

ACCORDO PER IL TRATTAMENTO DI DATI PERSONALI DATA PROCESSING AGREEMENT (DPA)

PREMESSO CHE

➤ Tra le parti è in essere un contratto di fornitura di uno o più dei seguenti servizi:

Connettività ad Internet

- Fibra ottica FTTH
- Fibra FTTC
- Rame xDSL
- Wireless (Connettività Radio)
- Sistemi di backp (Light, Smart, Always Up o similari)

Voice & Collaboration

- Soluzioni di UC&C (Unified Communication & Collaboration)
- Sistemi Telefonici in cloud
- Sistemi Telefonici on-premise
- Servizi e traffico Telefonia Fissa

Networking

- Network infrastructure assessment
- Cablaggi Wired e Wireless
- Router & Switching
- SDN (Software Defined Networking) & SD-WAN (Software Defined Wide Area Networking)

Data Center & Cloud

- Data center tradizionali
- Data center iperconvergenti (HCI)
- Cloud services
- Fornitura di armadi rack, sale server, cooling e ups

Security

- Cyber Security Framework (CSF)
- Servizi di sicurezza gestita (MSSP-Managed Security Service Provider)
- Backup e disaster recovery
- Soluzioni di endpoint management
- Sistemi di video sorveglianza
- Firewall
- Servizi Antispam/Antivirus

IOT (Internet of Things)

- Smart TIOT
- Metering+H2O

Web & Digital

- Web marketing (SEO-Search Engine Optimization, Google Ads, SMM-Social Media Marketing, DEM-Direct Email Marketing)
- Realizzazione siti web (UX/UI Design, sviluppo su CMS proprietario, sviluppo Wordpress)
- E-commerce (sviluppo su CMS proprietario, sviluppo su WooCommerce)
- Sviluppo App (iOS e Android)
- Assistenza, formazione online, report (supporto post-vendita, servizio di ticketing online)
- Servizi ISP (hosting, domini, mail, caselle pec e servizi simili)

- Axera S.p.A., in ragione dell'erogazione di uno o più dei summenzionati servizi, può trattare flussi di dati personali, così come definiti ai sensi dell'art. 4 del Reg. UE 679/2016 (alias GDPR), concernenti il Titolare, la Clientela e/o i collaboratori delle Parti.
- I servizi oggetto di fornitura, svolti direttamente o anche indirettamente per conto del Committente, possono, a seconda dei casi, essere ricompresi tra le attività di amministrazione di sistema, così come descritte ai sensi del Provvedimento 27 Novembre 2008 del Garante per la Protezione dei Dati Personali, e s.m.i., in particolare qualora garantiscano la configurazione e la gestione dei sistemi informativi coinvolti.
- Tutto ciò premesso, Il Cliente/Committente, in persona del legale rappresentante *pro tempore* (di seguito il "Titolare"), relativamente all'accordo/contratto/accordo quadro (di seguito il "Contratto") e ai relativi servizi sottoscritti con Axera S.p.A. (di seguito "Servizi").

DESIGNA

Axera S.p.A., in persona del proprio legale rappresentante *pro tempore*:

- Responsabile esterno del trattamento dei dati personali (di seguito "Responsabile" o "Società" o anche "Fornitore") per conto del Titolare (di seguito congiuntamente le "Parti"), ai sensi degli artt. 4 e 28 del GDPR (Regolamento Europeo per la protezione dei dati personali 2016/679).
- Amministratore di sistema, ai sensi del Provvedimento 27 Novembre 2008 del Garante per la Protezione dei Dati Personali, laddove i servizi forniti dal Responsabile comportino attività configurabili come tali e rientranti tra quelle previste dal Provvedimento stesso e smi.

