EU-Datengesetz („Data Act“): Online-Register und Informationen zu internationalen Datentransfers

Verpflichtende Informationen nach Art 26 und 28 Data Act (Verordnung (EU) 2023/2854) des Europäischen Parlaments und des Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung – Data Act)

Gültig ab: 12.09.2025

Wechsel zwischen Anbietern von Datenverarbeitungsdiensten

Nach dem EU-Datengesetz („Data Act“) haben Sie als Kund*in der nachfolgend aufgelisteten Produkte das Recht Ihre exportierbaren Daten und digitalen Vermögenswerte

- auf einen anderen Dienstanbieter zu übertragen („Wechsel“);
- auf die IKT-Infrastruktur in Ihren eigenen Räumlichkeiten zu übertragen („Wechsel“); oder
- sofern Sie keinen Wechsel wünschen, Ihre Daten nach Beendigung des Dienstes zu löschen.

Sie können angeben, nur in Bezug auf bestimmte Datenverarbeitungsdienste, Daten oder digitale Vermögenswerte zu wechseln.

Im Falle eines Wechsels werden die exportierbaren Daten und digitalen Vermögenswerte nach erfolgreichem Wechsel und Ablauf der vereinbarten Mindestfrist für den Datenabruf gelöscht. Sobald der Wechsel erfolgreich vollzogen ist, ist der Vertrag automatisch beendet.

Im Falle der Löschung ist der Vertrag automatisch beendet, sobald die in den SCCs vereinbarte Kündigungsfrist abgelaufen ist.

Details können Sie den **Standardvertragsklauseln für Datenverarbeitungsdienste zum Data Act („SCCs“)**, abrufbar unter post.at/i/c/agb-tochterunternehmen entnehmen.

Verfügbare Verfahren für Wechsel und Übertragung der Daten

Im Folgenden finden Sie aufgelistet pro Produkt unsere verfügbare Wechsel- und Übertragungsmethoden und -formate.

Des Weiteren werden Ihnen pro Produkt alle übertragbaren Datenkategorien aufgelistet.

Es gibt keine Datenkategorien, die für die internen Funktionsweise des Datenverarbeitungsdienstes spezifisch sind und aufgrund einer Verletzungsgefahr von Geschäftsgeheimnissen von den übertragbaren Datenkategorien ausgenommen wurden. Weiters sind uns keine technischen Beschränkungen oder Einschränkungen bekannt.

Produktname	Übertragbare Datenkategorien	Datenformat	Wechsel- bzw Übertragungsmethode
Bestellerfassung	Scan der Bestellungen	PDF	sFTP - verschlüsselter Filetransfer
Digitaler Posteingang	Scan der Eingangspost	PDF	sFTP - verschlüsselter Filetransfer
Dokumenten- und Archivdigitalisierung	Scan von Archivdokumenten	PDF	sFTP - verschlüsselter Filetransfer
Duale Zustellung	Adressdaten, Personenstammdaten, behördliche elektronische Sendungen	CSV CSV PDF	sFTP - verschlüsselter Filetransfer
E-Brief	Adressdaten, Personenstammdaten, Sendungsdaten	CSV CSV PDF	sFTP - verschlüsselter Filetransfer
e-Gehaltszettel	Adressdaten, Personenstammdaten, Gehaltsnachweise	CSV CSV PDF/XML/SAP IDOC	sFTP - verschlüsselter Filetransfer
EinfachBrief	Druckdaten	PDF	sFTP - verschlüsselter Filetransfer
Formularerfassung	Scan von Formularen	PDF	sFTP - verschlüsselter Filetransfer
Historische Archive	Scan von Archivdokumenten	PDF	sFTP - verschlüsselter Filetransfer
HybridSign	Signierte Dokumente	PDF	sFTP - verschlüsselter Filetransfer
Individualdruck	Druckdaten	PDF	sFTP - verschlüsselter Filetransfer
Klickbrief	Druckdaten	PDF	sFTP - verschlüsselter Filetransfer
Mikrofilmdigitalisierung	Scan von Microfilmen	PDF	sFTP - verschlüsselter Filetransfer
Rechnungserfassung	Scan der Eingangsrechnungen	PDF	sFTP - verschlüsselter Filetransfer
Transaktionsdruck	Druckdaten	PDF/AFP/XML	sFTP - verschlüsselter Filetransfer

Informationen zu internationalen Datentransfers

Gerichtsbarkeit unserer IKT-Infrastruktur

Die von uns für die Datenverarbeitung im Rahmen unserer Produkte genutzte IKT-Infrastruktur unterliegt der Gerichtsbarkeit der Europäischen Union.

