# Accordosulla responsabilità del trattamento ai sensi dell’art. 28 RGPD

tra il

................................................................................................

- titolare del trattamento – nel prosieguo mandante –

e il

................................................................................................

- responsabile del trattamento – nel prosieguo mandatario

Accordo sulla responsabilità del trattamento ai sensi dell’art. 27 RGPD [rappresentante ai sensi dell’art. 27 RGPD *se necessario*:

................................................................................................]

## 1. Oggetto e durata del mandato

1. Oggetto

Oggetto del mandato relativo al trattamento dei dati è l’esecuzione dei seguenti compiti da parte del mandatario: Supporto tecnico remoto via telefono e Team Viewer.

2. Durata

Il mandato è impartito per un solo svolgimento. Fare clic qui per immettere testo.

## 2. Concretizzazione dei contenuti del mandato

(1) Tipo e scopo del trattamento dei dati previsto

Descrizione dettagliata dell’oggetto del mandato in merito a tipo e scopo delle attività del mandatario: Il client consente all'appaltatore di connettersi al computer del cliente inviando un ID del Team Viewer. Il cliente segue le attività del contraente e può interrompere attivamente la connessione in qualsiasi momento.

Il trattamento dei dati concordato nel contratto si svolge esclusivamente in uno Stato membro dell’Unione europea o in un altro Stato parte contraente dell’Accordo sullo Spazio economico europeo. Ciascun trasferimento in un paese terzo necessita di previo consenso del mandante e può avvenire soltanto nel rispetto delle condizioni speciali di cui all’art. 44 e ss. RGPD. Il livello di protezione adeguato nel paese terzo interessato (……………………….) è garantito da l'uso di clausole contrattuali standard UE (articolo 46, paragrafo 2, lettere c) ed) DSGVO cui si rimanda qui: Clausole contrattuali standard per il trasferimento di dati personali al responsabile del trattamento stabiliti in paesi terzi ai sensi della direttiva 95/46 / CE del Parlamento europeo e del Consiglio.

(2) Tipo di dati

Sono oggetto del trattamento di dati personali i tipi/le categorie di dati riportati in [Allegato 1](#_Anlage_1_–).

(3) Categorie di persone interessate

Le categorie di persone interessate dal trattamento sono riportate in [Allegato 1](#_1.2_Kategorien_betroffener):

## 3. Misure tecniche e organizzative

(1) Prima del trattamento, il mandatario è tenuto a documentare l’attuazione delle misure tecniche ed organizzative necessarie presentate prima dell’assegnazione, in particolare per quanto riguarda lo svolgimento concreto del mandato, e di lasciare che il mandante proceda alla verifica. Con l’accettazione da parte del mandante, le misure documentate diventano la base del mandato. Se una verifica/un audit del mandante evidenzia un’esigenza di adeguamento, questo va attuato di comune accordo.

(2) Il mandatario deve garantire la sicurezza ai sensi degli artt. 28 par. 3 lett. c e 32 RGPD, in particolare in relazione all’art. 5, par. 1 e 2 RGPD. Si tratta nel complesso delle misure da prendere per la sicurezza dei dati e per la garanzia di un livello di protezione adeguato in quanto a riservatezza, integrità, disponibilità e resilienza dei sistemi. In questo senso occorre tenere conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'entità e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, ai sensi dell’art. 32 par. 1 RGPD ([Allegato 3](#_Anlage_2–_Technisch-organisatorisch)).

(3) Le misure tecniche e organizzative sono soggette al progresso tecnologico e all’evoluzione. Il mandatario ha dunque facoltà di attuare misure alternative adeguate. Non deve comunque scendere sotto il livello di protezione delle misure fissate. Le modifiche rilevanti vanno documentate.

## 4. Rettifica, limitazione e cancellazione di dati

(1) Il mandatario, non sua sponte bensì su indicazione documentata del mandante, può rettificare, cancellare o limitare i dati trattati nel quadro del mandato. Se un interessato si rivolge direttamente al mandatario a questo fine, questi inoltrerà la richiesta senza indugio al mandante.

