Jedes Unternehmen ist betroffen

Datenschutz-Grundverordnung oder warum Datenschutzverstöße kein Kavaliersdelikt sind

Verstöße gegen Datenschutzvorschriften werden oft als Kavaliers- oder Bagatelldelikte abgetan. Der geringe Verfolgungsdruck und die vergleichsweise niedrigen Bußgelder führen dazu, dass sich viele Unternehmen nur wenig oder schlimmstenfalls sogar gar nicht mit Fragen des Datenschutzes befassen. Durch die größte Reform des europäischen Datenschutzrechtes seit 1995 wird das Datenschutzrecht auf eine europaweit einheitliche Basis umgestellt und gleichzeitig werden die Bußgelder drastisch erhöht. Die Einführung neuer Aufgaben und die Ausweitung bereits bekannter Pflichten führen dazu, dass sich Unternehmen eingehend mit dem Datenschutz beschäftigten müssen, um die neuen Vorgaben einhalten zu können. Insbesondere im Personalbereich ergeben sich zahlreiche Neuerungen, wie die Pflicht Bewerber, Mitarbeiter und sonstige Personen über die Verarbeitung ihrer Daten zu informieren.

1 Einleitung

Neulich saß ich bei einem Geschäftsführer und erläuterte ihm die jüngste europäische Gesetzesänderung im Datenschutz. Je länger wir sprachen, desto weißer wurde mein Gegenüber. Er stellte sich vor, welche Auswirkungen das neue europäische Datenschutzrecht auf sein Geschäft haben wird. Sein Blick bliebt an einer Zahl hängen: zehn Mio. Euro Bußgeld – das fünffache seines Jahresumsatzes.

Die Reaktion meines Gesprächspartners macht deutlich, dass das neue europäische Datenschutzrecht, die Datenschutz-Grundverordnung, die Art und Weise wie Datenschutz im Unternehmen gelebt werden muss, deutlich verändern wird. Der folgende Beitrag gibt einen Überblick über wichtige Änderungen, die in den nächsten Ausgaben der Lohn & Gehalt an dieser Stelle vertiefend besprochen werden.

2 Die Datenschutz-Grundverordnung

Am 15. Dezember 2015 einigten sich EU-Kommission, EU-Parlament und EU-Rat im sogenannten Trilog auf die Formulierung des neuen europäischen Datenschutzrechts, die Datenschutz-Grundverordnung (DS-GVO abgekürzt). Die DS-GVO

- regelt zum ersten Mal ein Rechtsgebiet EU-weit unmittelbar fast abschließend und
- beansprucht Geltung auch für aus dem Ausland heraus auf dem europäischen Markt operierende Unternehmen.

Die Fakten im Überblick zeigt Tabelle 1.

3 Was sich ändern wird

Die Grundprinzipien des bisherigen Datenschutzrechts bleiben erhalten:

- Verbot mit Erlaubnisvorbehalt,
- Erforderlichkeit für die Verarbeitungszwecke,
- Zweckbindung,
- Löschpflicht und
- Pflicht zu angemessenen Schutzmaßnahmen.

Wie diese Prinzipien angewendet werden ändert sich und neue Vorgaben kommen hinzu. Dabei bleibt kein Bereich des Datenschutzes verschont (Abbildung 1). Im Folgenden werden ausgewählte bedeutende Änderungen angerissen.

3.1 Rechtsgrundlagen: Wann dürfen Daten verarbeitet werden?

Auch mit der DS-GVO gilt, dass personenbezogene Daten ausschließlich dann

Finale Beschlussfassung	**Durch EU-Rat und EU-Parlament voraussichtlich im April / Mai 2016**
Inkrafttreten	20 Tage nach Verkündung im EU-Amtsblatt
Wirksamwerden	2 Jahre nach Inkrafttreten (Übergangszeit)
Übergangszeit	Das bisherige Recht wird weiter angewendet.
Unmittelbare Gültigkeit	Das Gesetz gilt unmittelbar, d.h. es wird keine nationale Umsetzung mehr geben. Lediglich in wenigen Ausnahmen darf bzw. muss der deutsche Gesetzgeber eigene Gesetze erlassen.
Ende des Bundesdatenschutzgesetzes (BDSG)	Das BDSG wird mit dem Ablauf der Übergangszeit ungültig.
Inhaltliche Änderungen	Der Text ist final. Lediglich die redaktionelle Überarbeitung sowie die Übersetzung in die Nationalsprachen stehen aus.[1]
Betroffene Organisationen	Unternehmen, Verbände, Vereine, Parteien, Behörden, Ministerien usw.

Tabelle 1 Überblick über die DS-GVO

verarbeitet werden dürfen, wenn eine Rechtsgrundlage vorhanden ist. Daten sind auch in Zukunft personenbezogen, wenn sich diese „auf eine bestimmte oder bestimmbare natürliche Person beziehen“[2]. Daher fallen die Daten von juristischen Personen, wie Unternehmen und Verbänden, nicht unter das Datenschutzrecht. Daten, die nach heutigem Recht personenbezogen sind, werden es grundsätzlich auch im Lichte der DS-GVO sein.

Deutschland entwickelte ein relativ differenziertes Datenschutzrecht, das für verschiedene Anwendungen wie z. B. Werbung und Videoüberwachung detaillierte Regelungen vorsieht. Die DS-GVO kappt diese Detailregelungen weitestgehend. Was der Wegfall bedeutet, lässt sich nur im konkreten Einzelfall beantworten. Als erste Übersicht stellt Tabelle 2 (nächste Seite) sehr vereinfacht die alten und neuen Rechtsgrundlagen gegenüber.

