Allegato per termini e condizioni sull'elaborazione dell'ordine

Tra
il cliente
-committente-

e

bexio AG
Alte Jonastrasse 24
8640 Rapperswil
Svizzera
-Provider-

tramite elaborazione degli ordini ai sensi dell'articolo 28 par. 3 Regolamento generale sulla protezione dei dati (RGPD).

preambolo

Il presente allegato specifica gli obblighi delle parti in materia di protezione dei dati derivanti dal contratto tra le parti (condizioni generali del provider). Si applica a tutte le attività correlate al contratto e in cui i dipendenti del provider o il provider elaborano i dati personali (di seguito denominati "dati") del cliente.

1 Oggetto, durata e specifiche dell'elaborazione dell'ordine

1. I dettagli relativi al servizio del fornitore sono regolati nel rispettivo contratto tra il provider e il cliente (in seguito denominato "contratto"), questo contratto è costituito dalle condizioni generali del provider.
2. Il contratto deve indicare l'oggetto e la durata del contratto, nonché la natura e le finalità del trattamento, se non diversamente specificato nell'allegato A.
3. La durata di questo investimento dipende dalla durata del contratto, a condizione che le disposizioni del presente allegato non diano luogo a obblighi supplementari.

2 Scopo e responsabilità

1. Il provider elabora i dati specificati nell'allegato A per conto del cliente per lo scopo ivi indicato nella misura in esso specificata. Questo include le attività specificate nel contratto.
2. Nell'ambito del presente contratto, il cliente è l'unico responsabile del rispetto delle disposizioni legali delle leggi sulla protezione dei dati, in particolare per la liceità del trasferimento dei dati al provider e per la liceità del trattamento dei dati ("responsabile" ai sensi dell'articolo 4 n. 7 RGPD).
3. Le istruzioni sono inizialmente determinate dal contratto e possono quindi essere modificate, integrate o sostituite dal cliente in forma scritta o in formato elettronico (modulo di testo) dall'ente designato dal provider (istruzioni individuali). Le istruzioni che non sono previste nel contratto sono trattate come una richiesta di modifica delle

prestazioni. Le istruzioni verbali devono essere fatte immediatamente per iscritto o in forma testuale dal cliente.

3 Obblighi del provider

1. Il provider può trattare i dati delle persone interessate solo nell'ambito dell'ordine e delle istruzioni del cliente; a meno che non vi sia un caso eccezionale ai sensi dell'articolo 28 par. 3 a) DS-GMO. Il provider informa senza indugio il committente se ritiene che un'istruzione violi le leggi applicabili. Il provider può sospendere l'implementazione delle istruzioni fino a quando non sia stato confermato o modificato dal cliente.
2. All'interno della propria area di responsabilità, il provider progetterà l'organizzazione interna in modo tale da soddisfare i particolari requisiti di protezione dei dati. Adotterà misure tecniche e organizzative per proteggere adeguatamente i dati del cliente, che soddisfano i requisiti del regolamento generale sulla protezione dei dati (articolo 32 RGPD). Il provider dovrà adottare misure tecniche e organizzative per garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi relativi al trattamento su base permanente. Il cliente è a conoscenza di queste misure tecniche e organizzative ed ha la responsabilità di garantire che forniscano un livello adeguato di protezione dai rischi dei dati da elaborare.
3. Le misure adottate dal provider sono descritte in modo più dettagliato nell'allegato B. Le misure tecniche e organizzative sono soggette al progresso tecnico e all'ulteriore sviluppo. A tale riguardo, il provider è autorizzato a implementare misure adeguate alternative. In tal modo, il livello di sicurezza delle misure specificate non deve essere superato. Cambiamenti significativi devono essere documentati.
4. Il provider supporta, per quanto concordato, il cliente nell'ambito delle sue possibilità nell'adempimento delle richieste e dei reclami delle persone interessate ai sensi del capitolo III della RGPD e del rispetto degli obblighi di cui agli articoli da 33 a 36 RGPD.
5. Il provider garantisce che i dipendenti coinvolti nell'elaborazione dei dati del cliente e di altre persone che lavorano per il provider sono vietati dal trattamento dei dati al di fuori delle istruzioni. Inoltre, il provider garantisce che le persone autorizzate al trattamento dei dati personali si sono impegnate a mantenere la riservatezza o sono soggette ad un obbligo legale di riservatezza appropriato. L'obbligo di riservatezza / segretezza persiste anche dopo il completamento dell'incarico.
6. Il provider deve informare immediatamente il cliente se viene a conoscenza di violazioni della protezione dei dati personali del cliente. Il provider dovrà adottare le misure necessarie per proteggere i dati e mitigare le possibili conseguenze negative delle persone interessate e dovrà immediatamente discuterne con il cliente.
7. Il provider deve fornire al cliente la seguente persona di contatto per le questioni relative alla protezione dei dati che si presentano nel contesto del contratto: Il responsabile della protezione dei dati di bexio AG, datenschutz@bexio.com.
8. Il provider garantisce di rispettare i suoi obblighi ai sensi dell'art. 32 par. 1 lit. d) RGPD, di stabilire una procedura per la revisione periodica dell'efficacia delle misure tecniche e organizzative per garantire la sicurezza del trattamento.

