Ekeria

*We move your business forward*

**Data di efficacia della presente versione**: 01 / 01 / 2027

# Data Processing Agreement Hoida Facility

**Accordo sul trattamento dei dati personali e conferimento dell'incarico ai sensi dell'articolo 28 GDPR**

Il presente Data Processing Agreement ("DPA"), comprensivo degli Allegati 1, 2 e 3, costituisce parte integrante del Contratto Hoida Facility tra Ekeria S.r.l., identificata nei T&C ("Fornitore"), e il Cliente identificato nella Proposta.

## Conferimento dell'incarico

Con la sottoscrizione della Proposta che incorpora il presente DPA, il Cliente, quando agisce quale Titolare del trattamento, nomina Ekeria S.r.l. quale Responsabile del trattamento ai sensi dell'articolo 28 del Regolamento (UE) 2016/679, limitatamente ai trattamenti effettuati per suo conto nell'erogazione di Hoida Facility e descritti nell'Allegato 1.

Quando agisce quale Responsabile per conto di un diverso Titolare, il Cliente conferisce a Ekeria l'incarico di Sub-responsabile. Il Cliente dispone delle necessarie autorizzazioni del Titolare, ne conserva evidenza e la rende disponibile a Ekeria su richiesta; impartisce istruzioni coerenti con quelle ricevute e con il perimetro autorizzato.

Ekeria accetta l'incarico al perfezionamento del Contratto e tratta i dati secondo le istruzioni documentate e le condizioni del presente DPA, senza necessità di una sua sottoscrizione autonoma.

## Società Aderenti e poteri sui dati

Ciascuna Società Aderente aderisce al presente DPA mediante la sottoscrizione del relativo Modulo. Ai trattamenti effettuati per suo conto si applicano la medesima disciplina del conferimento dell'incarico prevista per il Cliente, la descrizione dei trattamenti dell'Allegato 1 e le istruzioni documentate ai sensi dell'articolo 2.1.1, senza necessità di una distinta descrizione o di istruzioni individuali per l'utilizzo ordinario del servizio. Ekeria accetta l'incarico al perfezionamento dell'adesione secondo il Modulo e i T&C, senza una sottoscrizione autonoma del DPA.

Il presente DPA disciplina gli incarichi affidati a Ekeria e non costituisce né sostituisce gli eventuali accordi sul trattamento dei dati tra il Cliente principale e le Società Aderenti. Tali soggetti provvedono, ciascuno per quanto di propria competenza e prima dei relativi accessi e trattamenti, alla definizione dei propri rapporti e alla predisposizione delle autorizzazioni e degli accordi richiesti dalla normativa applicabile.

Quando il Cliente principale affida a Ekeria attività di trattamento in esecuzione di un valido incarico ricevuto dalla Società Aderente Titolare, quest'ultima autorizza il ricorso a Ekeria quale Sub-responsabile alle condizioni del presente DPA. Restano fermi gli obblighi propri di Ekeria.

I diritti e gli obblighi riferiti al Cliente nel presente DPA si applicano, ove pertinenti, anche a ciascuna Società Aderente, esclusivamente per i trattamenti di propria competenza e secondo il ruolo effettivamente rivestito. Tale applicazione non modifica la ripartizione degli obblighi commerciali e di pagamento prevista dai T&C.

L'appartenenza allo stesso gruppo, la gestione informatica comune, la qualifica di Super Admin e l'intestazione di un Profilo di Fatturazione non determinano automaticamente titolarità, contitolarità o poteri di rappresentanza sui dati altrui. Le eventuali deleghe a un referente comune sono documentate. Nessun soggetto può impartire istruzioni di accesso, condivisione, esportazione o cancellazione dei dati di un diverso Titolare senza disporre dei necessari poteri.

**Trattamenti autonomi di Ekeria**

Il DPA non disciplina i trattamenti per i quali Ekeria determina autonomamente finalità e mezzi, quali la gestione amministrativa e contabile del rapporto, l'adempimento degli obblighi di legge e la tutela dei propri diritti. Tali trattamenti sono descritti nella relativa informativa privacy.

