposo ove appropriata al rischio; pseudonimizzazione o segregazione ove appropriata; protezione da accessi e trattamenti non autorizzati; gestione sicura delle chiavi.
Logging e monitoraggio	Registrazione degli accessi e degli eventi di sicurezza pertinenti; protezione dei log da alterazioni; monitoraggio e conservazione per un periodo coerente con il rischio e con le esigenze di audit.
Vulnerabilità e aggiornamenti	Gestione delle vulnerabilità; aggiornamenti e patch secondo priorità di rischio; protezione antimalware ove pertinente; verifica periodica dell'efficacia delle misure.

Backup e ripristino	Copie di sicurezza protette e separate; test di ripristino; procedure per ripristinare tempestivamente disponibilità e accesso; indicazione del backup utilizzato in caso di perdita dati e dell'intervallo potenzialmente interessato.
Continuità e resilienza	Piani per incidenti fisici o tecnici, indisponibilità del personale e interruzioni del servizio; procedure di escalation; test e riesami periodici.
Data breach	Procedura documentata di rilevazione, classificazione, contenimento, analisi, comunicazione al Titolare entro il termine contrattuale di 24 ore ~~ove possibile~~, e conservazione delle evidenze.
Cancellazione e supporti	Cancellazione sicura al termine del servizio; gestione dei supporti dismessi; restituzione in formato concordato; segregazione dei dati soggetti a conservazione obbligatoria.
Sub-responsabili e trasferimenti	Due diligence e accordi scritti; registro aggiornato; localizzazioni documentate; blocco di trasferimenti extra SEE non autorizzati; verifica del meccanismo GDPR applicabile.
Identificazione biometrica e sistemi di IA	Trattamento esclusivamente transitorio dei dati biometrici, con distruzione automatica e immediata al termine della verifica e configurazione dei sub-responsabili con conservazione disattivata, ove disponibile; esclusione dell'uso dei dati per addestramento o miglioramento dei modelli; cifratura in transito e segregazione dei flussi; accessi di assistenza da Paesi terzi limitati al minimo necessario e registrati; verifica periodica dell'accuratezza e dei tassi di errore dichiarati dal fornitore; possibilità di intervento umano.