   Il provider corregge o cancella i dati contrattuali se istruiti dal cliente e se ciò è incluso nel campo di applicazione della direttiva. Se una cancellazione della protezione dei dati conforme o una restrizione corrispondente del trattamento dei dati non è possibile, il

provider si assume la distruzione dei dati di protezione dal supporto e altri materiali sulla base di una singola messa in servizio da parte del cliente o restituisce questi supporti di dati al cliente, se non è già stato concordato nel contratto.

In casi particolari che devono essere determinati dal cliente, sussiste una conservazione o un trasferimento, in questo caso le misure di compensazione e protezione devono essere concordate separatamente, se non è già stato concordato nel contratto.

9. Dati, supporti di dati e tutti gli altri materiali devono essere emessi o cancellati dopo la fine dell'ordine su richiesta del committente. Se i costi aggiuntivi si verificano a causa di specifiche divergenti in caso di pubblicazione o cancellazione dei dati, ciò sarà a carico del cliente.
10. Nel caso di un reclamo del cliente da parte di una persona interessata in relazione a qualsiasi richiesta ai sensi dell'articolo 82 RGPD, il provider si impegna ad assistere il cliente nella difesa della richiesta nell'ambito delle sue possibilità.
11. I vantaggi di cui ai numeri 3, 4 (2), 5, 6 (2) e 6 (3) (ad es. emissione dei supporti di dati, indirizzamento delle persone interessate, esami) devono essere corrisposti al provider in base alle sue tariffe orarie o spese esterne correnti.

4 Obblighi del committente

1. Il committente deve informare il provider immediatamente e completamente se trova nell'ordine risultati errori o irregolarità riguardanti le norme sulla protezione dei dati.
2. In caso di reclamo del committente da parte di un interessato in relazione a qualsiasi richiesta di cui all'articolo 82 RGPD, la sezione 3 (10) si applica mutatis mutandis.
3. Il committente deve fornire al provider la persona di contatto per le questioni relative alla protezione dei dati che si presentano nel contesto del contratto, a condizione che ciò si discosti dalle persone di contatto già nominate dal cliente.

5 Richieste di persone interessate

Se una persona interessata con richieste di cancellazione di correzione o di informazioni al provider, il provider rimanda l'interessato al cliente, se è possibile un incarico al cliente in base all'interessato. Il provider inoltra immediatamente la richiesta dell'interessato al cliente. Il provider supporta il cliente nell'ambito delle sue possibilità su istruzioni per quanto concordato. Il provider non è responsabile se la richiesta dell'interessato non riceve risposta dal cliente, non correttamente o non in tempo.