Maßnahmen zur Verhinderung, dass Behörden in Ländern außerhalb der EU unrechtmäßig auf Daten zugreifen oder diese erhalten

Wir haben technische, organisatorische und vertragliche Maßnahmen getroffen, damit Behörden aus Ländern außerhalb der Europäischen Union nicht auf Ihre Daten zugreifen oder sie erhalten können, wenn das gegen EU-Recht oder österreichisches Recht verstößt.

1. Anfragenprüfung

Wenn Behörden aus Ländern außerhalb der EU verlangen, dass wir ihnen Ihre Daten übermitteln oder ihnen Zugang dazu gewähren, prüfen wir diese Anfragen sehr genau. Dabei halten wir uns an die Vorgaben des Data Act, der Datenschutz-Grundverordnung (DSGVO) und des österreichischen Datenschutzgesetzes (DSG). Wir geben Ihre Daten nur weiter oder erlauben den Zugriff, wenn diese Gesetze das erlauben.

Wenn die gesetzlichen Bedingungen erfüllt sind, um Daten an eine ausländische Behörde zu übermitteln oder Zugriff zu erlauben, geben wir nur so viele Daten weiter, wie gesetzlich erlaubt ist. Zusätzlich informieren wir Sie nach den gesetzlichen Bestimmungen vorher darüber.

2. Vertraulichkeit

Daten werden lediglich von autorisierten Benutzer*innen gelesen bzw. modifiziert. Dies gilt sowohl beim Zugriff auf gespeicherte Daten wie auch während der Datenübertragung.

2.1. Zutrittskontrolle

Es sind Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren, implementiert. Als Maßnahmen zur Gebäude- und Raumsicherung werden unter anderem automatische Zutrittskontrollsysteme, Chipkarten, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen werden in verschließbaren Serverschränken und Räumlichkeiten geschützt. Darüber hinaus werden organisatorische Maßnahmen, wie z. B. Dienstanweisungen und Verhaltensregeln gesetzt.

2.2. Zugangskontrolle

Es sind Maßnahmen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können, implementiert, z. B. Einsatz von Bootpasswörtern, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwortschutz. Darüber hinaus existieren organisatorische Maßnahmen, um beispielsweise eine unbefugte Einsichtnahme zu verhindern. Das können z. B. Benutzerverwaltungssysteme und gültige Richtlinien nach Stand der Technik zu Themen wie „Sicheres Passwort“, „VPN Tunnel“, „IP-Restrictions“, „Automatische Sperren“, „Löschen und Vernichten“, „Mobile Device“ etc. sein.

2.3. Zugriffskontrolle

Es sind Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, implementiert. Die Zugriffskontrolle wird durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen, sichergestellt. Des Weiteren sind geeignete Kontrollmechanismen und Verantwortlichkeiten definiert, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z. B. bei Einstellung, Wechsel des

Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit wird zudem auf die Rolle und Möglichkeiten der Administratoren gerichtet.

2.4. Trennungskontrolle

Es sind Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können, implementiert. Dies wird beispielsweise durch logische und physische Trennung der Daten gewährleistet.

2.5. Pseudonymisierung

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen, ist sichergestellt.

3. Integrität

Daten können nicht unbemerkt verändert werden. Alle Änderungen sind nachvollziehbar.

3.1. Weitergabekontrolle

Es existieren Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z. B. Verschlüsselungstechniken und Virtual Private Networks eingesetzt werden.

3.2. Eingabekontrolle

Es sind Maßnahmen implementiert, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Die Eingabekontrolle wird durch Protokollierungs-Maßnahmen erreicht, die auf verschiedenen Ebenen (z. B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) eingesetzt werden. Das Berechtigungskonzept beschreibt, welche Daten protokolliert werden, wer Zugriff auf die Protokolle hat, durch wen und bei welchem Anlass / Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

Kontaktdaten

Post Business Solutions GmbH

Customer Service Management

Halban-Kurz-Straße 11

1230 Wien

E-Mail: bs.kundenservice@post.at