dsb
datenschutzbeauftragte
des kantons zürich

Fernwartung von Systemen der Informations- und Kommunikationstechnologie (IT-Systeme)

Nach § 7 IDG muss das öffentliche Organ Personendaten durch angemessene organisatorische und technische Massnahmen schützen. Diese sind auch bei der Fernwartung von IT-Systemen zu berücksichtigen.

Bei sensitiven Daten ist ein Datenschutzvermerk in den Arbeitsverträgen der von der Fernwartungsfirma angestellten Mitarbeitenden als Sicherheitsmassnahme nicht geeignet. Vielmehr ist bereits die Kenntnisnahme der Daten durch diese Mitarbeitenden auszuschliessen.

Die Fernwartung von IT-Systemen mit besonderen Personendaten (§ 3 IDG, LS 170.4) kann aus datenschutzrechtlicher Sicht nur unter Beachtung der folgenden grundsätzlichen Überlegungen zugelassen werden:

- Die Dialogverbindung darf ausschliesslich durch Verantwortliche des zu wartenden Computers aufgebaut werden können. Damit wird die Nutzung der Fernwartungsverbindung durch Unbefugte ausgeschlossen. Der Verbindungsaufbau sollte im Normalfall über festgelegte Adressen erfolgen, die im System hinterlegt sind. Die Wartungsfachperson muss sich bei jedem Wartungsvorgang mittels einer starken Authentifizierung (z.B. Chipkarte mit PIN, Token und Passwort etc.), 2-Faktor-Authentisierung analog zu Online-Banking-Lösungen anmelden.
- Sichere Kommunikationsprotokolle mit starker Verschlüsselung müssen verwendet werden.
- Die Fernwartung ist so auszugestalten, dass sie im Notfall verfügbar ist. Eine entsprechende Notfallplanung ist zu erstellen.
- Fernwartungsaktivitäten sollen lokal mitverfolgt und unterbrochen werden können. Dafür muss beim verantwortlichen Organ vor Ort eine fachkundige Person anwesend sein.
- Fernwartungsaktivitäten sind revisionssicher aufzuzeichnen. Die Protokolle müssen durch Programme ausgewertet werden können und vor Manipulationen geschützt sein.
- Mit der Fernwartungsfirma ist eine vertragliche Vereinbarung abzuschliessen, die einen Hinweis auf die Strafbestimmung von § 40 IDG enthält.
- Es sind vertragliche Regelungen über die Geheimhaltung von Daten zu treffen. Insbesondere ist festzulegen, dass Daten, die im Rahmen der Wartung extern gespeichert wurden, nach Abschluss der Arbeiten sorgfältig gelöscht werden. Die Pflichten und Kompetenzen des externen Wartungspersonals sind sorgfältig festzulegen.

V 2.3 / März 2021

Datenschutzbeauftragte des Kantons Zürich
Postfach, 8090 Zürich, +41 43 259 39 99
datenschutz@dsb.zh.ch, datenschutz.ch, twitter: @dsb_zh