

Datenschutzerklärung

1. Einleitung

1.1. Zweck

Die Datenschutzerklärung hat den Zweck, den Schutz personenbezogener Daten innerhalb der Pius Bienz Treuhand- und Revisions-AG (PBTAG) zu gewährleisten. Es dient der Umsetzung der geltenden Datenschutzgesetze und -vorschriften sowie der Einhaltung der Datenschutzprinzipien. Ziel ist es, das Vertrauen der Kunden, Geschäftspartner und Mitarbeiter in den Umgang mit ihren personenbezogenen Daten zu stärken und den Schutz ihrer Privatsphäre zu gewährleisten. Die Datenschutzerklärung informiert auch über die Rechte der betroffenen Personen. Durch die Implementierung und regelmäßige Überprüfung des Datenschutzes in der Unternehmung streben wir an, Best Practices in allen Bereichen des Treuhandunternehmens zu etablieren und kontinuierlich zu verbessern.

1.2. Verantwortliche Stelle

Verantwortlich für die Datenschutzfragen und Auskünfte ist die

Pius Bienz Treuhand- und Revisions-AG,
Grosshofstrasse 9,
6010 Kriens,

info@bienz-treuhand.ch

+41 41 319 48 50

2. Vorgänge, Bearbeitung von Personendaten

2.1. Grundlegende Interpretation der Personendaten

PBTAG bearbeitet im Rahmen ihrer Geschäftstätigkeit die in der Ziffer 3 aufgeführten Kundendaten grösstenteils nicht als Personendaten im engeren Sinne des DSG. Es ist jedoch in der Natur eines Treuhandunternehmens, dass PBTAG als Auftragsbearbeiter im Rahmen der Mandate auch sensible Personendaten bearbeitet werden. Aus diesem Grund sind in der Folge auch Kundendaten als schützenswerte Daten aufgeführt.

2.2. Bearbeitungsvorgänge von Personendaten

- Offerten für Dienstleistungen
- Bearbeitung der Kundenmandate (Buchhaltung, Lohn, Steuern, Verträge, und weitere)
- Mitarbeiter-Bewerbungen
- Besuch Kundenanlass
- Newsletterversand
- Vertragliche Beziehungen mit Auftragsverarbeitern
- Anforderung von Kundendaten durch gesetzliche Revisionsstellen sowie bei Revisionen durch Sozialversicherungen und kommunale, kantonale und eidgenössische Steuerbehörden

3. Bearbeitete Personendaten

Folgende Personendaten werden bei der Bearbeitung der Kundenkontakte und im Rahmen der Mandate bearbeitet. Diese Daten werden uns grossmehrerheitlich von den Kunden und deren berechtigten Mitarbeitenden zur Verfügung gestellt.

- Kontaktinformationen (z.B. Name, Vorname, Adresse, Telefonnummer, E-Mail)
- Kundeninformationen (z.B. Geburtsdatum, Nationalität, Zivilstand, Beruf, Titel, Stellenbezeichnung, Pass / ID-Nummer, AHV-Nummer)
- Risikomanagementdaten (z.B. Bonitätsinformationen, Handelsregisterdaten)
- Finanzinformationen (z.B. Daten zu Bankverbindungen)

- Mandatsdaten, je nach Auftrag (z.B. Steuerinformationen, Geschäftsdaten (Statuten, Protokolle, Projekte, Verträge), Mitarbeitendendaten (z.B. Lohn, Sozialversicherungen), Buchhaltungsdaten, wirtschaftlich Berechtigte, Eigentumsverhältnisse, Bankverbindungen, usw.
- Bewerbungsdaten (z.B. Lebenslauf, Arbeitszeugnisse, Ausbildungsnachweise)
- Marketinginformationen (z.B. Anmeldung Newsletter, Berücksichtigung Weihnachtsgeschenk)
- Datenerhebung und -verarbeitung

3.1. Zweck der Datenerhebung

Die in Ziffer 3 aufgeführten Daten werden allein für die operative und administrative Bearbeitung im Rahmen der Geschäftstätigkeit erhoben.

3.2. Einwilligung der Datenerhebung

Der Kunde wird bei allen Vorgängen aufgefordert, die Einwilligung zur Bearbeitung der Daten im Rahmen der ordentlichen Bearbeitung zu geben. Ohne das Einverständnis werden die Daten nicht erhoben und nicht bearbeitet.

3.3. Datenerfassungsmethoden

Die Erfassung erfolgt i.d.R. durch Zur Verfügungstellung durch die betroffenen Personen und Unternehmen, oder wird in Zusammenarbeit mit diesen erstellt

Falls Daten benötigt werden, die nicht direkt durch den Kunden zur Verfügung gestellt werden, so wird der Kunde diese Stellen informieren, dass PBTAG sie Zwecks der Erhebung zur Erfüllung des Mandats benötigte Daten kontaktieren wird. Damit erklärt sich der Kunde auch einverstanden, dass Daten aus diesen Quellen erhoben und bearbeitet werden.