6 opzioni di dimostrazione

1. Il provider deve dimostrare al cliente il rispetto degli obblighi stabiliti nel presente allegato con mezzi adeguati. Ciò avviene attraverso una propria verifica e/o la certificazione ISO 27001.
2. Se, in singoli casi, sono richieste ispezioni da parte del cliente o un ispettore incaricato da quest'ultimo, queste devono essere eseguite durante il normale orario di lavoro senza interruzioni dell'operazione in seguito a richiesta, tenendo conto di un ragionevole tempo di consegna. Il provider può renderli dipendenti da una notifica preventiva con tempi di consegna ragionevoli e sulla firma di un accordo di riservatezza

riguardante i dati di altri clienti e le misure tecniche e organizzative che sono state istituite. Se l'esaminatore incaricato dal cliente è in una relazione concorrenziale con il provider, il provider ha il diritto di ricorrere contro quest'ultimo.

3. Se un'autorità di vigilanza sulla protezione dei dati o un'altra autorità di supervisione sovrana del cliente effettua un'ispezione, si applica di conseguenza il paragrafo 2. La firma di un obbligo di riservatezza non è richiesta se questa autorità di vigilanza è soggetta a un segreto professionale o legale in cui è punibile una violazione ai sensi del codice penale.

7 Subappaltatori (altri responsabili del trattamento)

1. La messa in servizio di subappaltatori da parte del provider è consentita, purché soddisfino i requisiti del presente allegato nella misura del subappalto. Un elenco degli attuali subappaltatori è disponibile qui:

   https://www.bexio.com/it-CH/linee-guida/subappaltatori

2. il cliente accetta che il provider coinvolga subappaltatori. Prima del coinvolgimento o la sostituzione dei subappaltatori, il provider informa il cliente. Il provider è obbligato a informare il cliente circa la messa in servizio di un subappaltatore aggiornando la panoramica di cui sopra. La panoramica deve essere aggiornata con almeno 14 giorni di anticipo. Il cliente vedrà regolarmente la panoramica. Il cliente può opporsi alla modifica, entro questi 14 giorni, per un motivo importante, nei confronti del provider. Se non ci sono obiezioni entro la scadenza, l'accettazione della modifica è considerata come data. Se esiste un motivo importante per la protezione dei dati e se una soluzione concordata tra le parti non è possibile, al provider viene concesso un diritto speciale di rescissione.
3. Un contratto di rapporto con un subappaltatore soggetto ad approvazione esiste se il provider commissiona a provider aggiuntivi il servizio totale o parziale del servizio concordato in questa appendice. Il provider stipulerà accordi con queste terze parti nella misura necessaria per garantire adeguate misure di sicurezza della privacy e delle informazioni. I subappaltatori che non hanno accesso ai dati dei clienti o non elaborano i dati dei clienti, sono esclusi da questo capitolo e non appariranno nell'elenco.
4. Se il provider emette ordini a subappaltatori, il provider è responsabile del trasferimento dei suoi obblighi di protezione dei dati ai sensi del presente allegato al subappaltatore.

8 Obblighi di informazione

Se i dati del cliente sono messi in pericolo da sequestro o confisca, da una procedura di fallimento o di regolamento o da altri eventi o misure di terze parti, il provider deve informare immediatamente il cliente. Il provider dovrà immediatamente informare tutte le persone responsabili a tale riguardo che la sovranità e la proprietà dei dati, come "responsabile", sono esclusivamente del cliente ai sensi del Regolamento Generale sulla Protezione dei Dati.

9 Responsabilità

La responsabilità è basata sul contratto.

10 Altro

1. Per il resto si applicano i regolamenti del contratto. In caso di contraddizioni tra i regolamenti del presente allegato e le disposizioni del contratto, prevarrà il presente allegato. Qualora le singole parti di questo allegato risultino inefficaci, ciò non pregiudica la validità del contratto e dell'allegato altrimenti.
2. Gli allegati A e B sono parte integrante del presente allegato.

