

Datenschutzkonzept

Definition: Ein Datenschutzkonzept stellt die Maßnahmen in einem Unternehmen dar, die getroffen wurden, um die Regelungen zum Datenschutz einzuhalten. Es wird folglich dargestellt, wie ein Unternehmen verhindert, dass personenbezogene Daten unbefugten Dritten zugänglich werden.

Stichpunkte:

- Dokumentation
- Vorlage Datenschutzbeauftragter
- Qualitätsmerkmal
- vorgeschriebenes Verzeichnisse
- BSI IT-Grundschutzbaustein M 7.3
- Skalierung nach Schutzwürdigkeit der Daten

Unternehmen und Praxen müssen die Anforderungen, die zum Beispiel in § 9 Bundesdatenschutzgesetz festgelegt werden, dokumentieren, die bei der Verarbeitung von personenbezogenen Daten erfüllt werden müssen. Dies wird durch ein Datenschutzkonzept realisiert, das dem verantwortlichen Datenschutzbeauftragten und gegebenenfalls dem Kunden vorgelegt werden kann. Des Weiteren kann es auch der Öffentlichkeit zugänglich gemacht werden, um ein Qualitätsmerkmal des Unternehmens oder der Praxis zu verdeutlichen.

Dabei muss zwischen einem allgemeinen und einem anwendungsspezifischen Datenschutzkonzept unterschieden werden. Im allgemeinen Datenschutzkonzept werden die Anforderungen an alle Systeme und Prozesse im Unternehmen dokumentiert. Es gilt somit auch für Anwendungen, die zu klein sind, um ein eigenes Datenschutzkonzept zu erhalten oder für gerade eingeführte Systeme, für die das spezielle Datenschutzkonzept noch nicht fertig gestellt wurde. In einem anwendungsspezifischen Datenschutzkonzept werden, vom unternehmensweiten Datenschutzkonzept ausgehend, die Anforderungen weiter spezifiziert und die Informationen auf die Anwendung hin zu geschnitten. Dabei empfiehlt sich eine Einteilung des Konzeptes in eine Problembeschreibung, eine Darstellung der betroffenen Gesetze, Darstellung des Ist-Zustands und der aus diesen Beobachtungen gezogenen Maßnahmen.

Das Bundesamt für Sicherheit in der Informationstechnik sieht im Rahmen seines IT-Grundschutzes den Maßnahmenbaustein M 7.3 (https://www.bsi.bund.de/cln_165/ContentBSI/grundschutz/baustein-datenschutz/html/m07003.html [1]) für Aspekte eines Datenschutzkonzeptes vor. Dabei sollte jedoch darauf geachtet werden, dass das Konzept auch den Anforderungen entspricht. Nicht jeder Punkt, der in diesen Maßnahmenbaustein eingeflossen ist muss auch für jedes Unternehmen oder jede Anwendung beantwortet werden. Maßgeblich dafür sollte die Schutzwürdigkeit der Daten sein.

Unter anderem sollten folgende Punkte in einem Datenschutzkonzept abgedeckt werden:

- **Verfahrensverzeichnis**
Bestandteil eines jeden Datenschutzkonzeptes sollte das gesetzlich vorgeschriebene Verfahrensverzeichnis sein. Auch für das anwendungsspezifische Datenschutzkonzept empfiehlt sich zumindest der Verweis auf dieses inklusive einer Einordnung der betrachteten Anwendung.
- **Rechtsgrundlage**
Es sollte dargestellt werden, auf welcher Grundlage die entsprechenden Daten erhoben und verarbeitet werden.

- **Löschung von Daten**

Unter diesem Punkt sollte beantwortet werden, wann welche Daten gelöscht werden und welche gesetzlichen Aufbewahrungspflichten dafür die Grundlage bilden.

- **Auftragsdatenverarbeitung**

Wenn teile der Datenverarbeitung außerhalb der Firma vorgenommen werden, muss dies dokumentiert werden. Eine Dokumentation enthält, welche Daten dies genau sind und an wen diese abgegeben wurden. Außerdem sollte das Vertragsverhältnis und die Kontrollmaßnahmen aufgeführt werden.

- **Datenschutzbeauftragter**

Unter diesem Punkt sollte der Datenschutzbeauftragte des Unternehmens aufgeführt werden und seine Anmerkungen zu dem entsprechenden System, wenn es welche gibt.

- **Zugriffe**

Unerlässlich ist auch die Dokumentation derer, die auf die Daten zugriff haben. Adäquat ist hier auch eine Dokumentation durch ein Berechtigungskonzept.

- **Auskunftserteilung**

§ 34 BDSG fordert von datenverarbeitenden Stellen, dass diese Auskunft gegenüber Betroffenen erteilen können, welche Daten sie über diese verarbeiten und wer auf diese Daten Zugriff hat. Die Prozesse für einen solchen Fall sollten definiert sein, um eine zügige Antwort erteilen zu können, um Bußgeldstrafen vermeiden. Auch die Prozesse zur Information der Betroffenen bei einer Datenpanne müssen festgelegt sein, um diese anstoßen zu können, sobald sie eintreten.

Source URL: <https://www.isdsg.de/beratung/konzepterstellung/datenschutzkonzept>

Links

[1] https://www.bsi.bund.de/Cln_165/ContentBSI/grundschutz/baustein-datenschutz/html/m07003.html