Das Bundesdatenschutzgesetz und die Datenschutz-grundverordnung

Im Rahmen der Informations- und Kommunikationstechnologien möchte ich Sie noch über ein Randthema informieren, das bereits Gegenstand der Prüfungen war und jederzeit wieder sein kann, das Thema Datenschutz.

Seit dem 25. Mai 2018 gibt es das sogenannte Bundesdatenschutzgesetz-neu, denn seit diesem Tag ist die EU-Datenschutzgrundverordnung, kurz DSGVO, für alle Mitgliedsländer der EU verbindlich anzuwenden. Die DSGVO ist unmittelbar anzuwendendes Recht und muss daher nicht erst in ein nationales Recht umgewandelt werden, sie gilt unmittelbar für alle Mitgliedsstaaten, auch für Deutschland. Sie hob die bis dahin geltende Datenschutz-Richtlinie der EU auf, die durch nationales Recht in den einzelnen Ländern umgesetzt wurde.
Richtlinien der EU sind im Gegensatz zu Verordnungen kein unmittelbares Recht, das in den Mitgliedsländern wirkt, sondern nur Vorgaben, die durch nationales Recht und entsprechende Gesetze umgesetzt werden müssen. Dadurch wurde der Schutz personenbezogener Daten, den die Datenschutz-Richtlinie regeln sollte, in den einzelnen Mitgliedsländern der EU unterschiedlich geregelt. Um einen einheitlichen Umgang mit personenbezogenen Daten zu schaffen, wurde diese Richtlinie durch die DSGVO abgelöst, die als Verordnung für alle Mitgliedsländer unmittelbares Recht ist. Dennoch gibt es immer noch ein Bundesdatenschutzgesetz. Denn die DSGVO hat an einigen Stellen Öffnungsklauseln. An diesen Stellen sind die Regelungen offen gehalten, sodass die einzelnen Länder einen Gestaltungsspielraum haben. Diese offenen Stellen regeln sie über ihr nationales Recht, sodass das Bundesdatenschutz-gesetz immer noch eine Rolle spielt. Wir schauen uns im weiteren Verlauf drei dieser Stellen an.

Der Gesetzestext der Datenschutzgrundverordnung umfasst über 80 Seiten. Damit Sie diese nicht alle durcharbeiten müssen, finden Sie hier die 12 zentralen und für Sie wichtigsten Inhalte zusammengefasst.

1. Sinn und Zweck des Gesetzes: Schutz personenbezogener Daten

Der Schutz der eigenen, personenbezogenen Daten ist ein Grundrecht und eine Grundfreiheit jeder natürlichen Person. Daher ist jede Erhebung, Verarbeitung, Speicherung und Weitergabe personenbezogener Daten grundsätzlich nur dann erlaubt, wenn diese Person ihre Zustimmung in diese Vorgänge erteilt hat, oder ein wichtiger Grund auch darüber hinaus eine Erhebung und Nutzung dieser Daten erlaubt, unabhängig von der Zustimmung der Person.
Das ist z.B. dann der Fall, wenn eine zuständige Behörde diese Daten erhebt und nutzt, um eine Straftat aufzuklären.
Oder wenn natürliche Personen diese Daten ausschließlich zu familiären und persönlichen Zwecken nutzen, etwa weil sie ein elektronisches Datenverzeichnis über alle Kontaktdaten von Familienangehörigen anlegen.

Auch die Erfüllung eines Vertrages oder vorvertragliche Maßnahmen können eine Verarbeitung ohne explizite Zustimmung der betroffenen Person rechtfertigen, etwa wenn eine Person eine Initiativbewerbung an ein Unternehmen sendet. In diesem Fall darf dieses die personenbezogenen Daten der Person speichern, um die Anbahnung eines Arbeitsverhältnisses durchführen zu können.

Eine Erhebung von Daten ist auch dann ohne die Einwilligung der Person zulässig, wenn das berechtigte Interesse des Verantwortlichen oder eines Dritten das Recht auf den Schutz der personenbezogenen Daten der betroffenen Personen überwiegt. Das kann z.B. dann der Fall sein, wenn das Nutzerverhalten auf einer Website analysiert werden soll, um das eigene Angebot optimal an die Bedürfnisse der Nutzer dieser Website anpassen zu können und dafür Nutzerdaten, wie die Verweildauer oder das Verhalten der Nutzer auf der Website, gespeichert und analysiert werden (Art. 1, 2, 6 und 13 DSGVO).

2. Einwilligung und Widerruf der Datenverarbeitung

Beruht die Verarbeitung von Daten auf einer Einwilligung der Person, deren Daten genutzt werden sollen, muss diese Einwilligung nachgewiesen werden können. Außerdem muss die Person die Möglichkeit haben, ihre Einwilligung auf einfache Weise widerrufen zu können. (Art. 7 DSGVO).