1. Descrizione del trattamento affidato nel ruolo di Responsabile ex art. 28 GDPR

Oggetto

Con il presente DPA, il Titolare nomina Axera S.p.A. Responsabile e provvede al conferimento alla stessa delle istruzioni relative al trattamento dei dati personali. Il Responsabile si impegna a trattare i dati personali secondo quanto previsto dalle suddette istruzioni, per il raggiungimento dello scopo del contratto principale sottoscritto dalle parti, cui si fa integrale rinvio e comunque evitando di trattare dati personali in quantità e per un tempo di conservazione che siano eccedenti rispetto a quanto effettivamente necessario per il raggiungimento delle finalità del trattamento, in ottemperanza al principio di minimizzazione dei dati.

Il Responsabile si impegna, altresì, a rispettare i principi di liceità, trasparenza e correttezza del trattamento di cui all'art. 5 GDPR.

Le parti convengono che quanto descritto nel presente contratto annulla e sostituisce qualsivoglia documento del medesimo oggetto, a qualunque titolo intercorso antecedentemente tra le parti.

Durata

La presente designazione avrà la medesima durata del contratto. Qualora questo venisse meno o perdesse efficacia per qualsiasi motivo, anche il presente DPA verrà automaticamente meno, senza bisogno di comunicazioni o di revoche e il Responsabile non sarà più legittimato a trattare i dati qui considerati, salvo i casi in cui sia previsto da normative vigenti o sia necessario in ragione di un proprio legittimo interesse.

Categorie di dati personali

I dati effettivamente trattati e raccolti dipendono dai Servizi di fatto erogati dalla Società in favore del Titolare del trattamento, e ai correlati servizi di assistenza e manutenzione, e possono ad ogni modo ricomprendere:

- dati personali, identificativi e di contatto (nome, cognome, data di nascita, indirizzo e-mail, numero di telefono, ...);
- dati connessi all'utilizzo dei servizi forniti dal Responsabile, ad esempio: tracce di connessioni effettuate relative ai parametri di qualità e/o all'adempimento di altri obblighi di legge;
- dati connessi alla natura del servizio stesso (configurazione reti e sistemi, gestione dei servizi sicurezza, configurazione e manutenzione della rete informatica o dei dispositivi forniti);
- credenziali quali username e password, nonché altre informazioni di sicurezza;
- dati statistici o altri dati di navigazione in rete;
- dati di fatturazione, contabilità e pagamenti;
- dati personali, anche eventualmente qualificati come particolari, correlati ai servizi che prevedono le attività di fornitura dei servizi di conservazione/archiviazione/salvataggio presso i datacenter o le unità di archiviazione di Axera spa

Categorie di interessati

I dati personali raccolti e trattati possono riferirsi a:

- Clienti e potenziali Clienti delle Parti
- Utenti internet o utenti del sistema informativo aziendale (rete e sistemi)
- Personale dipendente e consulenti interni delle Parti
- Collaboratori esterni delle Parti
- Agenti e mandatari delle Parti
- Fornitori delle Parti
- Visitatori

2. Obblighi del Responsabile

Riservatezza dei dati personali

La Società garantisce la riservatezza e la confidenzialità dei dati personali trattati, assicurando che le informazioni affidate ed archiviate siano accessibili solo alle persone autorizzate (dipendenti, collaboratori o incaricati) che, in base al trattamento definito per ciascuno di essi e documentato nelle istruzioni loro fornite, ne abbiano la facoltà, essendo stati altresì previamente istruiti dal Responsabile e abbiano ricevuto un'adeguata formazione in materia, a norma degli artt. 28 e 32 GDPR.

In caso di richiesta di modifica di un trattamento dei dati in essere, il Responsabile avvisa senza indebito ritardo il Titolare, nell'ipotesi in cui ravvisi in tale domanda il rischio di una violazione delle disposizioni in materia di protezione dei dati personali, e nel caso, può negarne l'attuazione.

Collaborazione con le autorità di controllo

Il Titolare deve essere immediatamente informato delle ispezioni ed ogni altro provvedimento eseguito dall'Autorità di controllo, con riferimento al presente contratto. Il Titolare e il Responsabile, su richiesta dell'Autorità di controllo, sono tenuti alla cooperazione.