## 1. Definizioni

Nel presente DPA, denominato anche "Atto", per "Regolamento" si intende il Regolamento (UE) 2016/679 e per "Dati Personali" i dati personali trattati per conto del Cliente nel perimetro dell'Allegato 1. I termini non definiti nel presente documento hanno il significato attribuito dalla normativa applicabile o dai T&C, secondo il rispettivo contesto. Si applicano inoltre le seguenti definizioni:

"**Misure di Sicurezza**", sono le misure intese a proteggere i dati personali dalla distruzione accidentale o illegale o dalla perdita, alterazione, divulgazione o accesso non autorizzato, come previste all'art. 32 del Regolamento;

"**Normativa Applicabile**", il Regolamento, il D. Lgs. 30 giugno 2003, n. 196, integrato con le modifiche introdotte dal D. Lgs. 10 agosto 2018, n. 101 (di seguito, il "**Codice**"), nonché qualsiasi altra normativa sulla protezione dei dati personali applicabile in Italia, già in vigore o che entrerà in vigore successivamente al perfezionamento del Contratto o della relativa adesione, ivi compresi i provvedimenti del Garante per la protezione dei dati personali emanati in attuazione della Normativa Applicabile;

"**Sub-responsabili**", i soggetti terzi ai quali il Fornitore affida specifiche attività di trattamento di Dati Personali per conto del Cliente nell'ambito dell'erogazione dei Servizi.

## 2. Obblighi delle parti

### 2.1 Obblighi del Fornitore

#### 2.1.1 Istruzioni del Cliente e finalità del trattamento

Il Fornitore tratta i Dati Personali esclusivamente per dare esecuzione al Contratto e sulla base delle istruzioni documentate del Cliente.

Costituiscono istruzioni documentate, nei limiti del rispettivo ambito, il Contratto, il presente DPA e i suoi allegati, gli Ordini, comprese le conferme semplificate dei Servizi Professionali perfezionate ai sensi dell'articolo 4.4 dei T&C, i Moduli di Adesione, le configurazioni selezionate e le operazioni effettuate dai soggetti autorizzati tramite Hoida o Ekeria Home, purché ne sia conservata evidenza. Le operazioni dei Super Admin valgono anche per le Società Aderenti nei limiti delle deleghe conferite nei rispettivi Moduli.

Per l'utilizzo ordinario dei Servizi non è richiesta la predisposizione di ulteriori istruzioni personalizzate all'attivazione dell'ambiente o all'adesione di una società. Restano consentite le ulteriori istruzioni lecite previste dal DPA, trasmesse attraverso i canali concordati e documentate.

Il Fornitore non tratta i Dati Personali per finalità proprie incompatibili con il proprio ruolo di Responsabile.

Qualora il Fornitore sia tenuto a effettuare un trattamento in forza del diritto dell'Unione europea o dello Stato membro cui è soggetto, ne informa il Cliente prima del trattamento, salvo che la legge vieti tale informazione per rilevanti motivi di interesse pubblico.

Il Fornitore informa senza ritardo il Cliente qualora ritenga che un'istruzione ricevuta violi il Regolamento o altre disposizioni applicabili in materia di protezione dei dati personali.

#### 2.1.2 Misure tecniche e organizzative

Tenendo conto dello stato dell'arte, dei costi di attuazione, della natura, dell'ambito, del contesto e delle finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche, il Fornitore adotta e mantiene misure tecniche e organizzative adeguate al rischio ai sensi dell'articolo 32 del Regolamento.

Le misure tecniche e organizzative applicabili sono descritte nell'Allegato 2, parte integrante del presente DPA.

Il Cliente autorizza l'aggiornamento delle modalità tecniche di attuazione e la sostituzione delle misure con soluzioni equivalenti o migliorative, senza necessità di una nuova sottoscrizione, purché rimangano adeguate al rischio, non riducano in misura sostanziale il livello complessivo di protezione concordato e non modifichino le istruzioni o gli impegni espressamente assunti. Non è richiesta la conservazione della medesima tecnologia.

Le modifiche documentali, le comunicazioni e la conservazione delle versioni seguono l'articolo 7. Le modifiche che eccedono la facoltà prevista dal presente articolo richiedono un preventivo accordo scritto. I cambiamenti relativi ai Sub-responsabili e ai trasferimenti internazionali seguono, rispettivamente, gli articoli 2.1.6 e 2.1.5.

**2.1.3 Persone autorizzate al trattamento**

Il Fornitore consente l'accesso ai Dati Personali esclusivamente alle persone che operano sotto la propria autorità e che ne abbiano necessità per l'esecuzione, la gestione, la sicurezza o il controllo dei Servizi.

Il Fornitore garantisce che tali persone:

a. siano autorizzate e adeguatamente istruite in relazione alle attività loro affidate;
b. trattino i Dati Personali esclusivamente secondo le istruzioni ricevute;
c. si siano impegnate alla riservatezza o siano soggette a un adeguato obbligo legale di riservatezza.

**2.1.4 Diritti degli interessati**

Tenuto conto della natura del trattamento, il Fornitore assiste il Cliente, mediante misure tecniche e organizzative adeguate e nella misura in cui ciò sia possibile, nel dare seguito alle richieste degli Interessati relative all'esercizio dei diritti previsti dalla Normativa Applicabile.

