DAS VERBINDET UNS.

Technische und organisatorische Maßnahmen des Datenschutzes

ANHANG ZUR VEREINBARUNG ÜBER DIE VERARBEITUNG PERSONENBEZOGENER DATEN IM AUFTRAG.

T-MOBILE AUSTRIA GMBH („AUFTRAGSVERARBEITERIN“)

1. Kompetenzklarheitsprinzip

Die Aufgabenverteilung bei der Datenverwendung zwischen der Auftragsverarbeiterin und zwischen den Mitarbeitern soll ausdrücklich festgelegt werden. Als Beispiele sind Stellenbeschreibungen oder auch Aufgabenbeschreibungen in Arbeits-oder Dienstverträgen zu nennen.

2. Auftragsprinzip

Mitarbeiter dürfen Daten nur auf Grund einer ausdrücklichen Anordnung ihres Arbeitgebers (Dienstgebers) übermitteln. Verantwortlicher und Auftragsverarbeiterin haben, sofern eine solche Verpflichtung ihrer Mitarbeiter nicht schon kraft Gesetzes besteht, diese vertraglich zu verpflichten, dass sie Daten aus Datenanwendungen nur auf Grund von Anordnungen übermitteln und das Datengeheimnis auch nach Beendigung des Dienstverhältnisses zum Verantwortlichen oder Auftragsverarbeiterin einhalten werden.

3. Belehrungspflichtprinzip

Jeder Mitarbeiter ist über seine Pflichten nach dem Datenschutzgesetz und dem Telekommunikationsgesetz und nach inner-organisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften zu belehren. Diese Belehrung sollte nach Möglichkeit in regelmäßigen Abständen (z.B. einmal im Jahr) erfolgen.

4. Zutrittsbeschränkungsprinzip

Mit dem Begriff „Zutritt“ ist der physische Zugang von Personen zu Gebäuden und Räumlichkeiten gemeint, in denen IT- Systeme betrieben und genutzt werden. Dies können z.B. Rechenzentren sein, in denen Web-Server, Applikationsserver, Datenbanken, Mainframes, Speichersysteme betrieben werden und Arbeitsräume, in denen Mitarbeiter Arbeitsplatzrechner nutzen. Auch die Räumlichkeiten, in denen sich Netzkomponenten und Netzverkabelungen befinden und verlegt sind, gehören hierzu. Es gelten die Konzernrichtlinien der Deutschen Telekom AG, insbesondere ie Binding Corporate Rules of Privacy.

5. Zugangskontrolle

Ergänzend zur Zutrittskontrolle ist es Ziel der Zugangskontrolle zu verhindern, dass DV- Anlagen von Unbefugten benutzt werden, mit denen personenbezogene Daten gespeichert, verarbeitet oder genutzt werden.

6. Zugriffsbeschränkungsprinzip

Dient zur Gewährleistung, 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 (Zugriffskontrolle)“.

Es ist die Zugriffsberechtigung auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte zu regeln (Passwörter, Benutzername). Die Zugriffsbeschränkung kann durch personelle (z.B. Einsatz bestimmter Mitarbeiter), organisatorische (z.B. Führung einer automationsunterstützten „User-Verwaltung“) und technische (z.B. Zugriffscodes) gewährleistet werden. Der Berechtigungsprozess zur Erlangung von Zugriffsrechten auf IT Systeme muss durch ein Mehrpersonenprinzip sichergestellt werden. Der Schutz der Daten, Programme und Datenverarbeitungsgeräte muss durch Authentifizierungs- und Autorisierungsmaßnahmen erfolgen.

7. Kontrolle der Weitergabe

In §20 Absatz d) der BCRP heißt es: „...zu 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 (Kontrolle der Weitergabe)“.

8. Kontrolle der Sub-Auftragnehmer

Dient zur Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können (Auftragskontrolle)".

9. Verfügbarkeitskontrolle

Dient zur Gewährleistung, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle)".

10. Trennungsgebot

Dient zur Gewährleistung, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennungsgebot)".

11. Organisationskontrolle

Definition, wie der Datenschutz im Unternehmen organisatorisch umgesetzt werden soll.

12. Protokollierungsprinzip

Es sind Protokolle zu führen, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können.

13. Dokumentationsprinzip

Es ist eine Dokumentation über die nach den Punkten 1-12 getroffenen Maßnahmen zu führen, um die Kontrolle und Beweissicherung zu erleichtern.

Impressum

Herausgeber T-Mobile Austria GmbH
Version 1.0
Stand 01.08.2018
Status final
Autor Legal
Wien, August 2018
T-Mobile Austria GmbH
Rolf-Dieter Kargl, LL.M., CIPM

Kurzinfo
Dieses Dokument ist nur gültig als Anhang eines Vertrags zur Datenverarbeitung im Auftrag und stellt einen Überblick der TOMs dar.