Accordo sul trattamento dei dati

bexio AG

Il presente Accordo sul trattamento dei dati specifica gli obblighi relativi alla protezione dei dati che derivano dal rapporto contrattuale tra bexio AG (di seguito "provider" o "responsabile del trattamento") e i suoi clienti (di seguito "committente/i" o "titolare/i"). Per tutte le questioni relative alla protezione dei dati, il committente può contattare l'addetto alla protezione dei dati del provider all'indirizzo datenschutz@bexio.com.

1. Oggetto

1.1. Esiste un rapporto giuridico tra le parti, per la cui esecuzione i dati personali vengono trasmessi dal titolare al responsabile ("contratto principale"). La relazione giuridica tra le parti si fonda sulle Condizioni generali ("CG") del provider. Il presente Accordo sul trattamento dei dati viene stipulato tra le parti al fine di garantire un'adeguata protezione in caso di trasferimento di dati personali.

1.2. A meno che il presente accordo non disponga diversamente, tutti i termini hanno un significato conforme alla Legge svizzera sulla protezione dei dati ("LPD"). Inoltre, il presente accordo permette alle parti di rispettare il Regolamento generale sulla protezione dei dati dell'UE ("GDPR") nei confronti dei dati personali protetti dei clienti dell'area UE.

2. Descrizione del trattamento dei dati

2.1. Il provider elabora i dati personali per conto del committente. L'oggetto e la durata del rapporto contrattuale, così come la natura e lo scopo dell'elaborazione, risultano generalmente dalle CG e dall'Allegato A all'Accordo sull'elaborazione dei dati. Il trattamento dei dati viene inoltre definito in modo dettagliato nella descrizione attuale del servizio sul sito web del provider e nella Dichiarazione sulla protezione dei dati ("DPD").

2.2. Compilando il modulo di registrazione per la creazione e l'ordinazione di un account utente ("account bexio") sul sito web del provider, il committente fornisce al provider l'istruzione corrispondente per il trattamento dei dati. Il committente può integrare, modificare o revocare le proprie istruzioni nel proprio account bexio o comunicandole al provider. Ogni istruzione non prevista dalle CG viene considerata come una richiesta di modifica delle prestazioni. A istruzioni comunicate verbalmente deve far seguito immediatamente una conferma per iscritto o devono essere confermate dal committente tramite l'apposita procedura nell'account bexio.

3. Obblighi del committente

3.1. 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 provider e della legalità del trattamento dei dati.

3.2. Il committente ritiene che le misure tecniche e organizzative ("MTO") utilizzate dal responsabile del trattamento, descritte nell'Allegato B, siano sufficienti a garantire un'adeguata protezione dei dati personali trasmessi.

3.3. Il committente deve informare immediatamente il provider, in modo completo e per iscritto, oppure tramite l'account bexio, di eventuali errori o irregolarità riguardanti le norme sulla protezione dei dati rilevate nell'ordine.

3.4. Il committente deve fornire al provider il nominativo della persona di contatto per questioni relative alla protezione dei dati che dovessero presentarsi nell'ambito della relazione contrattuale, qualora tale persone differisca dalla persona di contatto già nominata dal committente.

3.5. Il committente dichiara di assumersi l'intera responsabilità per l'informazione delle persone interessate dal trattamento dei dati riguardo alla possibile memorizzazione, utilizzo, elaborazione e trasmissione dei dati da parte del provider in conformità alle disposizioni delle CG, della DPD e del presente Accordo sul trattamento dei dati. Se singole persone interessate non fossero d'accordo con il trattamento dei dati previsto, il committente è responsabile della cancellazione dei rispettivi dati nel proprio account bexio.

3.6. Accettando le CG e l'Accordo sul trattamento dei dati, il committente dichiara **espressamente il proprio consenso alla trasmissione dei propri dati alla società madre del provider** e alle società affiliate. Il committente esonera il provider da ogni possibile reclamo. L'ottenimento del consenso delle persone interessate è di competenza del committente.

4. Obblighi del provider

4.1. Aspetti generali

4.1.1. Per quanto riguarda il trattamento dei dati personali, il responsabile del trattamento garantisce che

- tratterà questi dati personali in conformità con il presente accordo sul trattamento dei dati ed esclusivamente per le finalità perseguite dal titolare,
- le finalità perseguite dal titolare risultano dall'Allegato A, dall'account bexio o dalle istruzioni esplicite del titolare o sono determinate da un altro accordo con il titolare,
- fornirà al titolare le informazioni necessarie per verificare il rispetto degli obblighi di cui al presente Accordo,

- nei propri mezzi di lavoro, prodotti, applicazioni o servizi tiene conto dei principi di Data Privacy by Design e by Default,

- informerà il titolare nel caso non fosse più in grado di rispettare il presente accordo o se dovesse ritenere di non poterlo più rispettare in futuro, e

- collaborerà con le autorità di vigilanza competenti entro i limiti consentiti dalla legge.