Qualora riceva direttamente una richiesta riferita a Dati Personali trattati per conto del Cliente, il Fornitore la trasmette senza ingiustificato ritardo al Cliente e non vi dà autonomamente seguito, salvo che sia stato espressamente autorizzato o istruito dal Cliente.

**2.1.5 Comunicazione e trasferimento all'estero dei dati**

Il Fornitore comunica o rende disponibili i Dati Personali a terzi esclusivamente quando ciò sia previsto dal Contratto, derivi da un'istruzione documentata del Cliente, sia necessario per il ricorso a un Sub-responsabile autorizzato oppure sia imposto dalla normativa applicabile.

Qualsiasi trasferimento di Dati Personali verso un Paese terzo o un'organizzazione internazionale è effettuato sulla base delle istruzioni documentate del Cliente e nel rispetto del Capo V del Regolamento, salvo che il trasferimento sia imposto dal diritto dell'Unione europea o dello Stato membro cui il Fornitore è soggetto.

In tale ultimo caso, il Fornitore informa preventivamente il Cliente dell'obbligo giuridico, salvo che la normativa applicabile vieti tale informazione per rilevanti motivi di interesse pubblico.

**2.1.6 Sub-responsabili**

Il Cliente autorizza in via generale il Fornitore a ricorrere a Sub-responsabili per l'esecuzione delle attività di trattamento necessarie all'erogazione dei Servizi.

L'elenco dei Sub-responsabili direttamente incaricati dal Fornitore è contenuto nell'Allegato 3, parte integrante del presente DPA. Le informazioni pertinenti ai soggetti ulteriormente coinvolti sono rese accessibili secondo quanto indicato nel medesimo Allegato.

Il Fornitore può aggiungere o sostituire un Sub-responsabile senza necessità di una specifica autorizzazione preventiva del Cliente. Il Fornitore comunica attivamente al Cliente, mediante e-mail al recapito contrattuale o privacy e copia consultabile nel portale, ogni prevista aggiunta o sostituzione di un Sub-responsabile, con almeno trenta giorni di calendario di preavviso, aggiornando l'elenco. La sola modifica dell'elenco online non sostituisce la comunicazione.

Entro 10 giorni dalla comunicazione, il Cliente può formulare un'opposizione esclusivamente per motivi specifici, documentati e ragionevoli relativi alla protezione dei Dati Personali. L'opposizione non attribuisce al Cliente un generale diritto di veto sulle scelte organizzative o tecnologiche del Fornitore.

In caso di opposizione, le Parti collaborano in buona fede per individuare una soluzione ragionevole. Qualora non sia possibile adottare una soluzione alternativa senza costi o modifiche sproporzionati, ciascuna Parte può

cessare il solo Servizio interessato prima dell'avvio del trattamento da parte del nuovo Sub-responsabile, fatti salvi i corrispettivi già maturati.

Quando il termine ordinario non sia compatibile con un'esigenza urgente di sicurezza o continuità, il Fornitore ricerca prioritariamente una soluzione tramite Sub-responsabili già autorizzati. Per il ricorso a un nuovo Sub-responsabile acquisisce, ove necessario, un'autorizzazione specifica con procedura accelerata oppure adotta una comunicazione preventiva e un termine ridotto che consentano un'effettiva possibilità di opposizione, nei limiti dell'articolo 28 GDPR. Il presente Atto non autorizza in via generale l'impiego di un nuovo Sub-responsabile con la sola comunicazione successiva.

Non costituiscono aggiunta o sostituzione di un Sub-responsabile, e non richiedono la comunicazione prevista dal presente articolo:

a. il ricorso a fornitori che non trattino Dati Personali per conto del Fornitore;
b. le modifiche organizzative interne al medesimo soggetto giuridico;
c. le variazioni tecniche, infrastrutturali o di servizio effettuate dal medesimo Sub-responsabile che non comportino il coinvolgimento di un diverso soggetto giuridico, il trasferimento dei Dati Personali al di fuori dello Spazio Economico Europeo o di una diversa area geografica espressamente indicata nell'elenco dei Sub-responsabili o nel Contratto, oppure una riduzione sostanziale delle garanzie applicabili.

Il Fornitore impone al Sub-responsabile, mediante contratto o altro atto giuridico vincolante, gli stessi obblighi in materia di protezione dei dati applicabili al Fornitore ai sensi del presente Atto, nella misura pertinente alle attività affidate. Il Fornitore rimane responsabile nei confronti del Cliente dell'adempimento degli obblighi del Sub-responsabile secondo quanto previsto dall'articolo 28, paragrafo 4, del Regolamento.

### 2.1.7 Violazione dei Dati Personali

Il Fornitore informa il Cliente senza ingiustificato ritardo dopo essere venuto a conoscenza di una violazione dei Dati Personali trattati per conto del Cliente.

