Einleitung

Unternehmen sind verpflichtet den Datenschutz und die Datensicherheit sicherzustellen. Diese Verpflichtungen betreffen somit auch jeden Mitarbeiter im Unternehmen. Durch die zunehmende arbeitsteilige Tätigkeit und den zunehmenden Einsatz von Computern, Software und die Nutzung des Internets haben sich die Anforderungen hinsichtlich des Datenschutzes und der Datensicherheit stark verändert. Dieses Merkblatt will Sie mit den wichtigsten Begriffen und Vorschriften des Datenschutzes vertraut machen.

Allgemeines zur Datenschutzgrundverordnung (DS-GVO)

- Sie gilt seit dem **25. Mai 2018.**
- Sie ist **in allen Teilen verbindlich und gilt unmittelbar** in jedem Mitgliedstaat der Union
- Sie gilt **für die automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten,** die in Dateisystemen gespeichert sind oder gespeichert werden sollen.
- Sie ist anzuwenden auf **die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt,** unabhängig vom Ort der Verarbeitung.

Sie enthält einige Neuerungen

› Dokumentationspflichten
› Informations- und Hinweispflichten
› Betroffenenrechte (Auskunftspflichten, …)
› Datenschutz-Folgenabschätzung
› Meldung von Datenschutzverstößen binnen 72 Stunden
› Haftungsrisiken
› Beweislastumkehr/Rechenschaftspflichten

Ziele der DS-GVO sind

Schutz von Personen bei der Verarbeitung personenbezogener Daten

Schutz der Grundrechte Einzelner insbesondere im Hinblick auf den Schutz ihrer personenbezogenen Daten

Einige Begriffsdefinitionen der DS-GVO

- **Personenbezogene Daten:** alle Informationen die sich auf eine identifizierte oder eine identifizierbare Person beziehen (im Folgenden: Betroffener)
- **Verarbeitung:** Erheben, Erfassen, Organisiation, Ordnen, Speichern, Verändern, Übermitteln, Löschen
- **Dateisystem:** jede strukturierte Sammlung personenbezogener Daten
- **Verantwortlicher:** die natürliche oder juristische Person, Einrichtung, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung bestimmt
- **Empfänger:** eine natürliche oder juristische Person, Stelle, Einrichtung, der personenbezogene Daten offengelegt werden
- **Dritter:** eine natürliche oder juristische Person, Einrichtung, Stelle, außer der betroffenen Person, dem Verantwortlichen oder dem Auftragsverarbeiter

- **Einwilligung der betroffenen Person:** eine freiwillig und unmissverständlich für den bestimmten Fall in informierter Weise abgegebene Willenserklärung, die ein Einverständnis zur Datenverarbeitung beinhaltet
- **Gesundheitsdaten:** personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person beziehen, einschließlich der Erbringung von Gesundheitsdienstleistungen

Grundsätze für die Datenverarbeitung:

Die Datenverarbeitung muss folgende Gebote beachten

- **Transparenzgebot**
- **Zweckbindung**
- **Datenminimierung**
- **Richtigkeit**
- **Speicherbegrenzung**
- **Integrität und Vertraulichkeit**

Die Rechtmäßigkeit der Verarbeitung setzt entweder eine Einwilligung oder eine rechtliche Grundlage voraus (Art. 6 DSGVO)

Allgemeines zum Bundesdatenschutzgesetzes (BDSG)

Das BDSG soll den Einzelnen davor schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht, das ihm durch das Grundgesetz garantiert wird, beeinträchtigt wird.

Die wichtigsten Begriffe aus dem BDSG:

Personenbezogene Daten

sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, die in den Datenschutzgesetzen Betroffener genannt werden.

Automatisierte Verarbeitung

ist die Erhebung, Verarbeitung oder Nutzung personenbezogenen Daten unter Einsatz von Datenverarbeitungsanlagen.

Datei

Dateien im Sinne der DSG sind somit automatisierte Dateien und maschinell-lesbare Datensammlungen, wie z. B. Daten auf Magnetbändern, Magnetplatten, CD/ DVD oder Mikrofilmen, sowie alle strukturierten Akten und Aktensammlungen und ihre Deckblätter.

Datenerhebung

ist das Beschaffen von Daten über den Betroffenen.

Datenverarbeitung

ist Speichern, Verändern, Übermitteln, Sperren und Löschen von personenbezogenen Daten, ungeachtet der dabei angewandten Verfahren.

Hierbei bedeutet:

Speichern: das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung;

Verändern: das inhaltliche Umgestalten gespeicherter personenbezogener Daten;

Übermitteln: das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten (Empfänger); hierzu gehört auch das Bereitstellen zum Abrufen von Daten;

Sperren: das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken;

Löschen: das Unkenntlichmachen gespeicherter personenbezogener Daten; somit gehört nach dem BDSG z. B. die Altpapier-Vernichtung und auch die Vernichtung von digitalen Datenträgern zur Datenverarbeitung.