3. Definition personenbezogener Daten

Personenbezogene Daten sind solche Daten, die direkt oder indirekt mit einer Person in Verbindung gebracht werden können. Dazu zählen neben den offensichtlichen personenbezogenen Daten wie Name, Anschrift, Geburtsdatum, E-Mailadresse, Telefonnummer oder Bankverbindung auch Daten wie die IP-Adresse oder andere Cookie-Informationen, die etwa im Zuge der Nutzung einer Internetseite gespeichert werden (Art. 4 DSGVO). Der Artikel 4 DSGVO enthält außerdem sehr viele weitere wichtige Definitionen. Sollten Sie sich unsicher sein, was ein bestimmter Begriff bedeutet, können Sie in diesem Artikel nachsehen.

4. Grundsätze der Datenverarbeitung

Es gelten unter anderem die Prinzipien der „Datenminimierung“, der „Richtigkeit“ und der „Integrität und Vertraulichkeit“. Das bedeutet zum einen, dass so viele Daten wie nötig und so wenige wie möglich gespeichert werden. Es sind nur solche Daten zu verarbeiten, die für den Zweck der Verarbeitung notwendig sind. Soll z.B. ein Geschäftsabschluss durchgeführt werden, sind Daten wie der Name, die Anschrift und die Telefonnummer wichtig, es ist aber nicht von Belang, ob die Person verheiratet ist oder welche Blutgruppe sie hat, um ein deutliches Beispiel zu nennen. Der Verantwortliche muss außerdem dafür sorgen, dass die Daten richtig und aktuell sind oder ggf. korrigiert werden, was er aber im eigenen Interesse schon tun dürfte. Und er muss dafür sorgen, dass die Daten gegen einen Datenmissbrauch durch Unbefugte gesichert sind, z.B. indem Sicherheitssysteme eingerichtet werden, wie Passwörter und Firewalls, die einen Zugriff Unbefugter von innen und von außerhalb des Unternehmens verhindern (Art. 5 DSGVO).

5. Informationspflichten bei der Datenerhebung

Personen, deren personenbezogene Daten verarbeitet werden sollen, sind umfangreich darüber zu informieren, welche ihrer Daten zu welchem Zweck gespeichert werden, wer Einsicht in diese Daten hat, wer der Verantwortliche und ggf. wer der Datenschutzbeauftragte des speichernden Unternehmens ist und ob ggf. eine Übermittlung dieser Daten in ein Drittland stattfinden soll (Art. 13 DSGVO).

Innerhalb der Union ist der freie Verkehr personenbezogener Daten weder einzuschränken noch zu verbieten, da durch die DSGVO für alle Mitgliedsländer die gleichen Datenschutzvorschriften gelten und somit der Datenschutz in allen Ländern gleich gehandhabt wird. Die Länder haben dadurch alle das gleiche Datenschutzniveau erreicht (Art. 1 Abs. 3 DSGVO). Vor dem Inkrafttreten der DSGVO gab es strenge Auflagen im BDSG, die nun aufgehoben sind.

6. Recht auf „Vergessenwerden“

Unter bestimmten Umständen (unrechtmäßige Erhebung der Daten, Widerruf der Erlaubnis, weggefallener Zweck der Verarbeitung) kann eine Person verlangen, dass ihre personenbezogenen Daten unverzüglich vom Unternehmen gelöscht werden. Ist diese Forderung aus den genannten Gründen berechtigt, muss das Unternehmen ihr nachkommen (Art. 17 DSGVO).

7. Recht auf Datenübertragbarkeit

Eine Person hat das Recht, ihre übermittelten Daten vom Verantwortlichen so zur Herausgabe zu verlangen, dass sie diese Daten an einen anderen Verantwortlichen zwecks einer Datenübertragung übermitteln kann. Sie kann außerdem verlangen, dass der Verantwortliche die Daten direkt überträgt. So könnte z.B. ein Kunde einer Bank verlangen, dass seine Daten so aufbereitet werden, dass sie direkt einer anderen Bank übermittelt werden. Dadurch spart er sich eine umständliche Neuaufnahme seiner Daten bei seiner neuen Bank (Art. 20 DSGVO).

8. Technische Maßnahmen und Verantwortung des Verantwortlichen

Der Verantwortliche setzt geeignete technische und organisatorische Maßnahmen ein, um sicherstellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung der personenbezogenen Daten nach den Vorschriften der DSGVO erfolgt (Art. 24 DSGVO). Diese Maßgabe gilt unter Berücksichtigung des aktuellen Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen (Art. 25 DSGVO).