La comunicazione contiene, nella misura in cui le informazioni siano disponibili:

a. una descrizione della natura della violazione;
b. le categorie e il numero approssimativo degli interessati e delle registrazioni coinvolte;
c. le possibili conseguenze della violazione;
d. le misure adottate o proposte per porvi rimedio e limitarne gli effetti;
e. il riferimento di un punto di contatto presso il quale ottenere ulteriori informazioni.

Qualora non sia possibile fornire tutte le informazioni contestualmente, il Fornitore comunica inizialmente quelle disponibili e integra la comunicazione senza ingiustificato ritardo.

Il Fornitore collabora con il Cliente affinché quest'ultimo possa adempiere agli obblighi previsti dagli articoli 33 e 34 del Regolamento.

### 2.1.8 Assistenza al Cliente

Tenuto conto della natura del trattamento e delle informazioni a propria disposizione, il Fornitore assiste il Cliente nell'adempimento degli obblighi previsti dagli articoli 32–36 del Regolamento, inclusi:

a. la sicurezza del trattamento;
b. la gestione e la notifica delle violazioni dei Dati Personali;
c. la valutazione d'impatto sulla protezione dei dati;
d. l'eventuale consultazione preventiva dell'autorità di controllo.

Le modalità e l'estensione dell'assistenza sono determinate in funzione della natura dei Servizi e della richiesta del Cliente. Le eventuali attività straordinarie sono disciplinate dall'articolo 5 del presente DPA.

### 2.2 Obblighi del Cliente in qualità di Titolare

Il Cliente, in qualità di Titolare del trattamento:

a. determina le finalità e i mezzi essenziali del trattamento;
b. garantisce che i trattamenti affidati al Fornitore siano fondati su un'idonea base giuridica e conformi alla Normativa Applicabile;
c. fornisce agli Interessati le informazioni richieste dalla Normativa Applicabile;
d. impartisce al Fornitore istruzioni documentate lecite, complete e coerenti con il Contratto;

e. garantisce che i Dati Personali messi a disposizione del Fornitore siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità perseguite;
f. adempie agli obblighi relativi all'esercizio dei diritti degli Interessati, alle valutazioni d'impatto, alle notifiche alle autorità e alle comunicazioni agli Interessati, avvalendosi dell'assistenza del Fornitore nei limiti previsti dal presente Atto;
g. informa il Fornitore quando il trattamento richieda misure o condizioni ulteriori non desumibili dalla configurazione ordinaria dei Servizi.

Il Cliente è responsabile della liceità della raccolta e dell'utilizzo dei Dati Personali e dell'adeguatezza delle istruzioni impartite al Fornitore.

Per le funzioni di timbratura, verifica del luogo e gestione delle attività lavorative il Cliente, quale datore di lavoro o soggetto competente, valuta gli obblighi lavoristici e privacy, informa gli interessati e acquisisce gli eventuali accordi o autorizzazioni necessari. Il consenso al permesso di localizzazione del dispositivo non sostituisce tali adempimenti. Restano fermi gli obblighi propri di Ekeria quale Responsabile.

**3. Audit e verifica della conformità**

**3.1** Il Fornitore mette a disposizione del Cliente le informazioni necessarie a dimostrare il rispetto degli obblighi previsti dall'articolo 28 del Regolamento e consente e contribuisce agli audit, comprese le ispezioni, effettuati dal Cliente o da un revisore indipendente dallo stesso incaricato.

**3.2** Le verifiche vengono svolte in via prioritaria mediante l'esame di documentazione, questionari, descrizioni delle misure tecniche e organizzative, attestazioni, certificazioni e report di audit indipendenti resi disponibili dal Fornitore.

**3.3** Qualora le evidenze documentali non siano ragionevolmente sufficienti, oppure in presenza di concrete indicazioni di non conformità, di una violazione rilevante dei Dati Personali o di una richiesta dell'autorità di controllo, il Cliente può richiedere un audit presso i locali del Fornitore. Salvo tali casi, l'audit presso i locali non può essere richiesto più di una volta ogni dodici mesi e deve essere comunicato con almeno quindici giorni lavorativi di preavviso.

**3.4** L'audit si svolge durante il normale orario di lavoro, secondo un perimetro preventivamente concordato e senza interferire irragionevolmente con la sicurezza, la continuità e l'operatività dei Servizi. Esso non attribuisce al Cliente o al revisore un diritto di accesso diretto o non controllato ai sistemi di produzione, al Codice Sorgente, ai dati di altri clienti, alle credenziali, alle chiavi crittografiche o ai segreti commerciali del Fornitore. Il coordinamento del perimetro non attribuisce al Fornitore un diritto di veto su verifiche necessarie e proporzionate; sono concordate modalità protette equivalenti, senza accessi incontrollati ai dati di altri clienti.