Datennutzung

ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

Anonymisieren

ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr zugeordnet werden können.

Pseudonymisieren

ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

Verantwortliche Stelle

ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

Empfänger

ist jede Person oder Stelle, die Daten erhält

Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle.

Besondere Arten personenbezogener Daten

sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

Mobile personenbezogene Speicher- und Verarbeitungsmedien

sind Datenträger, die an den Betroffenen mit seinen personenbezogenen Daten ausgegeben werden und bei deren Nutzung ein automatisierter Verarbeitungsprozess erfolgt. Die Datenverarbeitung ist abhängig vom Einsatz des Mediums durch den Betroffenen.

Beschäftigte

im Sinne des BDSG sind:

Arbeitnehmer/innen, Auszubildende, Rehabilitanden/innen, behinderte Beschäftigte in Behinderten-werkstätten, FSJ-ler, Heimarbeitnehmer, Beamte/innen, Richter/innen des Bundes, Soldaten/innen, Zivis aber auch Bewerber/innen.

Datenvermeidung und Datensparsamkeit

Datenverarbeitung hat sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Es ist der Grundsatz der Erforderlichkeit zu beachten.

Die wichtigsten Vorschriften und Anforderungen des BDSG/ BayDSG

Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit das BDSG/Bay DSG, ein anderes Gesetz oder eine andere Rechtsvorschrift dies erlaubt (z. B. die Meldegesetze, Steuergesetz) oder wenn der Betroffene eingewilligt hat.

Personenbezogene Daten sind grundsätzlich beim Betroffenen zu erheben.

Ohne sein Mitwirken erlaubt das BDSG/ BayDSG eine Datenerhebung nur, wenn eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder eine zu erfüllende Verwaltungsaufgabe die Erhebung bei anderen Personen oder Stellen erforderlich macht oder die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordert und keine Anhaltspunkte bestehen, dass überwiegend schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

Werden Daten beim Betroffenen erhoben, so ist dieser über die verantwortliche Stelle, die Zweckbindung der Erhebung, Verarbeitung oder Nutzung seiner Daten sowie über die Übermittlung seiner Daten an Dritte zu unterrichten.

Die Unterrichtung kann entfallen, wenn der Betroffene auf andere Weise Kenntnis über die Datenerhebung, -verarbeitung und -nutzung erlangt hat.

Rechte des Betroffenen:

Der Betroffene hat das unabdingbare Recht auf Auskunft und auf Berichtigung, Löschung oder Sperrung seiner gespeicherten Daten. Die Auskunft ist schriftlich und unentgeltlich zu erteilen.

Unrichtige Daten sind zu berichtigen. Dies ist in der Praxis selbstverständlich, da aus eigenem Interesse keine falschen Daten gespeichert werden sollten. Daten müssen gelöscht werden, wenn die Speicherung unzulässig war oder wenn ihre Kenntnis für die Erfüllung des Zweckes der Speicherung nicht mehr erforderlich ist. Daten müssen gesperrt werden, wenn sie gelöscht werden müssten, aber wegen besonderer gesetzlicher oder vertraglicher Vorschriften (wie z. B. gesetzliche Aufbewahrungsfrist) nicht gelöscht werden dürfen oder aber schutzwürdige Interessen des Betroffenen durch die Löschung beeinträchtigt würden.

Datengeheimnis

Alle mit der Verarbeitung personenbezogener Daten beschäftigten Personen sind vor Aufnahme dieser Tätigkeit auf das Datengeheimnis zu verpflichten und entsprechend zu unterweisen.

Sicherungsmaßnahmen

Das BDSG/ BayDSG fordert eine Reihe von Sicherungsmaßnahmen, die gewährleisten sollen, dass Datenverarbeitungsanlagen nicht unbefugt benutzt werden und Unbefugte personenbezogene Daten (auch aus Akten bzw. Aktensammlungen) zur Kenntnis nehmen oder nutzen können. Dies muss durch technische oder organisatorische Maßnahmen geschehen.

Für die Datenverarbeitung wird in § 22 BDSG ein Katalog von möglichen Maßnahmen aufgeführt und u. a. auf die technisch organisatorischen Maßnahmen entsprechend der DS- GVO verwiesen.

Dies sind u. a. (entsprechend der Anlage 9 zu § 9 BDSG a. F.)

