Sachverständigenbüro Jacob

Bernhard Jacob Dipl. Verw. Wirt, Internationaler Sachverständiger für Datenschutz und Datensicherheit

Datenschutz

in Sachverständigenbüros, Vereinen und KMU

Nachfolgend habe ich gesetzliche Grundlagen, allgemeine Informationen und meine Erfahrungen aus über vierzig Jahren Arbeit im Bereich Datenschutz kurz und knapp zusammengefasst. Diese Informationen sollen als allgemeine Übersicht gelten und ersetzen nicht eine auf die Organisation bezogene detaillierte Betrachtung und Beratung.

Es können hier nicht alle relevanten Informationen angeführt werden, insbesondere wurde wegen der besseren Lesbarkeit auf die Anführung der Fundstellen und der Erwägungsgründe verzichtet. Die hier gewählte Zusammenstellung wurde mit großer Sorgfalt erarbeitet. Trotzdem kann für den Inhalt keine Gewähr gegeben werden. Für Hinweise und Ergänzungsbitten bin ich dankbar.

Nachfolgend habe ich wegen der besseren Lesbarkeit jeweils die männliche Form der Bezeichnung gewählt. Sie gilt jedoch ebenso für w und d.

Im Februar 2020

Bernhard Jacob, Dipl.-Verwaltungswirt

Internationaler Sachverständiger für Datenschutz und Datensicherheit

Warum Datenschutz?
Der Datenschutz soll die Bürger vor Schäden durch die missbräuchliche Nutzung ihrer personenbezogenen Daten schützen.

Gesetzliche Grundlagen
Den EU-weit gültigen Rahmen bestimmt die Datenschutzgrundverordnung, DS-GVO. Sie kann, an den Punkten, wo sie entsprechende Öffnungsklauseln enthält, durch nationale Regelungen ergänzt werden. Für die Bundesrepublik ist dies durch die Neufassung des Bundesdatenschutzgesetzes, BDSG, erfolgt. Die nationalen Regelungen dürfen der DS-GVO nicht widersprechen.

Für wen gelten diese Regelungen?
Sie finden keine Anwendung auf die Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten sowie im eng umrissenen Rahmen für Behörden im Rahmen der Strafverfolgung. Ansonsten gelten sie für alle Büros, Organisationen und Firmen.

Was sind eigentlich ‚personenbezogene Daten' genau?
‚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, einer Adresse, einer Mailadresse, zu einer Kennnummer (Kfz-Kennzeichen), zu Standortdaten, zu einer Online-Kennung (IP-Adresse) identifiziert werden kann. Entscheidend ist allein, dass es gelingen kann, die Daten mit vertretbarem Aufwand einer bestimmten Person zuzuordnen.

Wenn Sie also eine Telefonnummer und/oder den Zweck eines Anrufs für einen Rückruf aufschreiben, so verarbeiten Sie personenbezogen Daten und müssen die Regelungen des Datenschutzes einhalten. In diesem Beispiel bedeutet dies auch, dass Sie den Notizzettel vor der Entsorgung schreddern müssen.

E-Mails, die personenbezogene Daten beinhalten müssen verschlüsselt übermittelt werden.

Was bedeutet in diesem Kontext ‚Verarbeitung'?
Die Regelungen gelten für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

‚Verarbeitung' ist definiert als ‚jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung,

das Löschen oder die Vernichtung personenbezogener Daten‘. Dies bedeutet, dass alle gedruckten Entwürfe oder verworfenen Schreiben vor der Entsorgung geschreddert werden müssen. Dies muss mittels eines ‚Cross-Cut‘-fähigen Schredders erfolgen. Die meisten kostengünstigen Geräte erfüllen diese Voraussetzung nicht.

Was bedeutet dies konkret?
Für die tägliche Arbeitet bedeutet diese Definition von ‚Verarbeitung‘, dass eine ‚automatisierte‘ Verarbeitung bereits vorliegt, wenn personenbezogene Daten unter Einsatz von DV-Anlagen (PC, Laptop, Tablet, Handy) erhoben, verarbeitet oder genutzt werden. Hierunter fällt, soweit personenbezogene Daten betroffen sind, bereits die bloße Textverarbeitung mittels PC ebenso, wie grundsätzlich die Nutzung eines E-Mail Programms, wie z.B. Outlook oder Thunderbird.

Wie kann die Einhaltung der Regelungen des Datenschutzes sichergestellt werden?
Der ‚Verantwortliche‘ hat die geeigneten technischen und organisatorischen Maßnahmen (TOM) zu veranlassen und sie zu dokumentieren. Er hat die notwendigen Unterlagen zu erstellen und fortzuschreiben.

Wer ist der ‚Verantwortliche‘?
‚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. In der Praxis ist es die Unternehmensleitung, also der Sachverständige, der Vorstand ‚vertreten durch…‘ oder auch die Vereinsleitung.

Der Verantwortliche ist verantwortlich für die Einhaltung von Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung sowie Integrität und Vertraulichkeit. Datenpannen sind von ihm binnen 72 Stunden an die Aufsichtsbehörde zu melden.