**3.5** Il revisore deve essere professionalmente qualificato, indipendente, privo di conflitti di interesse e vincolato alla riservatezza. Il Fornitore può opporsi per ragionevoli motivi alla nomina di un proprio concorrente diretto.

**3.6** Il diritto di audit non comporta un diritto automatico di accesso diretto ai locali o ai sistemi dei Sub-responsabili. La relativa conformità può essere dimostrata mediante certificazioni, report di audit indipendenti e altre evidenze ragionevolmente disponibili. Se le evidenze ordinarie non sono sufficienti, il Fornitore coopera per ottenere ulteriori evidenze o organizzare le verifiche necessarie nei limiti della legge, senza negare in via assoluta i diritti previsti dall'articolo 28.

**3.7** Il Cliente sostiene i costi dei propri revisori e delle verifiche richieste. Il Fornitore può addebitare le attività straordinarie necessarie a supportare l'audit, previa comunicazione dei relativi costi, salvo che l'audit accerti una violazione sostanziale imputabile al Fornitore o sia richiesto direttamente da un'autorità di controllo. Gli eventuali costi sono ragionevoli, proporzionati, preventivamente indicati e non rendono impossibile o eccessivamente oneroso l'esercizio del diritto di audit obbligatorio.

**3.8** Le informazioni e i risultati dell'audit sono riservati. Restano impregiudicati i poteri delle autorità di controllo competenti.

**4. Referenti privacy**

Il Fornitore rende disponibili al Cliente i dati di contatto del proprio referente per le questioni relative alla protezione dei dati personali e, ove nominato, del proprio Responsabile della protezione dei dati.

**5. Corrispettivi**

Gli adempimenti ordinari previsti dal presente Atto sono compresi nei corrispettivi dei Servizi.

Le attività straordinarie richieste dal Cliente che eccedano la normale esecuzione degli obblighi del Fornitore, e che non siano conseguenza di un inadempimento imputabile al Fornitore, possono essere erogate come Servizi Professionali a pagamento, previa comunicazione e accettazione dei relativi corrispettivi e nei limiti consentiti dalla Normativa Applicabile.

## 6. Restituzione e cancellazione

Il presente DPA acquista efficacia con il perfezionamento del Contratto ai sensi dell'articolo 14.1 dei T&C e disciplina da tale momento i trattamenti effettuati per conto del Cliente, compresi quelli relativi a dati già presenti nel servizio. L'eventuale decorrenza economica anteriore indicata nella Proposta non anticipa l'efficacia del presente DPA. Il DPA rimane efficace fino alla restituzione o cancellazione dei Dati Personali e delle relative copie secondo il Contratto, anche dopo la cessazione dell'accesso operativo.

Per ciascuna Società Aderente, il DPA acquista efficacia con il perfezionamento della relativa adesione e comunque non prima della sottoscrizione del Modulo da parte del soggetto munito dei necessari poteri e della sua accettazione da parte di Ekeria. Un'eventuale decorrenza economica anteriore non anticipa tale efficacia. Restano fermi gli accordi validamente applicabili ai trattamenti precedenti.

Il Cliente sceglie la restituzione o la cancellazione secondo le modalità e i termini dell'articolo 8 dei T&C. In assenza di richiesta di restituzione nel termine applicabile, il Cliente impartisce istruzione di cancellare, ferme le richieste e i periodi di recupero ancora pendenti.

Al termine dei periodi applicabili il Fornitore cancella i Dati Personali e le copie esistenti, salvo obblighi di conservazione imposti dal diritto dell'Unione o degli Stati membri. Le copie di backup residue sono isolate e non impiegate per finalità ordinarie e vengono eliminate entro il ciclo massimo documentato nelle misure tecniche e organizzative. In caso di ripristino si riapplicano le cancellazioni dovute.

La sostituzione o rimozione di nomi, recapiti o altri identificativi non equivale automaticamente a cancellazione o anonimizzazione. Finché una persona è ragionevolmente identificabile, i dati restano soggetti al presente Atto. Il Fornitore non conserva dati applicativi dopo la cessazione per finalità proprie sulla base della sola de-identificazione delle anagrafiche. Eventuali elaborazioni anonime richiedono una verifica documentata e una base lecita e non eludono gli obblighi di cancellazione contrattuali o del Data Act.

## 7. Versioni e aggiornamenti

**7.1** Il DPA comprende gli Allegati 1, 2 e 3. La versione iniziale applicabile al Cliente è quella identificata nella procedura di sottoscrizione della Proposta. Per ciascuna Società Aderente si applica la medesima versione già applicabile al Contratto quadro al momento dell'adesione, tenendo conto degli aggiornamenti validamente intervenuti, identificata e resa disponibile con il relativo Modulo. Ekeria conserva le copie e le evidenze delle rispettive accettazioni.

