ÖFFENTLICH

Datenschutz-Richtlinie der abfallboerse schweiz.ch AG

Version 1.0, im August 2023

abfallboerse schweiz.ch AG • Bachstrasse 3 • Postfach 90 • CH-6362 Stansstad
Tel. +41 41 632 48 48 • info@abfallboerse.ch • www.abfallboerse.ch

Inhaltsverzeichnis

Präambel
Die abfallboerse schweiz.ch AG (abfallboerse) versucht generell, so wenige Personendaten über natürliche Personen wie möglich zu erheben, da sie im B2B-Segment tätig ist und daher weniger die Personendaten sondern vielmehr die zur Ausübung ihrer Tätigkeiten nötigen Informationen verarbeitet (Firmenstruktur, Funktionen, standortspezifische Verhältnisse an den Entsorgungsstandorten etc.). Ferner bearbeitet sie nicht besonders schützenswerte Personendaten oder führt auch kein Profiling mit hohem Risiko durch gemäss der Datenschutzverordnung (DSV).

Nichtsdestotrotz ist ihr die vertrauliche Verarbeitung allfälliger Personendaten, neben den sonst verarbeiteten Daten, sehr wichtig. Sie hat daher bereits seit mehreren Jahren eine Informationssicherheitspolitik erstellt, an welche sich ausnahmslos alle Mitarbeitenden der abfallboerse halten müssen. Ferner wird die Datenschutzrichtlinie der abfallboerse wie folgt festgehalten und umschrieben.

Ziele
Gemäss Art. 2 DSV wird darauf abgezielt, insbesondere die folgenden Elemente zu schützen: Vertraulichkeit, Verfügbarkeit, Integrität, Nachvollziehbarkeit und dies fortlaufend. Im Detail bedeutet dies:

- Nur Berechtigte haben Zugang (**Vertraulichkeit**)
- Daten sind verfügbar, wenn sie benötigt werden (**Verfügbarkeit**)
- Keine unberechtigte oder unbeabsichtigte Veränderung der Daten (**Integrität**)
- Bearbeitung/Anpassung der Daten ist nachvollziehbar (**Nachvollziehbarkeit**)
- Fortlaufender Schutz der Daten soll gewährleistet werden

Generelle Richtlinien innerhalb der abfallboerse
- Die abfallboerse schweiz.ch AG erhebt/bearbeitet/speichert oder verarbeitet in sonstiger Weise KEINE besonders schützenswerten Personendaten
- Allfällige Personendaten werden von den betroffenen Personen selbst an die abfallboerse eingereicht. Dabei werden die betroffenen Personen über den Zweck der Datenerhebung informiert (z.B. Newsletter-Anmeldung abfallboerse.ch)
- Bearbeitung der Daten wird nur durch Mitarbeitende und Organe der abfallboerse schweiz.ch AG vollzogen
- Die abfallboerse schweiz.ch AG gibt keine allfälligen Personendaten ins Ausland preis. Der Nutzungsspeicherort der digitalen Daten ist jeweils die Schweiz
- Die abfallboerse schweiz.ch AG gibt betroffenen Personen bei Bedarf Auskunft über die Beschaffung der Personendaten. Dies gem. Art. 18 DSV innerhalb der vorgeschriebenen Frist
- Die Daten werden nach Beendigung der Datenbearbeitung mindestens zwei Jahre (digital) aufbewahrt
- Meldungen von Verletzungen der Datensicherheit werden an den EDÖB gemäss geforderten Angaben in Art. 15 DSV getätigt sowie dokumentiert
- Es wird keine automatisierte Bearbeitung oder Profiling mit hohem Risiko von besonders schützenswerten Personendaten angestellt, wodurch die Protokollierung gem. Art. 4 DSV nicht nötig ist

Konkrete technische und organisatorische Massnahmen zur Zielerreichung
Um die aufgeführten Ziele zu erreichen, hat die abfallboerse einige Massnahmen ergriffen. Diese sind technischer sowie organisatorischer Art.