1. Zutrittskontrolle
   d. h. Unbefugten ist der Zugang zur Datenverarbeitungsanlage, mit denen personenbezogene Daten verarbeitet und genutzt werden, zu verwehren.
2. Zugangskontrolle
   d. h. es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.
3. Zugriffskontrolle
   d. h. es ist zu gewährleisten, dass die zur Nutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert verändert oder entfernt werden können.
4. Weitergabekontrolle
   d. h. es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.
5. Eingabekontrolle
   d. h. es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.
6. Auftragskontrolle
   d. h. es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.
7. Verfügbarkeitskontrolle
   d. h. es ist zu gewährleisten, dass personenbezogener Daten gegen zufällige Zerstörung oder Verlust geschützt sind.
8. Trennungsgebot
   d. h. es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Kontrollen

Zur Einhaltung der Bestimmungen der DS-GVO des BDSG/ LDSG gibt es drei Arten der Kontrolle:

1. **Die Eigenkontrolle durch den Betroffenen selbst.**
   Diese Kontrolle wird gewährleistet durch das unabdingbare Recht des Betroffenen auf Information, auf Auskunft und auf Berichtigung, Löschung oder Sperrung seiner gespeicherten Daten und der Weitergabe an Dritte, die seine Daten erhalten. Hierdurch erhält der Betroffene Transparenz über die zu seiner Person gespeicherten Daten und kann somit den Informationsfluss seiner Daten besser überschauen und ggf. korrigierend eingreifen.

2. **Die Selbstkontrolle durch den betrieblichen Datenschutzbeauftragten.**
   Er ist der Geschäftsleitung direkt unterstellt und hat durch die Anwendung seiner Fachkunde den Datenschutz im Unternehmen sicherzustellen, wobei das Unternehmen für die Durchführung des Datenschutzes verantwortlich ist.

3. **Die Fremdkontrolle durch den Landes-/Bundesbeauftragten für den Datenschutz bzw. durch die Aufsichtsbehörden.**
   Der Landesbeauftragte für den Datenschutz, der Bayerischen Landesbeauftragte sowie die zuständigen Aufsichtsbehörden können die Einhaltung von Datenschutzbestimmungen in öffentlichen und nicht-öffentlichen Stellen und Unternehmen überprüfen und ggf. Sanktionen verhängen (Bußgeld, Verbot von automatisierter Datenverfahren, Abbestellung des betrieblichen Datenschutzbeauftragten). Die Prüfung von Unternehmen/ Behörden usw. kann anlassfrei und somit zu jeder Zeit erfolgen.

Meldepflicht bei Datenschutzverletzungen Art. 33 DS-GVOI

Datenschutzverletzungen **müssen vom Verantwortlichen** innerhalb von 72 Stunden an die Aufsichtsbehörde gemeldet werden.

Begriff Datenschutzverletzung:

Die gesetzliche Definition der Verletzung des Schutzes pbD ist gem. Art. 4 (12) DS-GVO:

„*Verletzung des Schutzes personenbezogener Daten“ ist eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.“*

Gemeint ist also eine Verletzung des Schutzes personenbezogener Daten, die eine Verletzung der Sicherheit diese Daten und daher negative Folgen für den Betroffenen haben, wie z. B. die Vernichtung oder der Verlust der personenbezogenen Daten oder der Verlust der Integrität oder Vertraulichkeit dieser personenbezogenen Daten oder z. B. ein unbefugtes Offenlegen der Daten. In Betracht kommt hier neben der Verletzung personenbezogener Daten insbesondere auch jede Verletzung besonderer personenbezogener Daten.

Dabei spielt es keine Rolle, ob die Verletzung der Sicherheit absichtlich oder unabsichtlich erfolgt ist.

Im Falle einer Verletzung des Schutzes personenbezogener Daten **hat die Geschäftsführung** unverzüglich und möglichst binnen 72 Stunden, nachdem ihr die Verletzung bekannt wurde, diese der gemäß Artikel 55 DS-GVO zuständigen Aufsichtsbehörde zu melden, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

Wenn einem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese der Geschäftsführung unverzüglich.

Die DS-GVO regelt in den Artikeln 33 und 34 den Umgang bei Datenschutzverletzungen. Dabei sieht die DS-GVO eine abgestufte Meldepflicht vor:

1. Eine Meldung an die Aufsichtsbehörde hat immer zu erfolgen, es sei denn, dass die Datenschutzverletzung „voraussichtlich nicht zu einem Risiko“ für den Betroffenen führt.
2. Eine Benachrichtigung der betroffenen Person muss dagegen nur dann erfolgen, wenn ein hohes Risiko für deren Rechte und Freiheiten besteht

Bußgeldvorschriften

Die DS-GVO, das BDSG/ Bay DSG sieht Bußgelder für den vor, der unbefugt personenbezogene Daten, die nicht offenkundig sind, erhebt, verarbeitet oder nutzt. Der Bußgeldkatalog ist hinsichtlich seiner einzelnen Parameter umfangreicher, als noch vor einigen Jahren. Die Bußgelder gem. EU- DSGVO sind erheblich.

Verpflichtung nach § 203 Strafgesetzbuch /StGB)

Der § 203 StGB „Verletzung von Privatgeheimnissen umfasst die Strafbarkeit bei unbefugter Offenbarung eines fremden Geheimnisses, namentlich ein zum persönlichem Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, welches im Rahmen der beruflichen Tätigkeit anvertraut wird. Das Patientengeheimnis wird durch den § 203 StGB geschützt.