9. Vorgaben beim Einsatz von Auftragsverarbeitern

Setzt ein Unternehmen Auftragsverarbeiter ein, muss es sicherstellen, dass diese ebenfalls den Schutz der personenbezogenen Daten durch geeignete Maßnahmen sicherstellen und nur Zugriff auf solche Daten erhalten, die notwendig sind, um ihren Auftrag durchzuführen. Auftragsverarbeiter können verschiedene Unternehmen oder

natürliche Personen sein, wie etwa ein Call-Center, das Zugriff auf die Korrespondenz und die Verträge mit dem Kunden erhält; das Steuerbüro, das die Lohnbuchhaltung durchführt; oder ein Versanddienstleister, der die Bestellungen der Kunden abwickelt. Um die gesetzlichen Vorgaben zu erfüllen, führt der Verantwortliche des Unternehmens ein Verarbeitungsverzeichnis, das Angaben darüber enthält, welche Daten wo und wann zu welchem Zweck verarbeitet werden und wer darauf Zugriff hat, wie etwa der Auftragsverarbeiter (Art. 28-32 DSGVO).

10. Sicherheitslücken und Fehler

Wird einem Unternehmen bekannt, dass der Schutz personenbezogener Daten verletzt wurde, etwa durch einen Zugriff Dritter auf die Daten, muss dieser Vorfall innerhalb von 72 Stunden nach Bekanntwerden der zuständigen Aufsichtsbehörde gemeldet werden.

Die Meldepflicht umfasst:

- Eine Beschreibung der Art der Verletzung, soweit möglich mit Angabe der ungefähren Anzahl der betroffenen Personen und Datensätze.
- Den Namen und den Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen.
- Eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes der personenbezogenen Daten.
- Sowie eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung.
- Und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Ein Beispiel für einen solchen Vorfall wäre, wenn Hacker sich in eine Bank einhacken und dadurch Zugriff auf Zugangsdaten der Bankkunden erhalten. Die Bank müsste in dem Fall diese Verletzung der zuständigen Behörde melden und auch ihre Kunden darüber informieren, sodass diese z.B. ihre Passwörter ändern könnten und überprüfen können, ob unautorisierte Transaktionen stattgefunden haben (Art. 33 DSGVO).

11. Datenschutzbeauftragte

In vielen Fällen ist ein Unternehmen dazu angehalten, einen Datenschutzbeauftragten zu benennen. Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere seines Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung seiner Aufgaben.
Bei einem solchen Beauftragten darf es sich auch um einen Externen handeln, der z.B. wie ein Anwalt oder ein Steuerberater hinzugezogen und mit dem Datenschutz beauftragt wird.

Der Datenschutzbeauftragte muss frühzeitig in alle Fragen eingebunden werden, die mit dem Schutz personenbezogener Daten zusammenhängen. Der Verantwortliche und der Auftragsverarbeiter unterstützen den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben, indem sie ihm die erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur Erhaltung seines Fachwissens erforderlichen Ressourcen zur Verfügung stellen. Sie stellen außerdem sicher, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält, er ist nicht weisungsgebunden.
Der Datenschutzbeauftragte darf von dem Verantwortlichen oder dem Auftragsverarbeiter wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Er berichtet unmittelbar der höchsten Managementebene des Verantwortlichen oder des Auftragsverarbeiters.
Betroffene Personen, z.B. Mitarbeiter, können den Datenschutzbeauftragten zu allen Fragen zu Rate ziehen, die mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte im Zusammenhang stehen.
Der Datenschutzbeauftragte ist nach dem Recht der Union oder der Mitgliedstaaten bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung oder der Vertraulichkeit gebunden.
Der Datenschutzbeauftragte kann zusätzlich andere Aufgaben und Pflichten wahrnehmen. Der Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.
Der Datenschutzbeauftragte hat zumindest folgende Aufgaben:

a) Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten zur Einhaltung aller Datenschutzvorschriften.

b) Überwachung der Einhaltung aller Gesetzesvorgaben sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters, den Schutz personenbezogener Daten sicherzustellen, einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen.

c) Beratung des Verantwortlichen zur Folgenabschätzung von Datenerhebungen, die ein hohes Risiko für die Rechte und den Schutz der Daten natürlicher Personen bedeuten könnten, z.B. aufgrund eines geplanten Einsatzes neuer Technologien.

d) Zusammenarbeit mit der Aufsichtsbehörde (Art. 37-39 DSGVO).

12. Strafen bei Verstößen gegen die DSGVO

Die Aufsichtsbehörden sind angehalten, wirksame, verhältnismäßige und abschreckende Geldbußen zu verhängen, wenn gegen die Vorschriften der DSGVO verstoßen wird. Die Höhe der Geldbuße kann dabei bis zu 20 Millionen Euro oder einen Betrag bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres betragen, je nach Art, Umfang und Schwere des Verstoßes.

Auch andere Sanktionen nach nationalem Recht sind zusätzlich zulässig, wie etwa Freiheitsstrafen (Art. 83 und 84 DSGVO).

