Contratto di elaborazione degli ordini

bexio AG

Il presente Accordo sull'elaborazione degli ordini (di seguito "AEO") specifica gli obblighi relativi alla protezione dei dati che derivano dal rapporto contrattuale tra bexio AG (di seguito "Provider") e i suoi clienti (di seguito "Committente"). La relazione contrattuale tra le parti si basa sulle condizioni generali di contratto (qui di seguito denominate "CGC") e la dichiarazione sulla protezione dei dati (qui di seguito denominata "DPD") e queste costituiscono quindi parte integrante dell'AEO. L'AEO si applica a tutte le attività derivanti dal rapporto contrattuale tra le parti in cui i dipendenti del Provider o i terzi incaricati dal Provider elaborano i dati personali (di seguito "Dati") del committente. Per tutte le questioni relative alla protezione dei dati, il committente può contattare il responsabile della protezione dei dati del provider all'indirizzo datenschutz@bexio.com.

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

1.1. L'oggetto e la durata dell'ordine così come la natura e lo scopo dell'elaborazione risultano generalmente dalle CGC, a condizione che le seguenti disposizioni non comportino ulteriori obblighi.

1.2. Nell'allegato A dell'AEO sono specificati l'oggetto, la natura e lo scopo dell'elaborazione degli ordini.

2. Scopo e responsabilità

2.1. Il provider elabora i dati personali per conto del committente. Ciò include le attività che sono specificate nelle CGC, nella DPD, nell' allegato A dell'AEO e nella descrizione vigente del servizio sul sito web del provider.

2.2. Nell'ambito del rapporto contrattuale, il committente è l'unico responsabile del rispetto delle disposizioni legali delle leggi sulla protezione dei dati, in particolare della legittimità del trasferimento dei dati al fornitore e della legalità del trattamento dei dati.

2.3. Compilando la maschera di inserimento per la creazione e l'ordinazione di un account utente ("account bexio") sul sito web del Provider, il committente dà al provider l'istruzione corrispondente per il trattamento dei dati. Il committente può integrare, modificare o revocare le sue istruzioni nel suo account bexio o comunicandole al provider. Le istruzioni che non sono previste nelle CGC sono trattate come una richiesta di modifica delle prestazioni. Le istruzioni orali devono essere fornite immediatamente per iscritto o tramite l'apposita procedura nell'account bexio da parte del committente.

3. Obblighi del provider

3.1. Il provider elabora i dati delle persone interessate solo nell'ambito del rapporto contrattuale ai sensi delle CGC, della DPD e del presente AEO, a meno che non vi sia un caso eccezionale regolato dalla legge.

3.2. All'interno della propria area di responsabilità, il provider predisporrà l'organizzazione interna in modo tale da soddisfare i particolari requisiti in merito alla protezione dei dati.

Adotterà misure tecniche e organizzative volte a proteggere adeguatamente i dati del committente nel rispetto dei relativi requisiti legali. In particolare, garantirà la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi relativi al trattamento su base permanente. Il committente è a conoscenza di queste misure tecniche e organizzative e ha la responsabilità di garantire che forniscano un livello adeguato di protezione dai rischi dei dati da elaborare.

3.3. Le misure adottate dal provider sono precisate nell'allegato B. Le misure tecniche e organizzative sono soggette al progresso tecnico e all'ulteriore sviluppo. A questo proposito, il provider è autorizzato ad attuare in qualsiasi momento misure alternative adeguate. Il livello di sicurezza non deve essere inferiore a quello concordato contrattualmente con il presente AEO.

3.4. Nella misura in cui è stato concordato, il provider sosterrà il committente, nell'ambito delle sue possibilità, nell'adempimento delle richieste e delle rivendicazioni delle persone interessate e nell'osservanza degli obblighi previsti dalla legge sulla protezione dei dati. Secondo le CGC, il provider ha il diritto di richiedere un'indennità per le spese sostenute.

3.5. I dipendenti coinvolti nell'elaborazione dei dati del committente e altri terzi che lavorano per il provider elaborano i dati esclusivamente nell'ambito del rapporto contrattuale in conformità con le CGC, la DPD e il presente AEO e sono obbligati a mantenere la riservatezza.

3.6. Se il Provider dovesse venire a conoscenza di qualsiasi violazione della protezione dei dati personali, prenderà misure ragionevoli per assicurare i dati e per mitigare qualsiasi possibile conseguenza negativa per gli interessati. Inoltre, il provider rispetta pienamente le disposizioni di legge vigenti in materia di notifica di violazioni della protezione dei dati.