(2) Se compresi nell’entità delle prestazioni, la traccia della cancellazione, il diritto all’oblio, alla rettifica, alla portabilità dei dati e all’informazione sull’indicazione documentata del mandante vanno garantiti direttamente dal mandatario.

## 5. Controllo della qualità e altri obblighi del mandatario

Oltre a rispettare le presenti disposizioni, il mandatario è soggetto a obblighi giuridici ai sensi degli artt. 28 - 33 RGPD, per cui garantisce in particolare il rispetto delle norme che seguono:

1. Nomina scritta di un responsabile della protezione dei dati che svolga la propria attività ai sensi degli artt. 38 e 39 RGPD*. Se il mandatario non è tenuto a nominare un responsabile della protezione dei dati, designa una persona di contatto per le questioni giuridiche relative alla protezione dei dati*.

I dati di contatto del responsabile della protezione dei dati o della persona di contatto vanno comunicati al mandante [[Allegato 1](#_1.3_Datenschutzbeauftragter_/)] e qualsivoglia modifica va notificata senza indugio al mandante.

1. Se il mandatario ha sede fuori dall’Unione, designa il rappresentante nell’Unione ai sensi dell'art. 27, par 1. RGPD [Allegato 1]
2. La tutela della riservatezza ai sensi degli artt. 28 par. 3, frase 2, lett. b, 29, 32 par. 4 RGPD. Nello svolgimento dei lavori, il mandatario impiega soltanto collaboratori vincolati alla riservatezza che sono stati informati in precedenza delle disposizioni per loro rilevanti in materia di protezione dei dati. Il mandatario e ogni persona a questi sottoposta che abbia accesso ai dati personali possono trattare tali dati esclusivamente in base alle indicazioni del mandante, nel quadro delle autorizzazioni concesse nel presente contratto, a meno che non siano tenuti dalla legge al trattamento.
3. L’attuazione e il rispetto di tutte le misure tecniche e organizzative necessarie per questo mandato ai sensi degli artt. 28 par. 3, frase 2, lett. c e 32 RGPD ([Allegato 3](#_Anlage_3_–)).
4. Il mandante e il mandatario collaborano, su richiesta, con l’autorità di vigilanza per l’adempimento dei compiti di quest’ultima.
5. La notifica immediata al mandante su controlli e misure dell’autorità di vigilanza, se interessano il presente mandato. Questo si applica anche quando un’autorità competente indaga nel corso di una procedura amministrativa o penale sul trattamento di dati personali nel quadro dello svolgimento del mandato presso il mandatario.
6. Se il mandante da parte sua è soggetto a un controllo da parte delle autorità, a una procedura amministrativa o penale, alla responsabilità di un interessato o di un terzo, o di altro diritto legato allo svolgimento del mandato presso il mandatario , il mandatario si adopera per sostenerlo.
7. Il mandatario verifica regolarmente i processi interni e le misure tecniche e organizzative per garantire che, nella sua sfera di responsabilità, il trattamento si svolga in linea con quanto previsto dalla normativa sulla protezione dei dati in vigore e tutelare i diritti degli interessati.
8. Dimostrabilità dell’attuazione delle misure tecniche e organizzative nei confronti del mandante nel contesto dei suoi poteri di controllo di cui al punto 7 del presente contratto.

## 6. Rapporti di subappalto

(1) Ai sensi della presente disposizione, si intendono come rapporti di subappalto i servizi che si riferiscono direttamente all’erogazione della prestazione principale. Non vi rientrano i servizi secondari cui fa ricorso il mandatario, come telecomunicazioni, poste e trasporti, manutenzione e assistenza utenti, smaltimento di supporti dati e altre misure volte a garantire riservatezza, disponibilità, integrità e resilienza di hardware e software delle strutture di trattamento dei dati. Il mandatario è tuttavia tenuto ad attuare accordi contrattuali e misure di controllo adeguate e conformi alle legge per garantire la protezione e la sicurezza dei dati del mandante anche per servizi esternalizzati.