Allegato A dell'accordo di trasformazione dei contratti

Oggetto del contratto:	Il trattamento dei dati personali del cliente nel contesto del suo utilizzo dei servizi del provider per quanto riguarda il software come servizio.
Natura e scopo dell'elaborazione dei dati prevista:	I dati personali elaborati dal cliente vengono trasferiti al provider per quanto riguarda il software come servizio. Il provider elabora questi dati esclusivamente in base all'accordo stipulato (gestione degli ordini, gestione dei contatti (CRM), contabilità, e-banking, contabilità salari, gestione magazzino, gestione progetti).
Tipo di dati personali:	I tipi di dati dipendono dai dati trasmessi dal cliente. Questi sono (a seconda del mandato): · Dati personali (nome, data di nascita, indirizzo, datore di lavoro) compresi i dettagli di contatto (per es. telefono, e-mail) · Dati del contratto, compresi i dettagli di fatturazione e pagamento · Storia dei dati del contratto
Categorie di persone interessate:	Le categorie di persone interessate dipendono dai dati forniti dal cliente. Questi sono (a seconda del mandato): · Dipendenti (inclusi richiedenti ed ex dipendenti) del cliente, · Clienti del committente · Parti interessate del committente · Fornitore di servizi del committente · Dati di contatto per le persone di contatto
Cancellazione, blocco e rettifica dei dati:	Le richieste di cancellazione, blocco e rettifica devono essere indirizzate al cliente; in caso contrario si applicano le disposizioni del contratto.

Allegato B dell'accordo di trasformazione dei contratti

Misure tecniche e organizzative (TOM)

1 Misure tecniche e organizzative

Le seguenti misure tecniche e organizzative (TOM) sono fondamentali per l'elaborazione dei dati

1. Controllo di accesso:
   Esistono le seguenti misure per il controllo degli accessi:
    a. Definizione delle aree di sicurezza
    b. Realizzazione di una protezione di accesso efficace
    c. Definizione di persone autorizzate
    d. Gestione e documentazione dell'autorizzazione all'accesso personale per l'intero ciclo di vita
    e. Accompagnamento visitatori e personale esterno
    f. Monitoraggio delle stanze al di fuori degli orari di chiusura
    g. Registrazione dell'accesso
2. Controllo di accesso:
    a. Protezione dell'accesso (autenticazione)
    b. Autenticazione semplice dei dipendenti (tramite nome utente/password) con un alto livello di protezione
    c. Blocco/blocco di inattività e processo per reimpostare gli identificatori di accesso bloccati
    d. Disabilita la funzione di memoria per password e / o immissione moduli
    e. Designazione di persone autorizzate
    f. Amministrazione e documentazione dei supporti di autenticazione personali e autorizzazioni di accesso
    g. Blocco dell'accesso automatico
    h. Blocco dell'accesso manuale
    i. Trasmissione sicura di segreti di autenticazione (credenziali) nella rete
    j. Registrazione di accesso
3. Controllo di accesso:
   Esistono le seguenti misure per il controllo degli accessi:
    a. Creazione di un concetto di autorizzazione

b. Implementazione di restrizioni di accesso
c. Assegnazione di autorizzazioni minime
d. Amministrazione e documentazione dei diritti di accesso personali
e. Registrazione dell'accesso ai dati

4. Controllo trasporto/trasferimento:
   Esistono le seguenti misure per il controllo del trasferimento:
   a. Trasferimento dati sicuro tra server e client
   b. Protezione della trasmissione nel back-end
   c. Protezione della trasmissione verso sistemi esterni
   d. Implementazione di gateway di sicurezza nei punti di interscambio della rete
   e. Rafforzamento dei sistemi di backend
   f. Descrizione di tutte le interfacce e dei campi di dati personali trasmessi
   g. Autenticazione macchina-macchina
   h. Gestione disco (procedura)
   i. Processo per la raccolta e la gestione
   j. Procedura di cancellazione / distruzione della privacy
5. Controllo input:
   Le seguenti misure esistono per il controllo input:
   a. Documentazione delle autorizzazioni di input
   b. Registrazione degli ingressi
6. Controllo dell'ordine:
   Le seguenti misure esistono per il controllo input:
   a. Documentazione delle autorizzazioni di input
   b. Registrazione degli ingressi
7. Controllo di disponibilità:
   Esistono le seguenti misure di controllo della disponibilità:
   a. concetto di backup
   b. Piano di emergenza
   c. Archiviazione di backup
   d. Verifica delle strutture di emergenza
8. Requisito di separazione:
   Le seguenti misure esistono per il controllo di scopo:

a. Economia nella raccolta dei dati
b. Elaborazione separata