Le medesime prescrizioni valgono anche nel caso in cui la Società sia coinvolta in indagini da parte delle autorità competenti relativamente a violazioni in materia di trattamento di dati personali, con riferimento al presente Accordo.

Misure tecniche ed organizzative

Il Responsabile deve offrire garanzie sufficienti al fine di mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti degli Interessati.

Il Responsabile si impegna a fornire al Titolare le informazioni necessarie per dimostrare il rispetto dei propri obblighi di legge, in particolare dell'art. 28 GDPR, oltre che a contribuire alle attività di revisione, comprese le ispezioni (Audit), realizzate dal Titolare o da un altro soggetto da questi incaricato, e che dovranno essere notificate con un preavviso di almeno 30 giorni.

La valutazione del livello di adeguatezza delle misure di sicurezza, come sancito dall'art. 32 del GDPR, deve tener conto dei costi di realizzazione, dell'oggetto e degli scopi del trattamento, nonché della probabilità del verificarsi di un Data Breach (violazione dei dati personali).

Il Responsabile collaborerà pienamente durante gli Audit, consentendo compatibilmente con le finalità degli stessi, l'accesso ai locali e ai sistemi interessati, oltre a fornire le informazioni che possano essere necessarie al compimento dell'Audit stesso.

Altri obblighi di cooperazione con il Titolare

Il Responsabile interviene in appoggio al Titolare al fine dell'osservanza degli obblighi relativi alla sicurezza dei dati personali, nonché in caso di Data Breach, legato ai trattamenti posti in essere dal Responsabile, informa il titolare senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

Le attività di audit non comporteranno alcun onere economico in capo al Titolare. Qualora l'attività posta in essere da parte del Responsabile (risorse e tempistiche) si rivelasse ragionevolmente sproporzionata rispetto agli standard previsti per simili attività potrà essere richiesto da parte del Responsabile un adeguato compenso.

Privacy by Design e Privacy by Default

Il Responsabile si impegna ad osservare ai fini della selezione e dell'utilizzo nell'ambito della propria attività di strumenti, prodotti, applicazioni e/o servizi, i principi di Privacy by Design e Privacy by

Default, di cui all'articolo 25 del GDPR. Il principio di Privacy by Design ha la finalità di garantire un corretto livello di protezione dei dati in tutte le attività di trattamento e attuazioni effettuate all'interno di un'organizzazione. Il principio di Privacy by Default stabilisce, invece, che per impostazione predefinita le imprese dovrebbero trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini.

3. Impegni del Responsabile nel ruolo di Amministratore di sistema

Il Fornitore in ragione delle funzioni cui è tenuto nella prestazione dei Servizi contrattualizzati può assumere il ruolo di Amministratore di sistema.

In tal caso il Fornitore è tenuto ad osservare le disposizioni definite dal Provvedimento del Garante recante le "Misure ed accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema – 27 novembre 2008" così come modificato in base al provvedimento del 25 giugno 2009 e s.m.i.

Nei casi in cui l'attività svolta dal Responsabile, in virtù del Contratto, coinvolga quindi l'impiego di Amministratori di Sistema, il Responsabile si impegna a:

- Identificare e designare per iscritto i propri Amministratori di Sistema (di seguito "Ads"), fornendo loro istruzioni appropriate per iscritto e revocandone il ruolo in caso di necessità, con conferma al Titolare qualora richiesta;
- Vigilare sull'osservanza delle istruzioni impartite agli ADS, supervisionando le operazioni loro assegnate nell'ambito delle autorizzazioni conferite, richiamandoli all'obbligo di mantenere la massima riservatezza sui dati a cui accedono, anche per caso fortuito, nell'esercizio delle loro mansioni;
- Aggiornare periodicamente il documento che definisce le competenze dei singoli Amministratori di Sistema, comunicando loro per iscritto le eventuali modifiche apportate a tale documento;
- Mantenere una mappatura aggiornata degli Amministratori di Sistema, predisponendo la documentazione necessaria per la conformità normativa e creando profili di accesso in linea con le normative vigenti.