(2) Il mandatario può affidare incarichi a sub-mandatari (altri responsabili del trattamento) soltanto previo consenso scritto o altrimenti documentato del mandante.

1. Il mandante approva l’incarico dei sub-mandatari di cui in [Allegato 2](#_Anlage_2_–_1), a condizione di un accordo contrattuale secondo il disposto dell’art. 28 par. 2-4 RGPD.
2. L’esternalizzazione a sub-mandatari o la modifica del sub-mandatario esistente sono ammesse, purché:
* il mandatario informi il mandante in forma scritta di tale esternalizzazione o modifica con il dovuto anticipo e
* il mandante non si opponga in forma scritta all’esternalizzazione prevista prima della trasmissione dei dati nei confronti del mandatario e
* sussista un accordo contrattuale ai sensi dell’art. 28 par. 2-4 RGPD.

(3) L’inoltro di dati personali del mandante al sub-mandatario e l’attivazione di questi sono ammessi soltanto ove si compiano tutti i requisiti per un subappalto.

(4) Se il sub-mandatario eroga la prestazione concordata fuori dall’UE/dal SEE, il mandatario garantisce la liceità in materia di protezione dei dati mediante misure opportune. Lo stesso vale se sono impiegati fornitori ai sensi del par. 1 frase 2.

(5) Ulteriore esternalizzazione da parte del sub-mandatario necessita del consenso esplicito del mandante principale in forma scritta; tutte le disposizioni contrattuali nella catena dei contratti vanno applicate anche al rispettivo sub-mandatario.

## 7. Diritti di controllo del mandante

(1) Il mandante ha il diritto di svolgere controlli in consultazione con il mandatario o di farli svolgere da revisori nominabili nel singolo caso. Ha il diritto di verificare con controlli a campione, che di norma vanno annunciati per tempo, il rispetto del presente accordo da parte del mandatario nella sua attività.

(2) Il mandatario si assicura che il mandante possa convincersi del rispetto degli obblighi del mandatario ai sensi dell'art. 28 RGPD. Il mandatario si impegna a fornire le informazioni necessarie al mandante, in particolare dimostrando l’attuazione delle misure tecniche e organizzative.

(3) La dimostrazione di tali misure, che non interessano soltanto il mandato in sé, può avvenire mediante:

* rispetto delle norme di condotta approvate di cui all’art. 40 RGPD;
* certificazione in base a una procedura di certificazione autorizzata in linea con l’art. 42 RGPD;
* attestati, relazioni o estratti di rapporti aggiornati di istanze indipendenti (ad es. revisori contabili, visite, responsabili della protezione dei dati, dipartimento sicurezza IT, auditor della protezione dei dati, auditor di qualità) oppure
* adeguata certificazione mediante audit della sicurezza informatica o della protezione dei dati (ad es. ISO 27001 o protezione generale BSI).

(4) Per consentire i controlli da parte del mandante, il mandatario può far valere un diritto di compenso.

## 8. Comunicazione di violazioni del mandatario

(1) Il mandatario sostiene il mandante nel rispetto degli obblighi di cui agli articoli 32 - 36 RGPD per la sicurezza dei dati personali, obblighi di notifica in caso di violazione dei dati, valutazioni d’impatto in materia di protezione dei dati e consultazioni preventive. Vi rientrano tra le altre cose

1. la garanzia di un livello di protezione adeguato tramite misure tecniche e organizzative che tengano conto delle circostanze e finalità del trattamento, nonché della probabilità e gravità previste di una possibile violazione dovuta a falle nella sicurezza e che consentano la determinazione immediata degli illeciti;
2. l’obbligo di notificare senza indugio eventuali violazioni concernenti dati personali al mandante;
3. l’obbligo di sostenere il mandante nel quadro dell’obbligo di informazione nei confronti dell’interessato, fornendo senza indugio tutte le informazioni rilevanti del caso;
4. il supporto al mandante nella valutazione d’impatto sulla protezione dei dati;
5. il supporto al mandante nel quadro delle consultazioni preventive con l’autorità di vigilanza.

