Datenschutzbegehung

Warum überhaupt Datenschutz?

Auf den ersten Blick erschließt es sich nicht für Unternehmen Datenschutz zu betreiben. Die zu treffenden Maßnahmen kosten Geld und binden Mitarbeiterressourcen. Außerdem können die im Unternehmen vorhandenen Informationen nicht so miteinander verbunden werden, dass der bestmögliche Return on Investment erreicht werden kann.

Es gibt trotzdem mehrere verschiedene Gründe für Unternehmen Datenschutz zu betreiben.
Zum Einen stellt das Vertrauen der Kunden in ein Unternehmen einen Wettbewerbsvorteil dar. Vor allem in Zeiten in denen in der Presse immer wieder von Datenverlusten bei großen Unternehmen berichtet wird. Besonders im Gesundheitswesen ist dies essentiell, da hier besonders sensible Daten verarbeitet werden und fehlendes Vertrauen auch die beste Geschäftsidee zerstören kann.
Zum Anderen sieht der Gesetzgeber in Hessen seit 1970 und in der ganzen Bundesrepublik seit 1977 eine Vorrangstellung des Schutzes personenbezogener Daten im entsprechenden Datenschutzgesetz vor. Besonderen Ausdruck wurde diesem durch das Bundesverfassungsgericht 1983 verliehen, indem dieses das Recht auf informationelle Selbstbestimmung als ein Datenschutz-Grundrecht aus dem Allgemeinen Persönlichkeitsrecht im Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 („Die Würde des Menschen ist unantastbar.“) des Grundgesetzes ableitete. In §7 BDSG [1] (Bundesdatenschutzgesetz) ist geregelt, dass derjenige schadensersatzpflichtig gegenüber dem Geschädigten wird, der nicht hinreichend genug unternommen hat, um die Daten zu schützen.

Neben den finanziellen Gefahren, die einen erwarten, wenn keine Datenschutzmaßnahmen ergriffen werden, sollte vor allem die Kundenzufriedenheit genügend Anlass geben in seinem Unternehmen aktiv Datenschutz zu betreiben.

Und warum jetzt eine Datenschutzbegehung?

Das BDSG regelt den Umgang mit persönlichen Daten. Für Unternehmungen ist gefordert, dass diese die dort getroffenen Regelungen einhalten. Insbesondere §9 BDSG fordert technische und organisatorische Maßnahmen, die im angemessenen Verhältnis zu ihrem Schutzziel stehen. Diese Maßnahmen müssen nach ihrer Identifizierung im Unternehmen umgesetzt werden. Sei es durch Schulungen der Mitarbeiter, Anpassungen in der Betriebsstätte oder Dokumentation von Anwendungen und Prozessen.

Um die getroffenen Maßnahmen zu kontrollieren, sind regelmäßige Begehungen der Standorte nötig, da nur so Mängel aufgedeckt und behoben werden können, um einen konformen Betrieb nach dem Bundesdatenschutzgesetz zu ermöglichen.

Was sollte bei einer Begehung beachtet werden?

Durch die Datenschutzbegehung soll ein datenschutzkonformer Betrieb nach §9 BDSG kontrolliert werden. In der Anlage zum §9 werden dazu acht Kategorien bestimmt, die in der Organisation zu gewährleisten sind:

- **Zutrittskontrolle**
  Unbefugten soll kein Zugang zu DV-Anlagen (Datenverarbeitungsanlagen) gewehrt werden, insofern diese zur Verarbeitung von personenbezogenen Daten genutzt werden.

- **Zugangskontrolle**

Unbefugte sollen nicht die Möglichkeit haben entsprechende DV-Systeme zu nutzen.

- **Zugriffskontrolle**
  Anwender des Systems, das personenbezogene Daten verarbeitet, dürfen nur auf Daten zugreifen können, die ihren Berechtigungen entsprechen. Außerdem dürfen die Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

- **Weitergabekontrolle**
  Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder der Weitergabe über Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Außerdem muss es überprüfbar sein, wo es vorgesehen ist, welche Daten übertragen werden.
  Dies ist nur zu betrachten, wenn es Schnittstellen zu Dritten gibt.

- **Eingabekontrolle**
  Es muss nachträglich möglich sein, zu überprüfen, wer welche personenbezogene Daten eingegeben, verändert oder entfernt hat.

- **Auftragskontrolle**
  Personenbezogene Daten, die im Auftrag verarbeitet werden, dürfen dies nur im Rahmen dessen, was der Auftraggeber angewiesen hat.
  Dies ist nur zu beachten, wenn die Datenverarbeitung teilweise ausgelagert oder für andere übernommen wurde.

- **Verfügbarkeitskontrolle**
  Die Daten müssen gegen zufällige Zerstörung und Verlust geschützt werden.

- **Datentrennung**
  Daten, die zu unterschiedlichen Zwecken erhoben wurden, müssen auch getrennt voneinander verarbeitet und gespeichert werden.
  Dies ist nur relevant, wenn Daten zu unterschiedlichen Zwecken erhoben werden.

Jeder dieser Kategorien lassen sich nun technische und organisatorische Maßnahmen zuordnen, die kontrolliert werden müssen. Dies lässt sich am Besten über eine Checkliste realisieren, die bei einer Präsenzbetrachtung am Standort abgearbeitet wird.

Welche Resultate sollte die Begehung liefern?

Als zentrale Essenz der Begehung wird am Ende festgestellt, ob ein Betrieb der DV-Anlagen, der datenschutzkonform ist, gegeben ist oder nicht. Weiterhin sollte es Ziel der Begehung sein den aktuellen Ist-Zustand am jeweiligen Standort zu dokumentieren. Aus dieser Dokumentation können im Anschluss die Stärken und Schwächen abgeleitet werden, sodass Maßnahmen bestimmt werden können, die ergriffen werden müssen, um einen datenschutzkonformen Betrieb zu gewährleisten oder ihn auch weiterhin sicherzustellen.

Besonders wichtig sollte es dabei sein, neben einer detaillierten Beschreibung des Ist-Zustandes, auch für höhere Managementebenen eine übersichtliche Zusammenfassung an die Hand zu geben, damit diese alle nötigen Informationen besitzen, um eine Entscheidung treffen zu können.

Dienstleistungen des ISDSG zur Datenschutzbegehung

Das ISDSG steht Ihnen gerne bei allen Prozessschritten, die eine Begehung erfordert, zur Seite. Von der Erstbegehung über die Identifikation von Maßnahmen, der Erstellung des Datenschutzberichts, bis hin zur Wiederbegehung des Standortes, um die Umsetzung der beschlossenen Maßnahmen zu kontrollieren und gegebenenfalls neue Lücken aufzuzeigen. Auch bei der Umsetzung von Maßnahmen beraten wir Sie gerne.

Die Begehung führen wir anhand einer standardisierten Checkliste durch. Dabei werden alle in der Anlage zu §9 BDSG aufgezählten Kategorien durch spezifische Punkte erfasst und untersucht. So wird die Sicherung von Clients und Servern überprüft, genauso wie die nötige Dokumentation von Netzwerkplänen, über das Datenschutzkonzept, bis hin zum Verfahrensverzeichnis.

Auf Grundlage der Ergebnisse erstellen wir Ihnen eine fundierten Datenschutzbericht, der dies alles dokumentiert, festhält, ob ein datenschutzkonformer Betrieb momentan stattfindet, und Ihnen Vorschläge unterbreitet, wie sie den konformen Betrieb erreichen beziehungsweise sogar noch weiter verbessern können.

Links
[1] https://www.isdsg.de/informationen/gesetzestexte/bdsg