Information on ensuring data protection and data security when transferring personal data

The applicable statutory provisions require that personal data be processed in such a manner that the data subjects' rights to the confidentiality and integrity of their data are protected. Therefore, personal data may only be transferred to the extent and in the manner required to perform the assigned tasks.

The requirements to be complied with are presented below:

- Secure data transfer
- Data economy
- Technical requirements

Secure data transfer

The most secure way to transfer data for purposes of matching the addresses of your customers or potential customers is the sFTP Transfer via the online services of Deutsche Post Direkt (www.postdirekt.de/online-services). You will receive user-specific access and can set your own individual password. Data will always be transferred back to you by the same means. As an additional security measure, you can opt to transfer your data using password protection or PGP encryption.

Data transferred via e-mail will be deleted immediately by Deutsche Post Direkt. Please be sure to use only the online services secure transmission channel. If you elect to transfer data via e-mail, you bear the risk that your data will be lost during transfer.

Data economy

In order to provide its services, Deutsche Post Direkt requires the following data from you:

- Unique ID (e.g., customer number)
- First name
- Surname
- Street name
- Street number
- Postal code
- City
- District (to clarify any ambiguous streets)

Please note that Deutsche Post Direkt requires no other data beyond this. Should further information be required for analysis services, this must be kept to the absolute minimum necessary and may not, in particular contain any special categories of data or data meriting specific protection.

Special categories of data include data such as health data. Data meriting specific protection include, for example, bank account details, the transfer and processing of which represent a risk to the rights of the data subjects, the Customer and Deutsche Post Direkt as Contractor.

Therefore, should Deutsche Post Direkt determine that additional data beyond that which is required for the commission were transferred, all the transferred data will be deleted completely, as Deutsche Post Direkt is not able to extract the unnecessary data.

Technical requirements

The most important technical information for matching your customer or potential customer addresses is as follows:

- File format: text file (fixed or variable – csv, txt)
- Character sets: ISO-8859-1, ISO-8859-15, US-ASCII, WINDOWS-1252, UTF-8, IBM850
- Please also indicate the number of data sets per transferred file when transferring the data.

Data protection authorities

Deutsche Post Direkt is one of the leading German address service providers and, as such, maintains close contact with representatives of the data protection authorities. As a company that processes personal data, it is required to notify the North Rhine-Westphalia Commissioner for Data Protection and Freedom of Information when it processes personal data. Deutsche Post Direkt is also a member of the ad hoc working group "Advertising and address trading" of the German state and federal data protection authorities headed by the Bavarian Data Protection Authority (*Bayerisches Landesamts für Datenschutzaufsicht* – BayLDA). Moreover, Deutsche Post falls under the direct jurisdiction of the Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragte für den Datenschutz und die Informationsfreiheit* – BfDI) with whom it has a regular dialogue. Deutsche Post Direkt's own data protection officer is frequently included in this dialogue for monitoring and consultation purposes.

Commitment to confidentiality

The employees of Deutsche Post Direkt have undertaken in writing to comply with the obligation to maintain confidentiality pursuant to Article 24 GDPR and have informed themselves about any other existing obligations that customers may have regarding confidentiality such as banking secrecy or the protection of social data. Organisational and security measures ensure that only authorised employees have access to the data.

Certification by TÜV AUSTRIA GmbH

Deutsche Post Direkt is certified in accordance with ISO/IEC 27001. The certificate is issued by TÜV AUSTRIA GmbH as the certification body and covers data management and dialog marketing order processing and the required IT systems, including the network and communication links, of the DATAFACTORY and ADDRESSFACTORY product family, the portal and the associated data exchange platform. Within the information network, personal data is stored and processed in a data hub for the purposes of address, master and reference data management as well as dialog marketing. The certification shows that Deutsche Post Direkt implements special technical and organizational security measures as prescribed by Article 28 (1), Article 28 (3) c), and Article 32 (1) of the GDPR.

The TÜV certification releases customers from the obligation to monitor Deutsche Post Direkt (the contractor) as otherwise required by data protection law.