**7.2** Le modifiche delle condizioni contrattuali relative alle misure dell'Allegato 2 sono ammesse nei limiti dell'articolo 2.1.2 e comunicate con almeno trenta giorni di calendario di preavviso. Non è necessario attendere tale termine per eseguire aggiornamenti tecnici e interventi di sicurezza già consentiti dagli impegni pattuiti, che non modifichino le istruzioni o le condizioni contrattuali applicabili.

**7.3** L'aggiunta o la sostituzione dei Sub-responsabili segue esclusivamente il procedimento dell'articolo 2.1.6. Le altre modifiche del DPA richiedono il necessario accordo scritto tra le Parti, fatti salvi gli obblighi imposti dalla normativa applicabile.

**7.4** Ogni nuova versione identifica le parti modificate e la relativa data di efficacia. Ekeria conserva le versioni precedenti e le evidenze delle comunicazioni e degli accordi applicabili. La sola pubblicazione non sostituisce le comunicazioni o le accettazioni richieste. Le verifiche e le richieste documentali restano disciplinate dall'articolo 3.

# Allegato 1

## Descrizione dei trattamenti e dati ammessi

**Soggetti Interessati**
I trattamenti possono riguardare, in funzione delle funzionalità utilizzate:

- utenti, dipendenti, collaboratori e operatori del Cliente e delle società dallo stesso autorizzate;
- clienti, committenti, referenti e utenti esterni del Cliente;
- fornitori, appaltatori, partner e relativi referenti;
- ulteriori persone fisiche i cui dati siano legittimamente inseriti dal Cliente in Hoida o contenuti nei documenti e negli allegati caricati.

**Categorie di dati**
I trattamenti possono riguardare, in funzione della configurazione utilizzata:

- dati identificativi, anagrafici e di contatto;
- dati relativi agli account, ai profili, ai ruoli e alle autorizzazioni;
- dati professionali, lavorativi, organizzativi e contrattuali;
- dati relativi a turni, presenze, timbrature, assenze e attività svolte;
- dati relativi a commesse, cantieri, Work Order, ticket, checklist, audit e rapporti di intervento;
- Dati strettamente necessari alla verifica puntuale della compatibilità della timbratura con il luogo di lavoro previsto. Secondo la configurazione dichiarata da Ekeria, le coordinate del dipendente sono utilizzate per tale verifica e non vengono conservate come storico di posizione. Sono trattati gli ulteriori dati di timbratura e l'eventuale esito della verifica effettivamente registrati. Non è prevista da questa descrizione una localizzazione continua del dipendente;
- fotografie, firme, note, comunicazioni, documenti e allegati;
- dati relativi a note spese, acquisti, forniture e informazioni amministrative o contabili, ove presenti;
- dati tecnici relativi all'utilizzo del Servizio, quali indirizzi IP, identificativi del dispositivo, log di accesso e registrazioni tecniche.

Hoida Facility non è un sistema HR o payroll. I documenti caricati dal Cliente possono tuttavia contenere categorie particolari di dati ai sensi dell'articolo 9 GDPR, ad esempio dati sanitari o sindacali. La loro eventuale presenza non è esclusa dal presente Atto. Il Cliente limita il caricamento a quanto necessario e lecito, documenta le pertinenti condizioni di trattamento e configura gli accessi in modo adeguato. Prima di avviare trattamenti sistematici di categorie particolari o dati dell'articolo 10, informa Ekeria per verificare compatibilità del servizio, istruzioni e misure necessarie. Il mero caricamento non autorizza trattamenti vietati dalla legge e non trasferisce al Fornitore la scelta della base giuridica.

**Operazioni di trattamento**
Le operazioni possono comprendere raccolta, registrazione, organizzazione, strutturazione, conservazione, consultazione, utilizzo, estrazione, comunicazione mediante trasmissione, limitazione e cancellazione.

**Oggetto e finalità**
L'oggetto del trattamento consiste nell'erogazione, gestione, manutenzione, assistenza, sicurezza, backup ed eventuale esportazione del Software Hoida e dei Servizi attivati dal Cliente.

I Dati Personali sono trattati esclusivamente per consentire al Cliente di utilizzare Hoida secondo la configurazione selezionata e le istruzioni documentate impartite al Fornitore.

**Durata**
I trattamenti disciplinati dal presente DPA decorrono dalla sua efficacia ai sensi dell'articolo 6 e proseguono per la durata dei Servizi e per gli ulteriori periodi di restituzione, esportazione, conservazione e cancellazione previsti dal medesimo articolo e dall'articolo 8 dei T&C. Restano fermi gli accordi validamente applicabili ai trattamenti precedenti.

