

Accordo protezione dati personali

0. Prologo

Questo accordo sulla protezione dei dati personali, è parte integrante dell'offerta ricevuta (l'offerta). Le condizioni di questo accordo sono qui integrate nei Termini di Utilizzo e in qualsiasi altro accordo di servizio applicabile tra te e l'appaltatore. L'accordo viene concluso con l'accettazione dell'Offerta.

1. Oggetto e durata del contratto

1.1 Oggetto

L'oggetto dell'accordo è determinato dall'offerta e da tutti gli altri accordi di servizio applicabili tra il committente e l'appaltatore (di seguito denominato "Accordo di Prestazione").

1.2 Durata

La durata di questo accordo (termine) corrisponde alla durata del contratto.

2. Concretizzazione del contenuto dell'ordine

2.1 Natura e finalità del trattamento dei dati previsto

Tipo e scopo del trattamento dei dati personali da parte dell'appaltatore per conto del committente sono specificati nel contratto di servizio.

Il responsabile può salvare, elaborare o utilizzare i dati solo nell'ambito dell'accordo di servizio e in conformità con le istruzioni del cliente. Il trattamento dei dati concordato contrattualmente viene effettuato in uno stato membro dell'Unione Europea o in un altro stato che è parte dell'accordo sullo Spazio Economico Europeo. Qualsiasi trasferimento del servizio o di parti di esso in un paese terzo, richiede il consenso del cliente e può avvenire solo se i requisiti speciali richiesti nell'art. 44 e seguenti del GDPR, vengono rispettati (ad es. decisione di adeguatezza della Commissione, clausole standard di protezione dei dati, codici di condotta approvati).

I paesi terzi in cui viene effettuato il trattamento dei dati sono elencati nell'allegato 1.

2.2 Tipo di dati

I seguenti tipi / categorie di dati sono soggetti al trattamento dei dati personali:

- Dati di contatto (ad es. telefono, email)
- Dati di base del contratto (relazione contrattuale, interesse per il prodotto o il contratto)
- Storia del cliente
- Dati di fatturazione e di pagamento del contratto
- Coordinate bancarie
- Dati di pianificazione e controllo
- Dati patrimoniali
- Indirizzi IP
- Registri di attività
- Informazioni (da terzi, ad esempio istituti di credito, o elenchi pubblici)

2.3 Categorie di soggetti interessati

Le categorie di soggetti interessati dal trattamento di dati:

- Clienti
- Parti interessate
- Dipendenti
- Fornitori
- Rappresentanti di vendita
- Referente
- Partner commerciale

3. Misure tecnico-organizzative

- 3.1** Il responsabile documenta l'attuazione delle misure tecniche e organizzative descritte e richieste in vista dell'aggiudicazione dell'appalto prima dell'inizio della lavorazione, in particolare per quanto riguarda l'esecuzione concreta del contratto, e le consegna al cliente per la verifica. Se accettate dal cliente, le misure documentate diventano base di questo accordo. Se la verifica del cliente rivela la necessità di adeguamento, deve essere attuato di comune accordo.
- 3.2** Il responsabile deve fornire la garanzia ai sensi dell'art. 28 cpv. 3 lett. c, 32 GDPR, in particolare in combinazione con l'art. 5 cpv. 1, cpv. 2 GDPR. Nel complesso, le misure da adottare sono misure di sicurezza dei dati e misure per garantire un livello di protezione della riservatezza, dell'integrità, della disponibilità e della resilienza dei sistemi al rischio. Devono essere presi in considerazione lo stato della tecnica, i costi di attuazione e la natura, la portata e le finalità del trattamento, nonché la diversa probabilità la gravità di rischio per i diritti e le libertà delle persone fisiche ai sensi dell'articolo 32, paragrafo 1, della GDPR [dettagli nell'allegato 1].
- 3.3** Le misure tecniche e organizzative sono soggette allo sviluppo tecnico e all'ulteriore progresso. A questo proposito, il responsabile è autorizzato ad attuare misure alternative adeguate. In questo modo, il livello di sicurezza non deve scendere al di sotto del livello di sicurezza delle misure definite. I cambiamenti significativi devono essere documentati.

4. Correzione, limitazione e cancellazione dei dati

- 4.1** Il responsabile non può correggere, cancellare o limitare l'elaborazione dei dati elaborati per conto del cliente senza autorizzazione, ma solo in conformità alle istruzioni documentate del cliente. Se una persona interessata contatta direttamente il responsabile a tale riguardo, il responsabile deve inoltrare tale richiesta al cliente, senza alcuna esitazione.
- 4.2** Per quanto riguarda l'ambito delle prestazioni, il concetto di cancellazione, il diritto all'oblio, la correzione, la portabilità dei dati e le informazioni devono essere garantiti direttamente dal cliente secondo le istruzioni documentate.