Der 'Verantwortliche‘ muss über die Kenntnisse zur Umsetzung und Einhaltung der gesetzlichen Regelungen verfügen, oder sich Unterstützung durch einen Datenschutzbeauftragten (DSB) sichern.

Der Datenschutzbeauftragte
Der DSB kann Beschäftigter des Verantwortlichen sein (interner DSB) oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen (zertifizierter externer DSB). Bei der Bestellung eines internen DSB ist darauf zu achten, dass dieser nicht in einen Interessenkonflikt kommt. Leitungskräfte wie Vorstände, Personaler, Finanzer oder IT-ler dürfen nicht als interne DSB bestellt werden, da sie sich sonst selbst kontrollieren müssten. Der DSB ist nicht weisungsberechtigt, gibt aber Einschätzungen und Ratschläge an den Verantwortlichen weiter; dieser wird im Allgemeinen diesen Argumenten folgen.

Wann muss ein DSB bestellt werden?
Ein DSB muss bestellt werden, wenn in der Regel mindestens zwanzig Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind (die vorstehenden Ausführungen zur ‚Verarbeitung' sind zu beachten!).

Aufgaben des DSB
Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach den geltenden Regelungen, Überwachung der Einhaltung der entsprechenden Regelungen sowie der Strategien des Verantwortlichen für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten. Die Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen sowie die Zusammenarbeit mit der Aufsichtsbehörde.

Anforderungen an den DSB, Voraussetzungen für die Bestellung
Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung insbesondere der vorstehend benannten Aufgaben.

Voraussetzung für die Verarbeitung personenbezogener Daten, Erlaubnisnorm
Eine Verarbeitung personenbezogener Daten ist nur zulässig, wenn mindestens eine der folgende Erlaubnisnormen vorliegt: Einwilligung, Vertrag oder vorvertragliche Maßnahmen auf Anfrage der betroffenen Person, rechtliche Verpflichtung (Gesetz), lebenswichtige Interessen, öffentliches Interesse/öffentliche Gewalt (Gesetz), Interessenabwägung.

Rechte der Betroffenen
Der Betroffene hat gegenüber dem Verantwortlichen folgende Rechte: Recht auf Information über die Herkunft seiner Personenbezogenen Daten, Auskunftsrecht, Recht auf Berichtigung, Recht auf Löschung und Vergessenwerden, Recht auf Einschränkung der Verarbeitung, Recht auf Datenübertragbarkeit.

Für den Fall eines Auskunftsersuchens eines Betroffenen ist dieser zu informieren zum Umfang der Datenverarbeitung, zu den Rechtsgrundlagen, zur Dauer und Löschung seiner Daten, welche persönlichen Daten von wem wann, wo und wie verarbeitet werden und welche Auskunfts-, Berichtigungs- und Widerspruchsrechte der Betroffene hat

Beweislastumkehr
Im Fall einer Beschwerde eines Betroffenen bei der Aufsichtsbehörde muss sich der Beklagte (also SIE) durch den schriftlichen Nachweis die Anforderungen der Regelungen erfüllt zu haben entlasten.

Sanktionen
Es ist mit Geldbußen für nahezu jeden Verstoß gegen die Regelungen des Datenschutzrechts in Höhe (pro Verstoß) bis zu 20.000.000 Euro oder 4% des weltweiten Jahresumsatzes zu rechnen. Erste Bußgelder, in teils erheblicher Höhe, wurden bereits verhängt.

Begriffsdefinitionen aus den gesetzlichen Fundstellen

„**personenbezogene Daten**“
alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „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 ist

„**Verarbeitung**“
jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung

„**Profiling**“
jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen

„**Pseudonymisierung**“
die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden

„**Dateisystem**“
jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird

„**Einwilligung**“
der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist

„**Verletzung des Schutzes personenbezogener Daten**“
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 wurden10

„**verbindliche interne Datenschutzvorschriften**“
Maßnahmen zum Schutz personenbezogener Daten, zu deren Einhaltung sich ein im Hoheitsgebiet eines Mitgliedstaats niedergelassener Verantwortlicher oder Auftragsverarbeiter verpflichtet im Hinblick auf Datenübermittlungen oder eine Kategorie von Datenübermittlungen personenbezogener Daten an einen Verantwortlichen oder Auftragsverarbeiter derselben Unternehmensgruppe oder derselben Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, in einem oder mehreren Drittländern

„Datenschutz“
Summe der Maßnahmen zum Schutz der personenbezogenen Daten von Betroffenen und damit Schutz der Betroffenen12

„Datensicherheit / Informationssicherheit / IT-Sicherheit“
Summe der Maßnahmen zum Schutz aller Informationen und Daten in einem Unternehmen. Diese werden im Wesentlichen von den Compliancerichtlinien und den IT-Sicherheitsgesetzen und den Eigeninteressen der Firma bestimmt

„Datensicherung“
Summe der Maßnahmen zur Sicherung aller Firmendaten, meist im Wege der Erstellung von Sicherungssätzen und deren besicherter Aufbewahrung. Sie dienen zur schnellen Wiederherstellung des Datenbestandes im Schadensfall. Diese Maßnahmen erhalten besonderes Gewicht durch die DSGVO