4. Diritti degli interessati

Il Responsabile si impegna a prestare al Titolare tutta la propria assistenza affinché possa tempestivamente e regolarmente assolvere ai propri obblighi di riscontro alle richieste degli Interessati relative all'esercizio dei loro diritti di cui agli artt. 15 ss GDPR (tra cui, diritto di accesso, diritto di rettifica, di cancellazione e di opposizione, diritto alla limitazione del trattamento, diritto alla portabilità dei dati, diritto di non essere sottoposto ad una decisione basata unicamente su trattamento automatizzato, inclusa la profilazione, ecc.).

Il Titolare e il Responsabile si impegnano a coordinarsi tra loro al fine di evadere la richiesta dell'Interessato nel più breve tempo possibile e, comunque, nel rispetto dei termini previsti dal GDPR.

Il Titolare sarà informato tempestivamente dalla Società di ciascuna richiesta ricevuta, in modo da poter dare immediato riscontro all'Interessato.

La responsabilità in ordine al soddisfacimento delle richieste degli Interessati è in capo al Titolare.

5. Responsabile per la protezione dei dati

Il Responsabile in ottemperanza agli artt. 37 e ss. GDPR ha nominato un Responsabile della Protezione dei Dati (di seguito anche "DPO - Data Protection Officer") che può essere contattato al seguente indirizzo: dpo@axera.it.

6. Sub-responsabili del trattamento

Il Responsabile è autorizzato dal Titolare a richiedere ad un soggetto terzo (in seguito denominato "sub-responsabile") di svolgere specifiche attività di trattamento dei dati personali, ai sensi dell'art.28 GDPR.

In particolare, il Cliente e la Società hanno definito il seguente elenco concordato di soggetti che possono operare quali *Sub-Responsabili* (oppure *Sub-Responsabili* di secondo livello) del trattamento:

- Società controllanti, controllate o collegate ai sensi dell'articolo 2359 del Codice civile ovvero società sottoposte a comune controllo, per le finalità amministrativo contabili ivi espressamente previste;
- Professionisti anche in forma associata (quali, a titolo di esempio non esaustivo, tecnici, consulenti, avvocati, commercialisti, notai, periti) eventualmente coinvolti nell'esecuzione dei Servizi;
- Ulteriori soggetti che svolgono attività in outsourcing, quali i fornitori di Servizi di natura informatica, inclusi l'hosting e l'archiviazione in cloud, di cui si avvale la Società per l'esecuzione dei Servizi;
- Società di assicurazioni, nonché società fornitrici di luce e gas;
- Banche e Istituti di credito, società di recupero e/o cessione di crediti;
- Spedizionieri, trasportatori, Poste, aziende per la Logistica.

L'elenco aggiornato dei *sub-responsabili* è a disposizione presso la Società e può essere fornito su richiesta.

Il Responsabile si impegna a vincolare per iscritto il *sub-responsabile* agli stessi obblighi in materia di protezione dei dati personali assunti dalla Società nei confronti del Titolare, attraverso il presente documento.

Il Responsabile deve assicurarsi che il *sub-responsabile* abbia le stesse idonee garanzie in merito all'attuazione di adeguate misure finalizzate ad assicurare che il trattamento avvenga con modalità conformi a quanto richiesto dalla normativa in materia di protezione dei dati personali; in caso di inadempimento da parte del *sub-responsabile*, sarà la Società a rispondere nei confronti del Titolare.

La comunicazione dei dati al terzo *sub-responsabile* potrà avvenire soltanto a condizione che vengano rispettate le disposizioni dell'art. 28, par. 4 GDPR, anche in caso di trasferimento dei dati al di fuori dell'UE e dello SEE.

Il Responsabile terrà aggiornato prontamente il Titolare di qualsivoglia modifica dell'elenco dei *sub-responsabili*, ed il Titolare avrà la facoltà di opporsi, salvo in caso di opposizione, la facoltà del Responsabile di recedere dal contratto senza preavviso.