5. Garanzia di qualità e altri obblighi del contraente

Oltre all'adempimento delle disposizioni del presente contratto, il responsabile ha obblighi legali ai sensi degli art. 28-33 GDPR; a tale riguardo, il responsabile garantisce in particolare il rispetto dei seguenti requisiti:

- 5.1** Nomina scritta di un responsabile della protezione dei dati che svolge i suoi compiti ai sensi degli articoli 38 e 39 del GDPR. I dati di contatto attuali del responsabile vi sono inseriti sulla homepage del responsabile.
- 5.2** Il rispetto della riservatezza ai sensi dell'art. 28 cpv. 3 cpv. 2 lett. b, 29, 32 cpv. 4 GDPR. Nell'effettuazione dei lavori, il responsabile impiegherà solo dipendenti che sono vincolati al segreto professionale e che hanno precedentemente familiarizzato con le disposizioni sulla protezione dei dati che li riguardano. Il responsabile e qualsiasi persona subordinata al responsabile che abbia accesso ai dati personali può trattare tali dati solo in conformità con le istruzioni del cliente, compresi i poteri concessi ai sensi del presente accordo, a meno che non sia legalmente obbligato a trattarli.
- 5.3** L'implementazione e il rispetto di tutte le misure tecniche e organizzative necessarie per questo incarico ai sensi dell'Art. 28 comma 3 seconda frase lettera c, 32 del GDPR [dettagli nell'Allegato 1].
- 5.4** Il responsabile e il cliente cooperano con l'autorità di vigilanza, su richiesta, nell'esecuzione dei suoi compiti.
- 5.5** L'informazione e avviso immediato del cliente su eventuali azioni di controllo e sulle misure dell'autorità di vigilanza. Ciò vale anche nel caso in cui un'autorità competente indagherà su un procedimento amministrativo o penale relativo all'elaborazione di dati personali in relazione all'elaborazione di ordini presso il responsabile.
- 5.6** Se il cliente, è soggetto a un'ispezione da parte dell'autorità di controllo, a un procedimento amministrativo o penale, a una richiesta di responsabilità da parte di una persona interessata o di un terzo o a qualsiasi altro reclamo in relazione all'elaborazione dell'ordine presso la sede del contraente, il responsabile deve assisterlo al meglio delle sue capacità.
- 5.7** Il responsabile verifica regolarmente i processi interni e le misure tecniche e organizzative al fine di garantire che il trattamento nell'ambito della sua area di responsabilità sia effettuato in conformità con i requisiti della normativa applicabile e che la legge sulla protezione dei dati e la tutela dei diritti della persona interessata sia garantita.
- 5.8** Verificabilità delle misure tecniche e organizzative adottate nei confronti del cliente nell'ambito dei suoi poteri di controllo ai sensi dell'art. 7 del presente accordo.
- 5.9** L'obbligo di assistere il cliente nel suo dovere di informare la persona interessata e, in questo contesto, di fornirle senza indugio tutte le informazioni rilevanti.

6. Subappalto

- 6.1** Per subappalto ai sensi di questa disposizione si intendono quei servizi che sono direttamente correlati alla fornitura del servizio principale. Non rientrano in questa categoria servizi accessori che l'appaltatore può utilizzare, come servizi di telecomunicazione, servizi postali o di trasporto, manutenzione e assistenza all'utente, smaltimento di supporti dati e altre misure per garantire la riservatezza, la disponibilità, l'integrità e la robustezza dell'hardware e del software dei sistemi di elaborazione dati. Tuttavia, l'appaltatore è tenuto ad adottare accordi contrattuali adeguati e conformi alla legge, nonché misure di controllo, anche per i servizi accessori esternalizzati, per garantire la protezione dei dati e la sicurezza dei dati del committente.
- 6.2** Il cliente accetta la messa in servizio dei subappaltatori elencati nell'allegato 2, con riserva di un accordo contrattuale ai sensi dell'art. 28 cpv. 2-4 GDPR.
- 6.3** L'esternalizzazione a subappaltatori o la modifica del subappaltatore esistente è consentita a condizione che:
- il responsabile notifihi per iscritto tale esternalizzazione a subappaltatori entro un certo periodo di tempo.
 - Il cliente non si oppone all'esternalizzazione prevista per al momento della consegna dei dati, e
 - si basa su un accordo contrattuale ai sensi dell'articolo 28, paragrafi 2-4, del GDPR.
 - Il responsabile assicura di selezionare attentamente i subappaltatori, prestando particolare attenzione all'adeguatezza delle misure tecniche e organizzative adottate ai sensi dell'articolo 32 del GDPR.
- 6.4** Il trasferimento dei dati personali del cliente al subappaltatore e la sua prima azione sono consentiti solo dopo che sono stati soddisfatti tutti i requisiti per un subappalto.
- 6.5** Se il subappaltatore fornisce il servizio concordato al di fuori dell'UE/SEE, il responsabile deve garantire l'ammissibilità ai sensi della legge sulla protezione dei dati attraverso misure adeguate. Lo stesso vale per i fornitori di servizi ai sensi del cpv. 1 frase 2.
- 6.6** Il responsabile deve garantire contrattualmente che i regolamenti concordati tra il cliente e il responsabile si applichino anche da parte dei subfornitori.