(2) Per i servizi di supporto non contenuti nella descrizione delle prestazioni e non attribuibili a una condotta erronea del mandatario, questi può richiedere un compenso.

## 9. Autorità del mandante

(1) Le indicazioni orali sono confermate dal mandante senza indugio (in forma scritta).

(2) Il mandatario deve informare immediatamente il mandante se ritiene che un’indicazione vada a violare la normativa sulla protezione dei dati. Il mandatario ha diritto di bloccare l’esecuzione dell’indicazione in questione fino a quando essa non sia confermata o modificata dal mandante.

## 10. Cancellazione e restituzione dei dati personali

(1) Non si creano copie o duplicati dei dati all’insaputa del mandante. Sono escluse le copie di sicurezza, se necessarie per garantire un regolare trattamento dei dati, nonché i dati necessari per adempiere agli obblighi di conservazione di legge.

(2) Alla conclusione dei lavori concordati in via contrattuale, o anche prima se richiesto dal mandante (al più tardi al termine delle prestazioni concordate), il mandatario deve consegnare al mandante o, previo consenso in linea con la protezione dei dati, distruggere tutti i documenti in proprio possesso, gli esiti del trattamento e dell’utilizzo nonché gli insiemi di dati connessi al rapporto di mandato. Lo stesso si applica al materiale di test e di scarto. Il verbale della cancellazione va presentato su richiesta.

(3) La documentazione che serve a comprovare il trattamento regolare dei dati va conservata dal mandatario nel rispetto dei termini di conservazione anche dopo la fine del contratto. Alla fine del contratto, ha facoltà di cederla al mandante per liberarsi dall’obbligo.

## 11. Disposizioni finali

(1) Eventuali accordi accessori a questo accordo quadro necessitano della forma scritta.

(2) Le parti contrattuali del presente accordo concordano che eventuali “Condizioni generali” del mandatario non trovano alcuna applicazione per il presente accordo.

(3) La risoluzione richiede la forma scritta.

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Luogo, data |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| Autorità del mandante |  | Autorità del mandante |
| Firma, nome, posizione |  | Firma, nome, posizione |
|  |  |  |

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Luogo, data |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| ppp Andrea Spengler mandante |  | Mandatario |
| Firma, nome, posizione |  | Firma, nome, posizione |

## Tipi di dati

[ ]  Dati anagrafici

[ ]  Dati di contatto (ad es. telefono, e-mail)

[ ]  Dati contrattuali (relazione contrattuale, interesse prodotto e contratto)

[ ]  Cronologia clienti e fornitori

[ ]  Dati di contabilità e pagamento

[ ]  Informazioni (di terzi, ad es. agenzie di informazioni o registri pubblici)

[ ]  Immagini

[ ]  Particolari categorie di dati personali (art. 9 RGPD)

[ ]  Dati personali relativi a condanne penali e reati (art. 10 RGPD)

[ ]  L'indirizzo IP del client.

## 1.2 Categorie di persone interessate

[ ]  Clienti

[ ]  Parti interessate

[ ]  Abbonati

[ ]  Impiegati

[ ]  Impiegati di aziende con cui il mandante collabora

[ ]  Impiegati di aziende di cui il mandante detiene azioni

[ ]  Fornitori

[ ]  Rappresentanti commerciali

[ ]  Referenti

[ ]  …

## 1.3 Responsabile protezione dei dati / persona di contatto presso il mandatario

Nome e cognome: Arnd Fackeldey

Posizione / funzione: Datenschutzbeauftragter

Sede / indirizzo: Digital Compliance Consulting GmbH / Heinrich-Dauer-Straße 10, 52351 Düren