4.1.2. I nominativi delle persone autorizzate dal titolare vengono comunicate per iscritto al responsabile all'inizio del trattamento dei dati o tramite l'account bexio. In caso di cambiamenti o di impedimento a lungo termine della persona di contatto, il provider deve essere informato immediatamente per iscritto o tramite l'account bexio con l'indicazione del nominativo del successore o del rappresentante. Istruzioni fornite verbalmente sono vincolanti solo se confermate immediatamente per iscritto dal titolare. L'e-mail vale come forma scritta.

4.1.3. Il provider deve informare immediatamente il committente nel caso ritenesse che un'istruzione violi le norme di legge. Il provider ha il diritto di sospendere l'esecuzione delle istruzioni interessate fino a quando la loro legalità non viene confermata dal titolare o fino a quando le istruzioni non vengono modificate.

4.2. Sicurezza dei dati

4.2.1. Nell'ambito della propria area di responsabilità, il provider predisporrà l'organizzazione interna in modo tale da soddisfare i requisiti specifici in materia di protezione dei dati. Adotterà misure tecniche e organizzative volte a proteggere adeguatamente i dati personali del committente nel rispetto dei relativi requisiti legali. Nel fare ciò, il responsabile del trattamento tiene conto dello stato dell'arte, dei costi di attuazione e della natura, ambito e finalità del trattamento, nonché della probabilità e della gravità del rischio rispetto ai diritti fondamentali e della personalità delle persone interessate. Le misure sono descritte nell'Allegato B e vengono verificate periodicamente. Modifiche alle misure sono consentite a condizione che non diminuiscano il livello di sicurezza precedente. 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 nei confronti dei dati oggetto del trattamento.

4.2.2. Nell'esecuzione dei compiti, il provider impiegherà esclusivamente dipendenti vincolati a mantenere la riservatezza e che sono stati precedentemente informati delle disposizioni sulla protezione dei dati rilevanti per loro.

4.2.3. Nella misura in cui ciò è stato concordato, il provider sosterrà il committente, nell'ambito delle proprie 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 CG, il provider ha il diritto di richiedere un'indennità per le spese sostenute.

4.2.4. Se il provider dovesse venire a conoscenza di qualsiasi violazione della protezione dei dati personali, prenderà misure ragionevoli per assicurare i dati e mitigare ogni 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.

5. Subappaltatori (altri responsabili del trattamento)

5.1. Il provider può avvalersi di subappaltatori per l'adempimento della prestazione contrattuale. Il responsabile del trattamento può delegare il trattamento a terzi solo previa autorizzazione del titolare. L'affidamento di compiti in qualità di responsabili del trattamento in subappalto da parte del provider è consentito nella misura in cui tali ulteriori responsabili del trattamento, nell'ambito del subappalto, soddisfino a loro volta i requisiti del presente ATD. Il provider stipula accordi con i subappaltatori nella misura necessaria a garantire adeguate misure di protezione dei dati e di sicurezza delle informazioni. I subappaltatori che non hanno accesso ai dati personali o che non elaborano i dati personali in qualità di responsabili del trattamento sono esclusi dal presente capitolo. Un elenco degli attuali subappaltatori che agiscono in qualità di responsabili del trattamento dei dati (di seguito chiamati semplicemente "subappaltatori") è disponibile qui:

https://www.bexio.com/de-CH/lineeguida/subappaltatori

5.2. 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 pervengono obiezioni entro tale scadenza, la modifica viene considerata accettata. Qualora dovesse sussistere un motivo importante relativo alla protezione dei dati e una soluzione concordata tra le parti non fosse possibile, al provider viene concesso un diritto speciale di rescissione.

5.3. Di norma, non sono considerati subappalti i servizi accessori per il provider che non coinvolgono i dati del titolare ai sensi dell'Allegato A (p. es. servizi di telecomunicazione, servizi postali/di trasporto, manutenzione e servizi per gli utenti o lo smaltimento dei supporti dati e altre misure per garantire la riservatezza, la disponibilità, l'integrità e la durabilità dell'hardware e del software). Tuttavia, il provider è obbligato ad adottare misure di controllo adeguate per garantire la protezione e la sicurezza dei dati del committente, anche in caso di servizi accessori.