3.7. Il provider rispetta pienamente le disposizioni vigenti in materia di protezione dei dati e verifica regolarmente l'efficacia delle misure tecniche e organizzative volte a garantire la sicurezza del trattamento.

3.8. Il provider elabora e memorizza i dati personali finché sussiste il rapporto contrattuale tra il provider e il committente. Il provider corregge o cancella i dati contrattuali se istruiti dal committente e se ciò è incluso nel campo di applicazione della direttiva. Fanno eccezione i dati necessari per l'ulteriore trattamento ai sensi delle disposizioni di legge o per scopi interni inderogabili. La consegna dei dati e il relativo compenso sono regolati nelle CGC.

4. Obblighi del committente

4.1. Il committente deve informare il provider immediatamente e completamente per iscritto o tramite l'account bexio se trova nell'ordine risultati errori o irregolarità riguardanti le norme sulla protezione dei dati.

4.2. 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, qualora differisca dalla persona di contatto già nominata dal cliente.

4.3. Il cliente dichiara di essere l'unico responsabile per l'informazione delle persone interessate dal trattamento dei dati in merito alla possibile memorizzazione, utilizzo, elaborazione e trasmissione dei dati da parte del provider in conformità con le disposizioni delle CGC, della DPD e del presente AEO. Se le singole persone interessate non sono d'accordo con il trattamento dei dati previsto, il committente è responsabile della cancellazione dei rispettivi dati nel proprio account bexio.

4.4. Accettando le CGC e la DPD, il committente dichiara **espressamente il suo consenso alla trasmissione dei suoi dati alla società madre del provider** e alle società affiliate. Il

committente esonera il provider da ogni possibile rivendicazione. L'ottenimento del consenso delle persone interessate è di competenza del committente.

5. Richieste di persone interessate

5.1. Se una persona interessata si rivolge con richieste di cancellazione di correzione o di informazioni al provider, il provider rimanda la persona interessata al committente, se è possibile un incarico al committente in base alle indicazioni della persona interessata. Il provider inoltra la richiesta della persona interessata al committente entro un termine ragionevole. Il provider può supportare il committente, nell'ambito delle sue possibilità, in caso di richieste di protezione dei dati di una persona interessata. In questo caso, il provider ha il diritto di richiedere un'indennità per le spese sostenute. Il provider non è responsabile se la richiesta dell'interessato non riceve risposta dal committente, non correttamente o non per tempo.

6. Opzioni di dimostrazione

6.1. Il provider deve dimostrare al committente il rispetto degli obblighi stabiliti nel presente allegato con mezzi adeguati. Ciò avviene attraverso una propria verifica e/o la certificazione ISO.

6.2. Se, in singoli casi, sono richieste ispezioni da parte del committente o un ispettore incaricato da quest'ultimo (ad es. a causa dell'assoggettamento al RGPD), 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 committente ha un rapporto di concorrenza con il provider, quest' ultimo può rifiutarlo e proporre una persona neutrale. Eventuali costi associati alla verifica possono essere addebitati dal provider al committente, in particolare se non sono state rilevate irregolarità.

6.3. Se un'autorità di vigilanza sulla protezione dei dati o un'altra autorità di supervisione sovrana del committente effettua un'ispezione, si applica di conseguenza il punto 6.2. 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)

7.1. Il provider può avvalersi di subappaltatori per l'adempimento della prestazione contrattuale. La messa in servizio di subappaltatori come responsabili del trattamento da parte del Provider è consentito nella misura in cui questi, nell'ambito del subappalto, soddisfino a loro volta i requisiti del presente AEO. Il provider stipula accordi con i subappaltatori nella misura necessaria per garantire adeguate misure di protezione dei dati e di sicurezza delle informazioni. I subappaltatori che non hanno accesso ai dati dei clienti o che non elaborano i dati personali in qualità di responsabili del trattamento sono esclusi da questo capitolo. Un elenco degli attuali subappaltatori ai sensi di un processore (di seguito chiamati semplicemente "subappaltatori") è disponibile qui:
https://www.bexio.com/it-CH/linee-guida/subappaltatori

7.2. Il Committente accetta che il Provider si avvalga dei subappaltatori indicati sul sito web del Provider. Prima di ricorrere ad altri subappaltatori, il provider informa il committente aggiornando il proprio sito web. La panoramica sul sito web deve essere aggiornata almeno

14 giorni prima della consultazione. Il committente consulterà regolarmente la panoramica. Il committente può opporsi alla modifica per giusta causa entro 14 giorni dalla data in cui ne sia venuto a conoscenza. 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.