Telefono: +49 (0)2421/555933

Indirizzo e-mail: fackeldey@digital-compliance-consulting.com

## 1.4 Rappresentante del responsabile del trattamento (*se necessario ai sensi dell’art. 27 RGPD*)

Nome e cognome: Andrea Spengler

Unità organizzativa: Customer Service

Sede / indirizzo: Nikolaus-Groß-Strasse 13, 44329 Dortmund

Telefono: +49 231/5436-0

Indirizzo e-mail: privacy@tandbergdata.com

|  |  |  |
| --- | --- | --- |
| Sub-mandatario | Indirizzo | Servizio  |
| Fare clic qui per immettere testo. | Fare clic qui per immettere testo. | Fare clic qui per immettere testo. |
| Fare clic qui per immettere testo. | Fare clic qui per immettere testo. | Fare clic qui per immettere testo. |
| Fare clic qui per immettere testo. | Fare clic qui per immettere testo. | Fare clic qui per immettere testo. |
| Fare clic qui per immettere testo. | Fare clic qui per immettere testo. | Fare clic qui per immettere testo. |

# 1. Riservatezza (art. 32, par. 1, lett. b RGPD)

* Controllo delle entrate
Nessuna entrata non autorizzata alle strutture di trattamento dei dati, ad esempio: schede magnetiche o chip, chiavi, apriporta elettrici, milizia aziendale e portinai, impianti d’allarme e di videosorveglianza;
* Controllo degli accessi
Nessun utilizzo non autorizzato del sistema, ad esempio: password (sicure), meccanismi automatici di blocco, autenticazione a due fattori, cifratura dei supporti dati;
* Controllo degli interventi
Nessuna lettura, copia, modifica o rimozione non autorizzata nel sistema, ad esempio: autorizzazioni strutturate e diritti di accesso in base alle esigenze, verbalizzazione degli interventi;
* Controllo della separazione
Trattamento separato dei dati raccolti per finalità diverse, ad esempio competenza del mandante, sandboxing;
* Pseudonimizzazione (art. 32 par. 1 lett. a e art. 25 par. 1 RGPD)

Il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative adeguate.

## 2. Integrità (art. 32, par. 1, lett. b RGPD)

* Controllo degli inoltri
Nessuna lettura, copia, modifica o rimozione non autorizzata in caso di trasferimento elettronico o trasporto, ad esempio: cifratura, virtuale private network (VPN), firma elettronica;
* Controllo di immissione
Determinare se e da chi i dati personali nei sistemi di trattamento sono stati immessi, modificati o rimossi, ad esempio: verbalizzazione e gestione dei documenti;

## 3. Disponibilità e resilienza (art. 32, par. 1, lett. b RGPD)

* Controllo di disponibilità
Protezione da distruzione o perdita accidentale o dolosa, ad esempio: strategia di backup (online/offline; on-site/off-site), gruppo di continuità (UPS), antivirus, firewall, canali di comunicazione e piani d’emergenza;
* Integrità (art. 32, par. 1, lett. b RGPD)

## 4. Procedura per testare, verificare e valutare con regolarità (art. 32 par. 1 lett. e art. 25 par. 1 RGPD)

* Gestione della protezione dei dati;
* Gestione della reazione agli incidenti;
* Impostazioni predefinite non lesive della sfera privata (art. 25, par. 2 RGPD);
* Controllo del mandato
Nessun trattamento dei dati ai sensi dell’art. 28 RGPD in assenza di indicazione corrispondente del mandante, ad esempio: formulazione univoca del contratto, gestione del mandato formalizzata, selezione rigorosa del fornitore, obbligo di convincimento a priori, controlli ex post.

Tandberg Data GmbH

Amtsgericht Dortmund HRB 5589

Geschäftsführer Kurt Kalbfleisch