**DSGVO – Datenschutz- Grundverordnung**

Die Datenschutz-Grundverordnung ist eine Verordnung der Europäischen Union, mit der die Regeln zur Verarbeitung personenbezogener Daten durch die meisten Datenverarbeiter, sowohl private wie öffentliche, EU-weit vereinheitlicht werden. Der Vorgänger (Datenschutzgesetz) war nur Österreich weit gültig.

**Datenminimierung** ist ein Grundsatz der DSGVO. Personenbezogene Daten müssen angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt zu sein.

**Verantwortlicher** ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

**Personenbezogene Daten** sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

**Sensible Daten** sind personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

**Auftragsverarbeiter** ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen bearbeitet.

**Kopplungsverbot:** Personenbezogene Daten dürfen erhoben und verarbeitet werden, wenn der Betroffene in die Verarbeitung freiwillig eingewilligt hat. Die Einwilligung ist grundsätzlich unfreiwillig und unwirksam, wenn sie an einen Vertrag gekoppelt wird (Kopplungsverbot), also Voraussetzung für den Vertragsabschluss ist die Zustimmung.

**Datendiebstahl**: Das Unternehmen hat, sobald es vom Datendiebstahl erfährt, die Betroffenen vom Datendiebstahl grundsätzlich zu informieren. Diese als Data-Breach-Notification bezeichnete Informationspflicht dient insbesondere dazu, den Betroffenen die Möglichkeit zu geben, auf die Sicherheitsverletzung entsprechend zu reagieren: Wurde ein Passwort gestohlen, das nicht nur auf der Website des Unternehmens, sondern auch auf anderen Websites verwendet wurde, muss der Betroffene es rasch ändern können.