7. Obblighi del Titolare

Il Titolare si impegna a:

- mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario;
- documentare per iscritto tutte le istruzioni relative al trattamento dei dati forniti o che saranno fornite al Responsabile;
- assicurare, prima dell'avvio e per tutta la durata del trattamento, il rispetto da parte del Responsabile del trattamento degli obblighi previsti dal GDPR e, più in generale, dalla normativa applicabile in materia di protezione dei dati;
- vigilare sui trattamenti dei dati, comprese le ispezioni nei confronti del Responsabile;
- ai sensi degli artt. 13 e 14 GDPR il Titolare provvederà a fornire le informazioni previste per la tutela dei dati alle persone interessate dalle attività di trattamento al momento della raccolta dei dati e di mettere a disposizione degli Interessati la lista aggiornata dei Responsabili esterni al trattamento dei dati.
- Assicurarsi di disporre di una valida base giuridica, ai sensi degli artt. 6 e ss del GDPR, per procedere al trattamento nei confronti degli Interessati.
- Verificare su base annuale l'operato dell'Amministratore di sistema, in modo da controllare la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

8. Trattamento all'interno dell'UE e dello SEE

Il Responsabile si impegna a trattare i dati personali secondo quanto previsto nelle istruzioni fornite dal Titolare nel presente documento, ed in ogni caso il trattamento è autorizzato solo all'interno dell'UE e dello Spazio Economico Europeo (di seguito "SEE").

Qualora il Responsabile fosse tenuto a trasferire dei dati personali trattati per conto del Titolare in un paese *extra*-UE e/o ad un'organizzazione internazionale a norma del diritto dell'Unione o della legislazione dello Stato membro cui è soggetto, dovrà previamente informare il Titolare di quest'obbligo giuridico prima del trattamento, a meno che le leggi interessate proibiscano una tale informazione per rilevanti motivi di interesse pubblico.

Qualora il Responsabile dovesse ritenere che un'istruzione costituisca una violazione del GDPR o di qualsiasi altra disposizione applicabile al trattamento in oggetto, del diritto dell'Unione o della legislazione degli Stati membri relativa alla protezione dei dati, ne informerà immediatamente il Titolare.

Qualora il Responsabile si dovesse avvalere di subfornitori situati al di fuori della UE/SEE, il trasferimento dei dati non potrà avvenire se non nei confronti di Paesi per cui esistono decisioni di adeguatezza da parte dell'UE, o da accordi specifici tra quest'ultima e il Paese ove i dati sono trasferiti o tramite la definizione di BCR (binding corporate rules) o di SCC (standard contractual clauses), ai sensi dell'art. 46 GDPR.

9. Trattamento dei dati al termine del rapporto

A discrezione del Titolare al termine della prestazione di Servizi, il Responsabile può essere tenuto a cancellare tutti i dati raccolti o comunque trattati ai sensi del presente accordo, o a restituirli al Titolare, rispettando in ogni caso la normativa in materia di protezione dei dati personali.

Eventuali copie senza il consenso del Titolare non possono essere create dal Responsabile, salvo i casi in cui ciò sia previsto dalla legge e nel caso di creazione di copie di sicurezza.

La Società ha facoltà di conservare tutta la documentazione utile al fine di provare la correttezza delle attività di trattamento anche oltre la scadenza del contratto, rispettando ugualmente i termini previsti dalla legge per la relativa conservazione e può alternativamente consegnare la stessa al Titolare.

10. Responsabilità

Le parti del presente accordo si danno reciprocamente atto nel vincolarsi a risarcire l'altra parte dei danni eventualmente causati dal proprio inadempimento colposo o doloso dei sopracitati obblighi, anche di quelli commessi da chiunque presti la propria opera nell'interesse o a vantaggio di ciascuna delle parti (art. 82 GDPR).

Titolo del documento: DPA

Versione del documento: V.1.1

Data di ultima modifica: 13/11/2024

.....

(Il Titolare)

Axera S.p.A.

(Il Responsabile)