



Die einschlägigen gesetzlichen Vorschriften verlangen eine Verarbeitung personenbezogener Daten in der Form, dass die Rechte der durch die Verarbeitung betroffenen Personen auf Vertraulichkeit und Integrität ihrer Daten geschützt werden. Daher sind personenbezogene Daten nur in dem Umfang und in der Weise zu übermitteln, wie es zur Erfüllung der übertragenen Aufgaben erforderlich ist.

Im Folgenden wird erläutert, welche Anforderungen zu beachten sind:

- Sichere Datenübertragung
- Datensparsamkeit
- Technische Voraussetzungen

### Sichere Datenübertragung

---

Der sicherste Weg der Datenübertragung für den Abgleich Ihrer Kunden- oder Interessentenadressen ist der sFTP-Transfer über die Online-Services von Deutsche Post Direkt ([www.postdirekt.de/online-services](http://www.postdirekt.de/online-services)). Dazu erhalten Sie einen benutzerbezogenen Zugang und bestimmen Ihr Passwort individuell. Die Rückübertragung der Daten erfolgt ausschließlich über diesen Weg. Als zusätzliche Sicherheitsmaßnahme ist eine passwortgeschützte oder PGP-verschlüsselte Übertragung Ihrer Daten möglich.

Per E-Mail übermittelte Daten werden umgehend von Deutsche Post Direkt gelöscht. Bitte nutzen Sie ausschließlich den sicheren Übertragungsweg der Online Services. Sollten Sie den Weg der Mailübertragung wählen, so tragen Sie das Risiko des Datenverlusts während der Übertragung.

### Datensparsamkeit

---

Die Deutsche Post Direkt benötigt zur Durchführung ihrer Dienstleistung von Ihnen die folgenden Daten:

- Eindeutige ID (z. B. Kundennummer)
- Vorname
- Name
- Straße
- Hausnummer
- Postleitzahl
- Ort
- Ortsteil (zur Auflösung mehrdeutiger Straßen, falls vorhanden)

Bitte beachten Sie, dass darüber hinaus keine weiteren Daten von Deutsche Post Direkt benötigt werden. Sollten für Analyseleistungen weitere Informationen notwendig sein, so sind diese auf das absolut erforderliche Maß zu reduzieren und dürfen insbesondere



keine besonderen Kategorien personenbezogener Daten oder besonders schutzwürdige Daten enthalten.

Besondere Kategorien personenbezogener Daten sind Daten wie z. B. Gesundheitsdaten. Besonders schutzwürdige Daten sind Daten wie z. B. Bankverbindungsdaten, deren Übermittlung und Verarbeitung ein Risiko für die Rechte der Betroffenen, für den Kunden als Auftraggeber sowie für Deutsche Post Direkt als Auftragnehmer darstellen.

Sollte Deutsche Post Direkt daher feststellen, dass zusätzliche, über den für den Auftrag erforderlichen Umfang hinaus gehende Daten übermittelt wurden, werden die gesamten übermittelten Daten umgehend vollständig gelöscht, da ein Heraus-selektieren der nicht benötigten Daten durch Deutsche Post Direkt nicht erfolgen kann.

#### Technische Voraussetzungen

---

Dies sind die wichtigsten technischen Informationen für den Abgleich Ihrer Kunden- oder Interessentenadressen:

- Dateiformat: Textdatei (fix oder variabel – csv, txt)
- Zeichensätze: ISO-8859-1, ISO-8859-15, US-ASCII, WINDOWS-1252, UTF-8, IBM850
- Bitte teilen Sie bei Übertragung der Daten auch die Anzahl der Datensätze je übertragener Datei mit



#### **Datenschutzaufsichtsbehörden**

Als einer der führenden deutschen Adressdienstleister steht Deutsche Post Direkt in engem Kontakt zu den Vertretern der Datenschutzaufsichtsbehörden und unterliegt im Rahmen der Verarbeitung personenbezogener Daten der Meldepflicht gegenüber der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen. Die Deutsche Post Direkt ist auch Teilnehmer der Ad-hoc-Arbeitsgruppe „Werbung und Adresshandel“ der Aufsichtsbehörden für den Datenschutz der Länder und des Bundes unter Leitung des Bayerischen Landesamts für Datenschutzaufsicht. Zudem fällt die Deutsche Post in den direkten Geltungsbereich der Bundesdatenschutzbeauftragten. Mit ihr wird ein regelmäßiger Dialog geführt, in den auch der betriebliche Datenschutzbeauftragte von Deutsche Post Direkt prüfend und beratend einbezogen ist.

#### **Verpflichtung der Mitarbeiter auf die Vertraulichkeit**

Die Mitarbeiter von Deutsche Post Direkt haben sich schriftlich zur Einhaltung des Datengeheimnisses nach Art. 24 DSGVO verpflichtet und sind über ggf. auf Kunden-seite bestehende weitergehende Geheimhaltungspflichten wie z. B. Bank- oder Sozialgeheimnis informiert. Organisatorische und sicherheitstechnische Maßnahmen gewährleisten, dass nur befugte Mitarbeiter Zugang zu den Daten haben.

#### **Zertifizierung des Bundesamts für Sicherheit in der Informationstechnik**

Deutsche Post Direkt ist nach ISO 27001 auf der Basis von IT-Grundschutz zertifiziert. Das Zertifikat des Bundesamts für Sicherheit in der Informationstechnik umfasst die produktionsbezogenen Geschäftsprozesse und die dafür erforderlichen IT-Systeme der Produktfamilie ADDRESSFACTORY, das Portal und die damit verbundene Datenaustauschplattform. Mit der Zertifizierung dokumentiert Deutsche Post Direkt die Durchführung besonderer technischer und organisatorischer Sicherheitsmaßnahmen. Diese schreibt Art. 32 DSGVO für die Verarbeitung personenbezogener Daten im Kundenauftrag vor. Die Auszeichnung des BSI entlastet Kunden von ihrer datenschutzrechtlichen Kontrollverpflichtung gegenüber Deutsche Post Direkt als Auftragnehmer.