6. Divulgazione all'estero

6.1. Il trattamento dei dati di cui all'Allegato A avviene generalmente in Svizzera o in uno Stato membro dell'Unione europea o in un altro Stato parte dell'accordo sullo Spazio Economico Europeo. Qualsiasi trasferimento in un altro paese terzo può avvenire solo se sono soddisfatti i relativi requisiti legali.

6.2. Se il responsabile del trattamento impiega subappaltatori in Stati che non dispongono di un livello adeguato di protezione dei dati in conformità alle disposizione dell'Incaricato federale della protezione dei dati e della trasparenza, dell'Allegato all'OLPD o della Commissione UE, il responsabile del trattamento garantisce l'ammissibilità della divulgazione ai sensi della legge sulla protezione dei dati adottando misure adeguate al rispettivo trasferimento dei dati.

7. Diritti degli interessati

7.1. Quando una persona interessata si rivolge con richieste di cancellazione, di correzione o di informazioni al provider, il provider indirizza la persona interessata al committente, a condizione che un incarico al committente sia possibile sulla base delle indicazioni fornite dalla 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 proprie 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, se tale risposta non è corretta o non giunge per tempo.

8. Opzioni di dimostrazione

8.1. 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.

8.2. 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 delle operazioni, su richiesta e con un preavviso ragionevole. Il provider può subordinare ciò a una notifica preventiva con preavviso ragionevole e alla firma di un accordo di riservatezza riguardo ai dati di altri clienti e alle misure tecniche e organizzative adottate. Se l'ispettore incaricato dal committente ha un rapporto di concorrenza con il provider, quest' ultimo può rifiutarlo e proporre una persona neutrale. Eventuali costi associati all'ispezione possono essere addebitati dal provider al committente, in particolare se non sono state rilevate irregolarità.

8.3. 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 presente capitolo. La firma di un obbligo di riservatezza non è richiesta se questa autorità di vigilanza è vincolata al segreto professionale o legale secondo cui una violazione è punibile ai sensi del codice penale.

9. Obblighi di informazione

9.1. Se i dati del committente sono messi in pericolo da sequestro o confisca, da una procedura di fallimento o di insolvenza o da altri eventi o misure di terze parti, il provider deve informare immediatamente il committente. Il provider informerà immediatamente tutti i titolari in questo contesto che la sovranità e la proprietà dei dati spetta esclusivamente al committente.

10. Durata e cessazione

10.1. 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 su istruzione del 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. Il provider ha il diritto di sospendere l'esecuzione di eventuali istruzioni che potrebbero rappresentare una violazione fino a quando non viene dimostrata la loro legalità. Il rilascio dei dati e il relativo compenso sono regolati nelle CG.

11. Responsabilità

11.1. La responsabilità è disciplinata dalle disposizioni corrispondenti nelle CG.

12. Ulteriori disposizioni

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

12.2. L'Allegato A e l'Allegato B sono parti integranti del presente Accordo sul trattamento dei dati.

Ultima versione: settembre 2023

bexio AG

Alte Jonastrasse 24

8640 Rapperswil

Svizzera

Allegato A Oggetto, natura e scopo

Allegato B Misure tecniche e organizzative (MTO)

1. Allegato A – Oggetto, natura e scopo

Oggetto del contratto:	Il trattamento dei dati personali del committente nel contesto del suo utilizzo dei servizi software del provider.
Natura e scopo dell'elaborazione dei dati prevista:	I dati personali del committente oggetto di trattamento vengono trasferiti al provider nell'ambito dei servizi di software forniti. Il trattamento dei dati da parte del provider avviene esclusivamente in conformità con le CG 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 ● Istoriato dei dati contrattuali
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 CG, nella DPD e nel presente ATD.

2. Allegato B - Misure tecniche e organizzative (MTO)

I. Controllo dell'accesso:

Misure che impediscono alle persone non autorizzate di accedere ai dispositivi di trattamento dei dati con cui vengono elaborati o utilizzati i dati personali:

- Sistema di allarme
- Controllo dell'accesso automatizzato
- Sensori fotoelettronici/ rilevatori di movimento
- Gestione delle chiavi (rilascio delle chiavi, ecc.)
- Schede chip /sistema di chiusura transponder
- Sistema di chiusura manuale (uso limitato alle persone chiave in caso di errori nei sistemi di controllo degli accessi)
- Videosorveglianza nella zona d'ingresso
- Badge obbligatorio da indossare in modo visibile
- Definizione delle aree di sicurezza
- Determinazione delle persone autorizzate ad accedere
- Viene implementato un controllo separato e documentato per l'accesso ai data center e alle sale server solo da parte di personale specificamente autorizzato. L'accesso da parte di personale autorizzato viene registrato con il nome e il numero della carta o del token. Per i data center esistono controlli di accesso separati.