7. Diritti di controllo del cliente

- 7.1** Il cliente ha il diritto di effettuare controlli in accordo con l'appaltatore o di farli eseguire da ispettori designati caso per caso. Ha il diritto di verificare nel business dell'appaltatore la conformità a questa convenzione attraverso controlli a campione, che di norma devono essere annunciati in anticipo.
- 7.2** L'appaltatore garantisce che il committente possa verificare l'adempimento degli obblighi dell'appaltatore ai sensi dell'Art. 28 del RGPD. L'appaltatore si impegna a fornire al committente, su richiesta, le informazioni necessarie e in particolare a dimostrare l'attuazione delle misure tecniche e organizzative.
- 7.3** La prova di tali misure, che non riguardano solo l'ordine specifico, può essere fornita
- attraverso attestati, rapporti o estratti di rapporti attuali di istituzioni indipendenti (ad esempio, revisori contabili, revisione, responsabile della protezione dei dati, dipartimento di sicurezza informatica, auditor della protezione dei dati, auditor della qualità);
 - una certificazione adeguata tramite audit sulla sicurezza informatica o sulla protezione dei dati (ad esempio, secondo lo standard di base BSIGrundschutz).

8. Assistenza del cliente ai fini di adempimento degli obblighi di cui agli articoli 32–36

- 8.1** Il responsabile assiste il cliente nell'adempimento degli obblighi in materia di sicurezza dei dati personali di cui agli articoli da 32 a 36 del GDPR, degli obblighi di notifica in caso di violazione dei dati, delle valutazioni d'impatto sulla protezione dei dati e delle consultazioni preliminari. Questi includono:
- 8.1.1** mediante misure tecniche e organizzative che tengano conto delle circostanze e delle finalità dell'operazione di trattamento e della prevista probabilità e gravità di una possibile violazione dei diritti per violazione della sicurezza e consentano l'immediata individuazione di eventi di violazione rilevanti
 - 8.1.2** l'obbligo di comunicare le violazioni dei dati personali
 - 8.1.3** garantire un adeguato livello di protezione
 - 8.1.4** l'obbligo di assistere il cliente per quanto riguarda l'informazione dell'interessato e, a tale riguardo, di mettergli immediatamente a disposizione tutte le informazioni rilevanti
- 8.2** Il responsabile può richiedere un compenso per i servizi di supporto che non sono inclusi nelle specifiche di prestazione o che non sono dovuti ad una cattiva condotta da parte del responsabile.

9. Istruzioni da parte del cliente

- 9.1** Le istruzioni verbali sono confermate dal cliente immediatamente (almeno in forma di testo).
- 9.2** Il responsabile deve informare immediatamente il cliente se ritiene che un'istruzione violi le norme sulla protezione dei dati. Il responsabile ha il diritto di sospendere l'esecuzione della relativa istruzione fino alla conferma o alla modifica della stessa da parte del cliente.

10. Cancellazione e restituzione dei dati personali

- 10.1** Non verranno effettuate copie o duplicazioni dei dati senza che il cliente ne sia a conoscenza. Sono escluse le copie di sicurezza, nella misura in cui sono necessarie per garantire il corretto trattamento dei dati, nonché i dati necessari per l'adempimento degli obblighi di conservazione previsti dalla legge.
- 10.2** Al termine dei lavori concordati contrattualmente o prima su richiesta del cliente – immediatamente dopo la risoluzione del contratto – il responsabile è tenuto a consegnare tutti i documenti, i risultati elaborati e utilizzati, nonché dati entrati in suo possesso e collegati al rapporto contrattuale, oppure a distruggerli in conformità alle leggi sulla tutela dei dati personali. Lo stesso vale per i test e per i materiali di scarto. La registrazione della cancellazione deve essere fornita su richiesta.
- 10.3** La documentazione che serve come prova dell'ordinato e corretto trattamento dei dati sarà conservata dal contraente in conformità con i rispettivi periodi di conservazione oltre la fine del contratto. Può consegnarli al cliente alla fine del contratto per liberarlo.