3.4. Bearbeitungen von Bewerbungen

Bewerbungsinformationen betrachten wir als schützenswerte Personendaten im engeren Sinne des DSGVO.

Bewerbungsinformationen erhalten wir i.d.R. vom Bewerber direkt oder von ihm beauftragten Personaldienstleistern. Die Daten werden nur von den mit der Selektion beauftragten internen und externen involvierten Personen bearbeitet. Im Rahmen des Selektionsprozesses werden diese durch die bearbeitenden Personen ergänzt.

Nach dem Abschluss der Selektion werden die Daten von den nicht berücksichtigten Bewerbern spätestens nach 6 Monaten gelöscht. Zur Verfügung gestellte Dossiers werden den Bewerbenden zurückgeschickt, erstellte Kopien sicher entsorgt.

3.5. Webanalyse

PBTAG betreibt eine eigene Webseite. Auf der Webseite werden keine Benutzungsdaten mittels Cookies gesammelt.

Allfällige Nutzungsdaten, die das Webseiten-Hosting erfasst, werden von PBTAG nicht ausgewertet.

4. Datenweitergabe und -übermittlung

4.1. Dritte Empfänger von personenbezogenen Daten

Personendaten werden ohne das Einverständnis der betroffenen Personen nur an die gesetzlich vorgeschriebene Sozial- und Gesundheitsinstitutionen weitergegeben.

An weitere Dritte (z.B. Personalberater, Rechtsanwalt, ...) werden Personen- und Kundendaten nur nach Vorlage des Einverständnisses der betroffenen Personen weitergegeben. Dazu muss ein expliziter Auftrag mit der Benennung der weiterzugebenden Daten und des Empfängers vorliegen.

4.2. Internationale Datenübermittlung

Eine internationale Übermittlung von Personendaten findet nur auf Auftrag der betroffenen Person (z.B. Bewerbung aus EU-Raum) statt.

Gleichermassen werden schützenswerte Kundendaten nur auf Auftrag des Kunden international übermittelt.

4.3. Vereinbarungen und Maßnahmen zum Datenschutz bei Datenweitergabe

Schützenswerte Daten werden gesichert übertragen. Der Kommunikationskanal und ob die Daten verschlüsselt werden müssen, muss mit dem Kunden abgesprochen und bewilligt werden. Falls die Daten verschlüsselt werden müssen, muss der Kunde die Verschlüsselungstechnik vorgeben und die notwendige Infrastruktur bereitstellen. Auf den Speichersystemen von PBTAG sind die Daten unverschlüsselt gespeichert und gesichert.

5. Rechte der betroffenen Personen

Die in der Folge aufgeführten Rechte stehen den betroffenen Personen zu. Dies gilt im gleichen Mass auch für die bearbeiteten Kundendaten.

1. **Auskunftsrecht:** Die betroffene Person hat das Recht, von der verantwortlichen Stelle Auskunft darüber zu erhalten, ob und welche personenbezogenen Daten über sie verarbeitet werden.
2. **Recht auf Berichtigung:** Falls personenbezogene Daten unrichtig oder unvollständig sind, hat die betroffene Person das Recht, eine Berichtigung oder Ergänzung dieser Daten zu verlangen.
3. **Recht auf Löschung ("Recht auf Vergessenwerden"):** Unter bestimmten Umständen hat die betroffene Person das Recht, die Löschung ihrer personenbezogenen Daten zu verlangen, beispielsweise wenn die Daten für den ursprünglichen Zweck nicht mehr erforderlich sind oder die Verarbeitung unrechtmässig ist.
4. **Recht auf Einschränkung der Verarbeitung:** Die betroffene Person kann unter bestimmten Voraussetzungen verlangen, dass die Verarbeitung ihrer personenbezogenen Daten eingeschränkt wird, z.B. wenn die Richtigkeit der Daten bestritten wird oder die Verarbeitung unrechtmässig ist.
5. **Recht auf Datenübertragbarkeit:** Sofern technisch möglich, hat die betroffene Person das Recht, ihre personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und diese Daten einem anderen Verantwortlichen ohne Behinderung zu übermitteln.
6. **Widerspruchsrecht:** Die betroffene Person kann in bestimmten Situationen der Verarbeitung ihrer personenbezogenen Daten widersprechen, insbesondere wenn die Verarbeitung aufgrund eines nicht berechtigten Interesses erfolgt.
7. **Recht auf Beschwerde bei der Aufsichtsbehörde:** Die betroffene Person hat das Recht, bei der zuständigen Datenschutzbehörde eine Beschwerde einzureichen, wenn sie der Ansicht ist, dass ihre Rechte verletzt wurden.