8. Obblighi di informazione

8.1. Se i dati del committente 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 committente. Il provider informerà immediatamente tutti i responsabili in questo contesto che la sovranità e la proprietà dei dati sono esclusivamente del committente.

9. Responsabilità civile

9.1. La responsabilità è disciplinata dalle disposizioni corrispondenti nelle CGC.

10. Altro

10.1. Per il resto valgono le disposizioni delle CGC e della DPD. In caso di eventuali contraddizioni tra l'AEO e le CGC, prevarranno le disposizioni contenute nelle CGC. Qualora singole parti dell'AEO risultino inefficaci, ciò non pregiudica la validità delle CGC e delle altre disposizioni dell'AEO.

10.2. Gli allegati A e B sono parte integrante dell'AEO.

Ultima versione: giugno 2022

bexio AG
Alte Jonastrasse 24
8640 Rapperswil
Svizzera

Allegato A Oggetto, natura e scopo
Allegato B Misure tecniche e organizzative (MTO)

Allegato A – Oggetto, natura e finalità

Oggetto del contratto:	Il trattamento dei dati personali del committente nel contesto del suo utilizzo dei servizi del provider come software.
Natura e scopo dell'elaborazione dei dati prevista:	I dati personali elaborati dal committente vengono trasferiti al provider per quanto riguarda il software come servizio. Il provider elabora questi dati esclusivamente in conformità con le CGC e la corrispondente descrizione delle prestazioni sul sito web del provider (gestione degli ordini, gestione dei contatti (CRM), contabilità, e-banking, contabilità salariale, gestione delle scorte, gestione dei progetti, ecc.).
Tipo di dati personali:	I tipi di dati dipendono dai dati trasmessi dal committente. Questi sono, nella fattispecie (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 committente. Questi sono, nella fattispecie (a seconda del mandato): ● Collaboratori (inclusi candidati ed ex dipendenti) del committente ● 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 committente; per il resto valgono le disposizioni contenute nelle CGC, nella DPD e nel presente AEO.

Allegato B - Misure tecniche e organizzative (MTO)

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

I. Controllo dell'accesso:

- Definizione delle aree di sicurezza
- Realizzazione di un'efficace protezione d'accesso
- Determinazione delle persone autorizzate ad accedere
- Gestione e documentazione delle autorizzazioni di accesso personali per l'intero ciclo di vita
- Sorveglianza dei locali al di fuori degli orari di chiusura
- Registrazione dell'accesso

II. Controllo degli accessi:

- Protezione dell'accesso (autenticazione)
- Autenticazione semplice dei dipendenti (tramite nome utente/password) con un alto livello di protezione
- Blocco in caso di tentativi falliti/inattività e processo di ripristino degli identificativi di accesso bloccati
- Determinazione delle persone autorizzate
- Gestione e documentazione dei supporti di autenticazione personali e delle autorizzazioni di accesso
- Blocco automatico dell'accesso
- Blocco manuale dell'accesso
- Trasmissione sicura dei segreti di autenticazione (credenziali) sulla rete
- Registrazione di accesso

III. Controllo degli accessi:

- Creazione di un concetto di autorizzazione
- Implementazione di restrizioni di accesso
- Assegnazione di autorizzazioni minime
- Gestione e documentazione delle autorizzazioni di accesso personali
- Registrazione dell'accesso ai dati

IV. Controllo trasporto/trasferimento:

- Trasferimento sicuro dei dati tra server e client
- Protezione della trasmissione nel back-end
- Protezione della trasmissione verso sistemi esterni
- Implementazione di gateway di sicurezza nei punti di interscambio della rete
- Rafforzamento dei sistemi di backend
- Descrizione di tutte le interfacce e dei campi di dati personali trasmessi
- Autenticazione macchina-macchina
- Gestione disco (procedura)
- Processo di raccolta e smaltimento
- Procedura di cancellazione/ distruzione conforme alla protezione dei dati

V. Controllo input:

- Documentazione automatica delle autorizzazioni di immissione
- Registrazione degli ingressi

VI. Controllo dell'ordine:

- Documentazione delle autorizzazioni di immissione
- Registrazione degli ingressi

VII. Controllo di disponibilità:

- Concetto di backup
- Piano di emergenza
- Archiviazione di backup
- Controllo dei dispositivi di emergenza

VIII. Divieto di separazione:

- Economia nella raccolta dei dati
- Elaborazione separata