# Allegato 2

## Misure tecniche e organizzative

### 1. Oggetto e ambito di applicazione

Il presente Allegato descrive le misure applicate ai trattamenti disciplinati dal DPA. Il perimetro comprende l'applicazione web, i servizi utilizzati dall'app mobile e i componenti di autenticazione, archiviazione, backup e assistenza che trattano dati per conto del Cliente. Gli aggiornamenti seguono gli articoli 2.1.2 e 7 del DPA.

### 2. Misure applicate

| Ambito | Descrizione delle misure applicate |
|---|---|
| Infrastruttura e localizzazione | Hoida Facility utilizza infrastruttura AWS con archiviazione dei dati applicativi nell'Unione europea. La protezione fisica delle infrastrutture ospitate è affidata al fornitore cloud; Ekeria gestisce le configurazioni e i controlli di propria competenza. I Sub-responsabili e gli eventuali trasferimenti internazionali sono disciplinati dal DPA e dal relativo elenco. |
| Autenticazione e accessi tecnici | L'autenticazione degli utenti applicativi è gestita tramite Amazon Cognito. Gli account sono nominativi e l'accesso è subordinato alle abilitazioni assegnate. Gli accessi tecnici gestiti da Ekeria sono riservati al personale autorizzato, limitati alle attività affidate e revocati al venir meno della necessità. Le credenziali tecniche sono protette da accessi e condivisioni non autorizzati. Gli accessi amministrativi interattivi del personale Ekeria ai sistemi che trattano i dati sono protetti mediante autenticazione a più fattori. |
| Autorizzazioni e separazione dei dati | L'applicazione verifica l'ambiente, le autorizzazioni e il perimetro dati associati all'utente prima di consentire le operazioni. I controlli sono applicati anche dai servizi che elaborano le richieste, non soltanto nell'interfaccia.<br>All'interno del medesimo ambiente, i Profili di Fatturazione non determinano una segregazione dei dati per società. I Super Admin dispongono di poteri di gestione trasversale sulle configurazioni e sui dati dell'ambiente; le relative autorizzazioni sono disciplinate dal Contratto, dai Moduli di Adesione e dalle istruzioni documentate. Per gli altri utenti si applicano i ruoli e i permessi effettivamente configurati. |
| Comunicazioni e dati conservati | Le comunicazioni tra browser o app e i servizi Hoida sono protette mediante HTTPS/TLS. L'accesso ai dati conservati è limitato tramite controlli applicativi e infrastrutturali. |

| Ambito | Descrizione delle misure applicate |
|---|---|
| Personale e postazioni | Le persone autorizzate operano secondo le istruzioni e gli obblighi di riservatezza previsti dal DPA. Le postazioni utilizzate per accedere ai dati sono protette mediante autenticazione, blocco dell'accesso quando incustodite e aggiornamenti di sicurezza. L'accesso alle informazioni è limitato a quanto necessario per le attività affidate. |
| Backup e ripristino | Il database è sottoposto a backup giornaliero durante le ore notturne. L'accesso alle relative copie è riservato al personale autorizzato; le verifiche dell'esito delle copie e le prove di ripristino riguardano il database. I tempi massimi di conservazione delle copie residue sono indicati al punto 3.<br>I documenti gestiti mediante il modulo di gestione documentale sono conservati su Amazon S3 con attivo il sistema di versioning che consente il recupero delle versioni ancora conservate.<br>Per allegati, quali ad esempio le fotografie degli Ordini di Lavoro, non si dispone di un sistema di backup separato e non sono recuperabili dopo la cancellazione definitiva. La gestione delle copie e delle versioni conservate segue i termini di cancellazione previsti dal DPA. |
| Registrazione, assistenza e incidenti | Sono registrati gli eventi necessari alla sicurezza e alla gestione tecnica, limitando il contenuto dei log ai dati pertinenti. L'accesso alle registrazioni è riservato ai soggetti autorizzati. Gli accessi ai dati per assistenza sono collegati a esigenze di servizio e limitati al perimetro necessario. Le anomalie vengono valutate e gestite dal personale tecnico; le violazioni dei dati personali seguono l'articolo 2.1.7 del DPA. |
| Aggiornamenti e verifica delle misure | Gli aggiornamenti e le vulnerabilità sono valutati in funzione dell'impatto e del rischio. Le modifiche sono verificate prima del rilascio, compatibilmente con gli interventi urgenti necessari a proteggere il servizio. L'utilizzo di dati reali in attività di test o manutenzione è limitato al necessario e sottoposto ad autorizzazioni e protezioni coerenti con il trattamento. L'efficacia dei controlli è riesaminata regolarmente e in occasione di modifiche rilevanti o incidenti, documentando le azioni correttive. |

## 3. Conservazione delle copie e cancellazione

La restituzione e la cancellazione dei dati seguono l'articolo 6 del DPA e l'articolo 8 dei T&C.

