Schutz der (Daten)Freiheit - ARAG IT-Experten über den Schutz von Verbraucherdaten

Wirtschaft Finanzen Versicherung ©

Das Zeitalter der Digitalisierung birgt viele Vorteile, aber auch Gefahren. So können beim Surfen im Internet oder bei E-Mails sensible Details wie die eigene Krankheitsgeschichte, Bankdaten oder sonstige private Informationen anderen zugänglich gemacht werden. Der Umgang mit personenbezogenen Daten ist daher gesetzlich geregelt: Sobald persönliche Daten von Kunden und auch Mitarbeitern im Spiel sind, haben Unternehmen und Behörden sie vor Missbrauch zu schützen. Doch was heißt das genau? Die ARAG IT-Experten geben einen Überblick.

Was ist die gesetzliche Grundlage?

Nach Artikel 8 der Grundrechtecharta hat jeder Mensch das Recht auf Schutz seiner personenbezogenen Daten und soll selbst entscheiden können, ob und wie persönliche Informationen von ihm genutzt werden. In Deutschland regelt das Bundesdatenschutzgesetz (BDSG) seit 1978 den Umgang mit personenbezogenen Daten in Unternehmen und Behörden. Dieses Gesetz wurde im Mai 2018 eng mit der europaweiten Datenschutz-Grundverordnung (DSGVO) verknüpft. Die DSGVO verpflichtet die Verantwortlichen dazu, die Verarbeitung von personenbezogenen Daten rechtmäßig, nachvollziehbar und transparent zu gestalten. Hinweis der ARAG IT-Experten: Sobald sich BDSG und DSGVO widersprechen, hat die DSGVO immer Vorrang.

Nach europäischer und nationaler Ebene folgt in Deutschland noch die Landesebene. Individuelle Gesetze, die für einzelne Bundesländer gelten, regeln die Landesdatenschutzgesetze (LDSG). Hier sind spezielle Vorgaben für den Umgang mit personenbezogenen Daten durch Landesbehörden, Gemeinden und andere öffentliche Stellen enthalten. Die ARAG IT-Experten

weisen darauf hin, dass für privatrechtliche Unternehmen wie eine AG, GmbH oder OHG die Landesdatenschutzgesetze nicht gelten.

Wie werden Verbraucher geschützt?

Verantwortliche Personen oder Unternehmen haben dem Verbraucher gegenüber eine Informationspflicht. Das bedeutet, dass betroffene Personen umfassend darüber informiert werden müssen, welche Daten in welcher Form über sie gespeichert sind – und auch wie diese verwendet werden. Die mit der DSGVO verschärfte Dokumentations- und Rechenschaftspflicht verpflichtet Verantwortliche zudem dazu nachzuweisen, dass Kunden ihre ausdrückliche Zustimmung zur Datenspeicherung und -verwendung gegeben haben. Darüber hinaus ist beispielsweise bei Kundendateien festzuhalten, wie personenbezogene Daten verarbeitet werden und wer darauf Zugriff hat. Auch dürfen Kundendaten nur zweckgebunden verwendet und E-Mail-Adressen von Privatpersonen nicht für Kaltakquise herausgegeben oder Kunden ungefragt kontaktiert werden.

Neu eingeführt wurde mit der DSGVO auch das sogenannte "Recht auf Vergessen werden“. Demnach sind personenbezogene Daten unverzüglich zu löschen, sobald die Daten zum ursprünglichen Verarbeitungszweck nicht mehr notwendig sind, bzw. die betroffene Person ihre Einwilligung widerrufen hat und die Daten nicht aus anderen notwendigen Aspekten oder Sachverhalten benötigt werden.

Sind auf einer Unternehmenswebsite Cookies oder Tracking-Tools im Einsatz, muss der Nutzer darüber klar und umfassend informiert werden und seine ausdrückliche Einwilligung geben. Das stillschweigende Einverständnis genügt schon lange nicht mehr. Dafür gibt es Kontrollkästchen und die Auswahl spezifischer Einstellungen. Zudem müssen strenge Datenschutzeinstellungen Standard sein. Bei der Umsetzung des erhöhten Datenschutzes helfen das sogenannte „Privacy bei Design“ und „Privacy bei Default“. Privacy by Design steht dabei für „Datenschutz durch Technikgestaltung“ und greift den Grundgedanken auf, dass sich der Datenschutz am besten einhalten lässt, wenn er bereits bei Art der Datenerfassung und -verarbeitung technisch integriert ist. Der Schutz personenbezogener Daten im Sinne der DSGVO erfolgt somit durch das frühzeitige Ergreifen technischer und organisatorischer Maßnahmen im Entwicklungsstadium. Privacy by Default ist der „Datenschutz durch datenschutzfreundliche Voreinstellungen“. Es bedeutet, dass die Werkseinstellungen datenschutzfreundlich sein müssen. Dadurch sollen auch Nutzer geschützt werden, die weniger technikaffin und eher nicht geneigt sind, die datenschutzrechtlichen Einstellungen ihren Wünschen entsprechend anzupassen.

Wie werden Angestellte und deren Daten geschützt?

Im Anstellungsverhältnis greift der Beschäftigtendatenschutz. Dieser regelt den datenschutzrechtlichen Rahmen innerhalb eines Arbeitsverhältnisses – also welche Informationen ein Arbeitgeber über Beschäftigte erheben, speichern, nutzen oder weitergeben darf. Hierzu gehören zum Beispiel Personalnummer, Kontaktdaten, Gehaltsinformationen, Krankheitsdaten oder auch Daten aus Mitarbeitergesprächen. Das BDSG enthält in Paragraf 26 eine spezielle Regelung für den Beschäftigtendatenschutz. Danach ist die Verarbeitung von Mitarbeiterdaten in Deutschland zulässig, wenn sie für die Begründung, Durchführung oder Beendigung des Arbeitsverhältnisses erforderlich ist oder der Beschäftigte eingewilligt hat. Auch bei der internen Kommunikation zwischen Kollegen in einem Unternehmen gilt das Prinzip, dass personenbezogene Daten nur mit Zustimmung der betroffenen Person weitergegeben werden dürfen. Das bedeutet, dass Informationen über einen Kollegen, wie zum Beispiel Krankheitsgründe, private Kontaktdaten oder persönliche Angelegenheiten, nicht ohne dessen Einwilligung an andere Mitarbeiter weitergeleitet werden dürfen.

Hinweis der ARAG IT-Experten: Schon während des Bewerbungsprozesses findet diese Regelung

Anwendung. Bewerber gelten somit bereits als „Beschäftigte“. Kommt es nicht zur Einstellung, sollten die Daten aber spätestens nach sechs Monaten gelöscht werden. Denn laut DSGVO dürfen Daten nur so lange gespeichert werden, wie dies für den vorgesehenen Zweck erforderlich ist.