Für die Wahrnehmung der Rechte der betroffenen Personen wenden sie sich diese an die für den Datenschutz bezeichnete Stelle gemäss Ziffer 1.2.

6. Datensicherheit und Datenintegrität

Das Unternehmen unternimmt die branchenüblichen Massnahmen und die bearbeiteten Personen- und Kundendaten zu schützen. In der Folge ist eine Übersicht der wichtigsten Massnahmen aufgeführt.

- **Zugriffskontrollen und Authentifizierung**
Der Zugriff auf die Systeme und Infrastrukturen der Unternehmung ist erst nach einer zumindest 2 phasigen Identifikation-Überprüfung möglich. Dies gilt für den Zugriff auf die Netzwerkinfrastruktur und Applikationen.
Der Zutritt zum Firmengebäude ist nur mittels Schlüssel möglich, oder durch Einlass durch das Sekretariat.
Der Zugriff vom Home-Arbeitsplatz erfolgt ausschliesslich über firmeneigene Geräte und mittels VPN-geschützter Kommunikation. Für den Aufbau der Kommunikation ist ein Multifaktor-Authentifizierung notwendig.
- **Verschlüsselung und Anonymisierung**

Die verwalteten und bearbeiteten Daten werden nicht anonymisiert und verschlüsselt. Falls schützenswerte Daten weitergegeben werden, erfolgt dies immer auf einem geschützten Kommunikationskanal.

- **Protokollierung von Zugriffen und Datenverarbeitungsvorgängen**
Die Remote-Zugriffe werden durch Netzwerk-Aktiv-Komponenten protokolliert. Der Zugriff auf die Firmendaten und Applikationen wird mit 2 Ausnahmen (E-Mails, Revisionsdaten) nicht protokolliert.
- **Datenlöschung / -Archivierung**
Die verwalteten Personen- und Geschäftsdaten des Unternehmens werden gemäss den gesetzlichen Vorgaben aufbewahrt und nach Ablauf der Aufbewahrungsfrist vernichtet.
Kundendaten werden nach Beendigung des Mandats dem Kunden übergeben und nach Ablauf der gesetzlich vorgeschriebenen Datenaufbewahrungsfristen von den internen Speichermedien (Server, Ablage) gelöscht.
Die Daten datenspeichernde Geräte werden bei der Ausserbetriebnahme gezielt gelöscht. Wo dies nicht möglich ist, wird der Datenträger unbrauchbar gemacht.
- **Datensicherheitsrichtlinien und -verfahren**
Auf der technischen Ebene werden folgende Sicherheitsmassnahmen, unterstützt durch beauftragte Partner, unternommen:
 - Tägliche Datensicherung mittels Generationen-Konzept, inhouse/extern Kopien
 - Redundante Netzwerk-Firewall
 - VPN-geschützte Kommunikation mit Auftragsbearbeiter
 - Malware-Protection der Arbeitsgeräte
 - Redundante Server, Datenspiegelung

Auf der organisatorischen Ebene gelten die interne Datenschutzrichtlinie und die Richtlinie ICT-Nutzung für die Mitarbeitenden.

7. Auftragsverarbeitung

7.1. Einsatz von Auftragsverarbeitern

PBTAG arbeitet geschäftlich seit Jahren mit einem Set von Partnern zusammen. Diese arbeiten im Sinne eines Auftragsbearbeiters in folgenden Bereichen mit der Unternehmung zusammen.

- Personalberater
- Rechtsanwalt
- Applikationsberater / -lieferant
- IT-Infrastrukturbetreiber

In der Beilage 'Verzeichnis der Bearbeitungstätigkeiten' sind weitere Angaben zur Zusammenarbeit mit den Auftragsbearbeitern ersichtlich.

7.2. Vertragliche Vereinbarungen und Datenschutz bei Auftragsverarbeitung

Grundlage für die Zusammenarbeit ist ein schriftlicher Auftrag in diesem sind i.d.R. folgende Punkte geregelt.

- Auftragsgegenstand
- Liefergegenstand
- Rechte / Pflichten
- Kommerzielle Regelung
- Vertraulichkeit / Datenschutz / Sicherheit
- Zusammenarbeit (Ansprechpersonen, Datenaustausch)

8. Datenschutz-Schulungen und Sensibilisierung

Folgende Themen werden periodisch intern geschult:

- Grundlagen zu IT-Sicherheit und Datenschutzes
- Anwendung der Datenschutzrichtlinie
- Anwendung der Richtlinie der ICT-Nutzung

9. Änderung Datenschutzerklärung

Wir behalten uns die jederzeitige Änderung dieser Datenschutzerklärung ausdrücklich vor.

Kriens, August 2023