Zum Vergleich – die Bußgelder bei Verstößen gegen das BDSG lagen bis zur Einführung der DSGVO bei 50.000 -300.000 €. Mit diesen erhöhten Bußgeldsätzen können auch große Konzerne spürbar gestraft werden, da für Konzerne mit einem Milliardenumsatz 50.000 € wie Peanuts sein dürften.

Öffnungsklauseln und Vorgaben des BDSG

Eine wichtige Öffnungsklausel, die eine spezifische Gestaltung im Rahmen des nationalen Rechts ermöglicht, enthält Artikel 88 DSGVO. Dort heißt es, dass die Verarbeitung personenbezogener Daten und ihr Schutz im Rahmen eines Beschäftigungsverhältnisses dem nationalen Recht unterliegen sollen.
Werfen wir daher noch einen Blick auf die ergänzenden Vorschriften des Bundesdatenschutzgesetzes.

§ 26 BDSG besagt:
(1) Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über

1. die Begründung eines Beschäftigungsverhältnisses
2. oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung
3. oder Beendigung
4. oder zur Ausübung oder Erfüllung der sich aus
    a. einem Gesetz oder einem Tarifvertrag
    b. einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.

Weiterhin gilt:
(2) Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Der Arbeitgeber hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Artikel 7 DSGVO in Textform aufzuklären.

Wichtig ist außerdem die ergänzende Vorschrift des **§ 38 BDSG:**
Ergänzend zu Artikel 37 DSGVO benennen der Verantwortliche als Unternehmer und der Auftragsverarbeiter einen Datenschutzbeauftragten, soweit sie in der Regel

mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.
Nehmen der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vor, die einer Datenschutz-Folgenabschätzung nach Artikel 35 DSGVO unterliegen, oder verarbeiten sie personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung, haben sie unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen einen Datenschutzbeauftragten zu benennen.
§ 6 Absatz 4, 5 Satz 2 und Absatz 6 BDSG finden Anwendung, § 6 Absatz 4 jedoch nur, wenn die Benennung einer oder eines Datenschutzbeauftragten verpflichtend ist.
In den genannten Absätzen heißt es sinngemäß:
(4) Die Abberufung der oder des Datenschutzbeauftragten ist nur in entsprechender Anwendung des § 626 des Bürgerlichen Gesetzbuchs zulässig (fristlose Kündigung aus wichtigem Grund).
Die Kündigung des Arbeitsverhältnisses ist unzulässig, es sei denn, dass Tatsachen vorliegen, welche zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen.
Nach dem Ende der Tätigkeit als Datenschutzbeauftragte oder als Datenschutzbeauftragter ist die Kündigung des Arbeitsverhältnisses innerhalb eines Jahres unzulässig, es sei denn, dass das Unternehmen zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigt ist.
(5) Die oder der Datenschutzbeauftragte ist zur Verschwiegenheit über die Identität der betroffenen Person sowie über Umstände, die Rückschlüsse auf die betroffene Person zulassen, verpflichtet, soweit sie oder er nicht davon durch die betroffene Person befreit wird.
(6) Wenn die oder der Datenschutzbeauftragte bei ihrer oder seiner Tätigkeit Kenntnis von Daten erhält, für die der Leitung oder einer bei der öffentlichen Stelle beschäftigten Person aus beruflichen Gründen ein Zeugnisverweigerungsrecht zusteht, steht dieses Recht auch der oder dem Datenschutzbeauftragten und den ihr oder ihm unterstellten Beschäftigten zu. Über die Ausübung dieses Rechts entscheidet die Person, der das Zeugnisverweigerungsrecht aus beruflichen Gründen zusteht, es sei denn, dass diese Entscheidung in absehbarer Zeit nicht herbeigeführt werden kann. Soweit das Zeugnisverweigerungsrecht der oder des Datenschutzbeauftragten reicht, unterliegen ihre oder seine Akten und andere Dokumente einem Beschlagnahmeverbot.

Interessant ist außerdem noch **§ 42 BDSG**, in dem es heißt, dass ein Verstoß gegen die Schutzvorschriften der DSGVO auch mit einer Freiheitsstrafe von bis zu drei Jahren geahndet werden kann.
Darüber hinaus ist das Bundesdatenschutzgesetz seit dem Inkrafttreten der Datenschutzgrundverordnung für Sie und Ihre Prüfung nur noch von untergeordneter Bedeutung, da es nur noch ergänzenden Charakter hat, so ist es auch nur noch in kurzen Auszügen in den Gesetzessammlungen abgedruckt. Maßgeblich ist die DSGVO als EU-Verordnung, die unmittelbaren Rechtscharakter besitzt und auch für uns Deutsche daher maßgeblich ist.