*Massnahmen, um die **Vertraulichkeit** zu gewährleisten:*

- Berechtigte Personen haben lediglich auf jene Personendaten Zugriff, die sie zur Erfüllung ihrer Aufgaben benötigen (Zugriffskontrolle, need-to-know-Prinzip mit Rollenverteilung innerhalb der Unternehmung)
- Berechtigte Personen haben nur zu den Räumlichkeiten und Anlagen Zugriff, zu welchen sie diesen benötigen, um ihre Aufgabe zu absolvieren (Zugangskontrolle mittels individualisierten Badges, Alarmanlage, 2FA für Userauthentisierung)
- Unbefugte Personen sollen Einrichtungen zur Datenübertragung nicht benutzen können (Benutzerkontrolle mittels sicheren Passwörtern, 2FA, Rollenverteilung, Onboarding von externen Usern auf Ökosystem der Unternehmung)

*Massnahmen, um die **Verfügbarkeit** und **Integrität** zu gewährleisten:*

- Unbefugte Personen können Datenträger nicht lesen, kopieren, verändern, verschieben, löschen oder vernichten (Datenträgerkontrolle (Cloud-Speicher) mittels 2FA, individualisierte Benutzer sowie Rollenverteilung)
- Unbefugte Personen können Daten im Speicher nicht speichern, lesen, ändern, löschen oder vernichten (Speicherkontrolle mittels 2FA, individualisierte Benutzer sowie Rollenverteilung im Ökosystem der Unternehmung)
- Unbefugte Personen können bei Bekanntgabe von Personendaten oder beim Transport von Datenträgern Personendaten nicht lesen, kopieren, verändern, löschen oder vernichten (Transportkontrolle sowie Sensibilisierung mittels Schulung der MA, One-Pager für Massnahmenerhebung im Notfall)
- Verfügbarkeit der Personendaten und Zugang dazu bei physischem oder technischem Zwischenfall rasch wiederherstellen (Wiederherstellung mittels (physisch an unterschiedlichen Orten, ca. 15km getrennt, liegenden) offline-Backups, online-Backups (OneDrive, 30 Tage Versionierung))
- Fehlfunktionen sollen gemeldet werden können (Zuverlässigkeit sowie Dienstleistungsservice über MS365 Info-Mails an IT-Admin der Unternehmung)
- Gespeicherte Personendaten sollen nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität durch manuelle Anpassungen von Seiten der Benutzer:innen, ansonsten nicht möglich beim Original der Daten (Dritte haben lediglich Lese-, nicht aber Bearbeitungsberechtigungen))
- Betriebssysteme und Anwendungssoftware soll stets auf dem neusten Sicherheitsstand gehalten und bekannte kritische Lücken geschlossen werden (Systemsicherheit durch automatisierte Updates der Tools und Geräte sowie bestehender und beobachtete Informationskanäle (z.B. Youtube-Channels, Newsletter, MS365 Info-Mails) durch IT-Verantwortliche Person)

*Massnahmen, um die **Nachvollziehbarkeit** zu gewährleisten:*

- Es soll überprüft werden können, welche Personendaten zu welcher Zeit und von welcher Person im automatisierten Datenbearbeitungssystem eingegeben oder verändert werden (Eingabekontrolle mittels individualisierten Usern und MS365, kein automatisiertes Datenbearbeitungssystem im Einsatz)
- Es soll überprüft werden können, wem Personendaten mit Hilfe von Einrichtungen zur Datenübertragung bekanntgegeben werden (Bekanntgabekontrolle über MS365 Kontrolle, wer an wen Mails gesendet hat → Nachrichtenablaufverfolgung über Exchange Admin Center)
- Verletzungen der Datensicherheit sollen rasch erkannt (Erkennung) und Massnahmen zur Minderung oder Beseitigung der Folgen ergriffen werden können (Beseitigung) → Microsoft 365 Defender

Inkrafttreten und Änderungen
Diese Datenschutzrichtlinie tritt ab sofort in Kraft. Überprüfungen dieser Richtlinie finden in regelmässigen Abständen sowie bei umfassenden Anpassungen der DSV statt. Änderungen werden durch den Sicherheitsbeauftragten initialisiert, von der Geschäftsleitung abgesegnet und unterzeichnet sowie den Mitarbeitenden sachgerecht kommuniziert.

Stansstad, im August 2023

Mario Wermelinger
Geschäftsführer