



VAFA-SPECIAL

Nur intern für VAFA-Mitglieder

Datenschutz und IT- Sicherheit – geht es nicht auch ohne?

Die Datenschutzgrundverordnung (DSGVO) ist in aller Munde und führt vielfach zu Unsicherheit. Auch IT-Sicherheit wird in vielen Betrieben kaum beachtet, oft sogar als störend empfunden. Beides ist bestenfalls problematisch und schlimmstenfalls für Ihr Unternehmen existenzbedrohend: Wie lange blieben Sie im Geschäft, wenn von heute auf morgen Ihre IT ausfällt?

Im Folgenden wollen wir kurz erläutern, was es mit der DSGVO auf sich hat und welche Anforderungen Sie erfüllen müssen um gesetzeskonform und sicher unterwegs zu sein.

Die Datenschutzgrundverordnung

Die DSGVO ist seit dem 25.05.2018 wirksam und verbietet die Verarbeitung personenbezogener Daten, **wenn die Verarbeitung nicht ausdrücklich erlaubt wurde**. Dadurch sollen insbesondere die Rechte der Bürger, das heißt Ihrer Kunden, gestärkt werden. Wichtig für Sie ist, dass die DSGVO für **alle** Unternehmen, die in der EU ansässig sind gültig ist. Es gibt

keine Ausnahmen. Sie müssen sich mit der korrekten Umsetzung beschäftigen.

Kundenrechte

Um DSGVO-konform zu sein, müssen Sie Ihren Kunden und Partnern, sofern Sie deren Daten speichern und verarbeiten, diverse Rechte einräumen:

1. Auskunft: Betroffene Personen haben das Recht zu erfahren, ob personenbezogene Daten verarbeitet werden.
2. Verarbeitungseinschränkung: Betroffene Personen dürfen die Verarbeitung Ihrer Daten auf bestimmte Zwecke beschränken oder ganz verbieten.
3. Löschung: Auf Wunsch müssen die bei Ihnen gespeicherten Daten restlos entfernt werden.
4. Widerspruchsrecht: Jederzeit darf eine gegebene Erlaubnis zur Verarbeitung widerrufen werden.
5. Portierbarkeit: Sie müssen die gespeicherten Daten auf Anfrage aushändigen, so dass diese zu einem anderen Anbieter mitgenommen werden können.

Darüber hinaus muss **Datenminimalismus** eingehalten werden:

Erheben Sie nur notwendige Daten! Diese Rechte können mit Verpflichtungen kollidieren, z.B. verlangt das Finanzamt die Speicherung von Abrechnungen, während ein Kunde die Löschung fordern kann. Da hier individuelle Fragen zu beachten sind, sollten Sie sich beraten lassen!

Was ist konkret zu tun?

VAFA-SPECIAL

Nur intern für VAFA-Mitglieder

Um Ihr Unternehmen DSGVO-konform aufzustellen müssen Sie:

1. Einwilligungs- und Datenschutzerklärungen, z.B. auf Webseiten erzeugen oder bestehende anpassen. Diese müssen über die genannten Rechte aufklären und weitere Anforderungen erfüllen. Holen Sie im Zweifel Beratung ein, da es hier zu teuren Abmahnungen kommen kann.
2. Einen Datenschutzbeauftragten bestellen falls notwendig, z.B. wenn mehr als neun Mitarbeiter Zugriff auf personenbezogene Daten haben.
3. Verarbeitungsverzeichnis erstellen und pflegen, d.h. eine Auflistung aller Tätigkeiten, die Daten verwenden und dem Grund für die Verwendung.

IT-Sicherheit

Neben der DSGVO sollten Sie sich mit der IT-Sicherheit Ihres Unternehmens befassen, um die Vertraulichkeit, Integrität und Verfügbarkeit gespeicherter Daten sicher zu stellen. Das ist auch im Ihrem Interesse. Für viele Firmen sind Computer und Daten überlebenswichtig und ein Verlust kann heute schnell in die Insolvenz führen!

Must Haves

Um eine sinnvolle Basisabsicherung Ihres Unternehmens zu erreichen sollten Sie sich mindestens über die folgenden Punkte Gedanken machen:

- Datensicherung der wichtigsten Systeme. Erproben Sie den Ernstfall, die Wiedereinspielung der Datensicherung!
- Schulung der Inhaber und des Personals im Umgang mit IT-Risiken wie etwa dem sogenannten „Social Engineering“, bei dem einfache Kommunikationstricks angewendet werden um z.B. Kennworte zu erfahren.
- Betriebssysteme und Software stets durch Updates auf dem aktuellen Stand halten.
- Gesunden Menschenverstand im Umgang mit der Informationstechnologie walten lassen! Vorsicht ist hier stets besser als Nachsicht... und angesagt.

Fazit

Für Datenschutz und IT-Sicherheit gilt: **Nicht wissen schützt nicht vor Strafe, Panik aber auch nicht.** Gehen Sie beides ruhig und gründlich an, um Gefahren zu reduzieren.

Die Autoren P. Schütz und S. Krings sind Mitarbeiter des Kompetenzzentrums für Informationssicherheit der Hochschule Niederrhein CLAVIS. Für weitere Informationen stehen wir gerne unter clavis@hs-niederrhein.de zur Verfügung.

Die Ausführungen sind freibleibend und unverbindlich, da sie nicht alle individuellen Besonderheiten und späteren Änderungen berücksichtigen können. Im Einzelfall wenden Sie sich bitte an die Geschäftsstelle oder unsere Vertragsanwälte. Im Haftungsfall ist die Haftungshöhe bzgl. aller Angaben in diesen Formularen VAFA-seitig auf maximal einen ¼-Jahresbeitrag des Mitglieds beschränkt.

DSGVO © Philipp Schütz, Sebastian Krings – VAFA 19.01 Alle Rechte vorbehalten.