Al termine dei periodi applicabili, Ekeria elimina i dati dal sistema attivo e gestisce le copie residue secondo il ciclo indicato di seguito. Le copie residue sono escluse dall'utilizzo ordinario e accessibili soltanto per le attività autorizzate di sicurezza, ripristino o adempimento di obblighi applicabili.

Le copie residue di backup del database sono eliminate entro quattordici giorni dalla cancellazione dei relativi dati dal sistema attivo. I documenti e gli allegati conservati in Amazon S3 sono cancellati secondo l'articolo 6 del DPA e l'articolo 8 dei T&C. Le eventuali versioni precedenti o ulteriori copie effettivamente presenti devono essere comprese nel processo di cancellazione e nei termini applicabili.

In caso di ripristino, le cancellazioni dovute vengono riapplicate prima di rendere nuovamente disponibili i dati per l'utilizzo ordinario. Restano ferme le conservazioni specificamente imposte dalla legge, limitatamente ai dati e ai periodi necessari.

## 4. Configurazione e responsabilità del Cliente

Il Cliente gestisce gli utenti, i ruoli, i permessi e le condivisioni di propria competenza attraverso le funzionalità disponibili. È responsabile della corretta attribuzione di tali autorizzazioni e della protezione dei dispositivi sotto il proprio controllo.

Negli ambienti utilizzati da più società, gli accessi devono corrispondere ai poteri e ai perimetri effettivamente autorizzati. Restano fermi gli obblighi di Ekeria relativi alla sicurezza del Software e ai trattamenti svolti per conto del Cliente.

# Allegato 3

## Elenco dei Sub-responsabili

### 1. Tabella dei Sub-responsabili

| Sub-responsabile e sede | Attività e dati trattati | Localizzazione dei trattamenti e giurisdizioni dell'infrastruttura |
|---|---|---|
| **Amazon Web Services EMEA SARL** — 38 Avenue John F. Kennedy, L-1855 Lussemburgo. Servizi: AWS, incluso Amazon Cognito. | Hosting e servizi infrastrutturali utilizzati da Hoida; autenticazione tramite Amazon Cognito. Dati applicativi e documenti conservati nell'infrastruttura; identificativi degli utenti e informazioni degli account necessarie all'autenticazione. | Archiviazione dei dati applicativi Hoida nell'Unione europea. Paesi o regioni utilizzati per produzione, database, documenti, autenticazione e backup: Germania - Francoforte. Giurisdizioni pertinenti all'infrastruttura e ai servizi utilizzati: Germania - Francoforte. Gli eventuali ulteriori trattamenti e accessi pertinenti sono individuati nella documentazione dei soggetti coinvolti. |
| **HubSpot Ireland Limited** — HubSpot House, One Sir John Rogerson's Quay, Dublin 2, Irlanda. Servizio: HubSpot. | Gestione delle richieste di assistenza e delle comunicazioni correlate. Dati personali contenuti nei ticket, nei messaggi e negli eventuali allegati, nella misura in cui siano trattati per conto del Cliente per gestire la richiesta. | Localizzazione principale dell'account Ekeria: Germania. Eventuali ulteriori Paesi di trattamento o accesso sono individuati nella documentazione della catena applicabile alle funzionalità utilizzate. |

### 2. Documentazione dei fornitori e localizzazione

Ekeria verifica l'idoneità dei Sub-responsabili rispetto ai trattamenti affidati e la presenza degli accordi richiesti dall'articolo 28 GDPR, aggiornando le verifiche in caso di cambiamenti rilevanti.

Sono rese accessibili le informazioni identificative e di contatto e la documentazione pertinente sui soggetti coinvolti nella catena dei trattamenti. La sede legale del fornitore non coincide necessariamente con i luoghi di archiviazione, trattamento o accesso ai dati.

Eventuali trasferimenti al di fuori dello Spazio economico europeo seguono l'articolo 2.1.5 del DPA e il Capo V del GDPR.

I collegamenti alla documentazione dei fornitori hanno funzione informativa: non sostituiscono il DPA Hoida, non ne riducono le garanzie e non autorizzano automaticamente nuovi trattamenti o nuovi Sub-responsabili.

**AWS — Elenco dei Sub-responsabili**
https://aws.amazon.com/compliance/sub-processors/

**HubSpot — Data Processing Agreement**
https://legal.hubspot.com/dpa

**HubSpot — Elenco dei Sub-responsabili**
https://legal.hubspot.com/sub-processors-page