II. Controllo degli accessi:

Misure che impediscono l'uso dei sistemi di trattamento dei dati da parte di persone non autorizzate:

- Assegnazione dei diritti dell'utente
- Assegnazione della password
- Autenticazione con nome utente / password / MFA
- Blocco automatico dell'accesso
- Blocco manuale dell'accesso
- Registrazione degli accessi
- Utilizzo di firewall hardware
- Utilizzo dei profili utente
- Misure aggiuntive: firewall delle applicazioni web, scansioni periodiche di vulnerabilità, test di penetrazione regolari, gestione delle patch, requisiti minimi per la complessità della password e modifica forzata della password, utilizzo di scanner antivirus.

- Assegnazione dei profili utente ai sistemi IT
- Utilizzo della tecnologia VPN
- Crittografia dei supporti di memorizzazione mobili
- Utilizzo di una gestione dei dispositivi mobili (per esempio: blocco e pulizia remoti degli smartphone)
- Crittografia hardware per notebook

III. Controllo degli accessi:

Misure atte a garantire che le persone autorizzate all'utilizzo di un sistema di trattamento dei dati possano accedere esclusivamente nell'ambito della propria autorizzazione di accesso e che i dati personali non possano essere letti, copiati, modificati o rimossi senza autorizzazione durante il trattamento, l'utilizzo e dopo la memorizzazione:

- Introduzione di un concetto di autorizzazione (Identity Access Management)
- Numero di amministratori ridotto al "minimo assoluto"
- Assegnazione minima di autorizzazioni
- Implementazione di restrizioni di accesso
- Pulizia sicura dei dispositivi prima del riutilizzo
- Crittografia hardware (nastri di backup, notebook)
- Gestione dei diritti da parte degli amministratori di sistema
- Linee guida riguardanti le password che implicano requisiti per la lunghezza della password, gestione del cambiamento della password
- Archiviazione sicura di supporti dati

IV. Controllo della divulgazione

Misure atte a garantire che i dati personali non possano essere letti, copiati, modificati o rimossi senza autorizzazione durante la trasmissione elettronica o durante il trasporto o la memorizzazione su supporti dati e che sia possibile verificare e stabilire in quali punti è prevista la trasmissione di dati personali da parte di dispositivi per la trasmissione di dati:

- Creazione di una connessione permanente o di una connessione VPN
- Crittografia (backup per archiviazione off-site)
- Crittografia TLS per tutte le comunicazioni (client Web, API, app mobili)
- 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
- Procedura di cancellazione/ distruzione conforme alle normative di protezione dei dati

V. Controllo dell'input

Misure atte a garantire che sia possibile verificare a posteriori se e da chi sono stati inseriti, modificati o rimossi dati personali nei sistemi di trattamento dei dati:

- Concessione di diritti per l'immissione, la modifica e la cancellazione di dati sulla base di un concetto di autorizzazione
- Documentazione automatica delle autorizzazioni di immissione
- Registrazione delle immissioni

VI. Monitoraggio della disponibilità:

Misure atte a garantire che i dati personali siano protetti da distruzione o perdita accidentale:

- Gruppo di continuità (UPS)
- Dispositivi per il monitoraggio della temperatura e dell'umidità nelle sale server
- Sistemi di allarme antincendio e antifumo
- Allarme in caso di accesso non autorizzato alle sale server
- Creazione di concetti di backup e ripristino
- Creazione di backup di dati
- Test di recupero dati
- Archiviazione sicura off-site di backup di dati
- Condizionatori d'aria nelle sale server
- Estintori nelle sale server
- Piano di emergenza
- Archiviazione di backup
- Verificadegli impianti di emergenza

VII. Obbligo di separazione

Misure atte a garantire che i dati personali raccolti per scopi diversi siano trattati separatamente:

- Creazione di un concetto di autorizzazione
- Diritti di database autorizzati e documentati

- Logical Client Separation/separazione logica dei committenti (a livello di software)
- Separazione di sistemi produttivi e di test
- Economia nella raccolta dei dati