Abbildung 1: Überblick über betroffene Bereiche des Datenschutzrechts

3.2 Betroffenenrechte: Mehr Transparenz

Eine wesentliche Neuerung ist, dass die Datenverarbeitung gegenüber den betroffenen Personen (Mitarbeiter, Bewerber usw.) offengelegt werden muss. Zwar kannte das BDSG auch Informationspflichten, die aber dank zahlreicher Ausnahmen eher selten zur Anwendung kamen. Diese Ausnahmen entfallen weitestgehend, so dass Bewerber bspw. bei der Abgabe der Bewerbung künftig u.a. folgende Informationen erhalten müssen:[4]

- Alle Zwecke der Datenverarbeitung (z. B. Bewerberauswahl, Effizienzanalyse von Bewerberportalen)
- Empfänger der Daten (z. B. Konzernunternehmen)
- Datenquellen (z. B. Xing-Profile, Bonitätsabfragen, Backgroundchecks)
- Speicherfrist oder Kriterien, um die Frist zu bestimmen (z. B. drei Monate nach Entscheidung)
- Hinweis auf die Rechte auf Auskunft, Berichtigung, Löschung, Beschränkung, Widerspruch und Datenportabilität
- Hinweis auf das Beschwerderecht gegenüber der Datenschutzaufsichtsbehörde

Die Informationspflicht gilt immer, sobald personenbezogene Daten verarbeitet werden. Auch Vertriebsaktivitäten im B2B-Geschäft, wie z. B. die Sammlung der Kontaktdaten von Ansprechpartnern im Einkauf, sind betroffen.

Die heutigen Rechte auf Auskunft, Berichtigung und Löschung bleiben erhalten. Sie werden durch neue Rechte ergänzt:

- Recht auf Datenmitnahme: Sofern die Datenverarbeitung im Rahmen eines (Arbeits)vertrags oder auf Basis einer Einwilligung erfolgt, kann z. B. ein Mitarbeiter eine maschinenverarbeitbare Kopie seiner Daten verlangen.[5]
- Recht auf Einschränkung der Verarbeitung: Die Verarbeitung der Daten kann auf Wunsch des Betroffenen (Mitarbeiter, Bewerber usw.) und unter bestimmten Voraussetzungen weitestgehend dem operativen Betrieb entzogen werden.

Die DS-GVO legt neben weiteren Vorgaben zur Bearbeitung auch einen Monat als Reaktionsfrist für die Bearbeitung der Betroffenenrechte fest, von der nur in engen Ausnahmen abgewichen werden darf.

3.3 Dokumentationspflichten

Im Vergleich mit der DS-GVO fällt auf, dass das BDSG kaum Dokumentationspflichten kennt. Die Zielsetzung der DS-GVO ist, dass das Unternehmen jederzeit in der Lage sein muss, sein mit der DS-GVO konformes Handeln zu belegen. Dazu werden verschiedene Dokumentationspflichten eingeführt. In der Konsequenz bedeutet das bspw., dass

- Prozesse definiert sein müssen,
- Mitarbeiter nachweisbar informiert werden müssen, was sie dürfen und was nicht,

BDSG	DS-GVO	Beispiele
Vertrag	Vorhanden	Kaufvertrag
Andere Gesetzliche Vorschrift	Vorhanden	Sozialgesetze, Steuergesetze
Andere Rechtsvorschriften	Vorhanden	Betriebsvereinbarung
Interessensabwägung	Vorhanden	
Einwilligung	Vorhanden	Nutzung von Mitarbeiterfotos
Allgemein zugängliche Daten	Grundsätzlich entfallen[3]	Angaben im Handelsregister
Besondere Daten	Vorhanden	Angaben zu Krankheiten, Religion
Automatisiere Einzelentscheidung	Vorhanden	Automatische Bewerbungsbearbeitung
Videoüberwachung	Entfallen	Lagerüberwachung
Mobile personenbezogene Speicher- und Verarbeitungsmedien	Entfallen	Werksausweise mit Zutrittskontrolle
Automatisierte Abrufverfahren	Entfallen	
Werberegelungen wie z.B. „Listenprivileg"	Entfallen	Briefwerbung
Werbewiderspruch	Vorhanden	
Datenübermittlung an Auskunfteien	Entfallen	Meldung an die Schufa
Scoring	Teilweise im Profiling mitgeregelt	
Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung	Entfallen	Adresshandel
Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung in anonymisierter Form	Entfallen	
Geschäftsmäßige Datenerhebung und -speicherung für Zwecke der Markt- oder Meinungsforschung	Entfallen	
Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses	Wird durch dt. Gesetzgeber geregelt	Begründung, Durchführung und Beendigung des Arbeitsverhältnisses

Tabelle 2: Vergleich der Rechtsgrundlagen nach BDSG und DS-GVO

- die Rechtsgrundlagen für alle Daten, die verarbeitet werden, dokumentiert sein müssen,
- die Löschfristen bestimmt sein müssen und
- ein Verzeichnis der Datenverarbeitungen[6] geführt werden muss.

Auftragnehmer, die als Auftragsdatenverarbeiter tätig sind, müssen zusätzlich ein Verzeichnis der Datenverarbeitungen[7], die sie für ihre Kunden durchführen, inklusive der zugehörigen Kundenliste führen. Beide Verzeichnisse sind auf Anforderung der Datenschutzaufsichtsbehörde zur Verfügung zu stellen. Das im BDSG verankerte Einsichtsrecht für jedermann entfällt.

3.4 IT-Sicherheit

Dem Schutz der Vertraulichkeit, Verfügbarkeit und Authentizität personenbezogener Daten räumt die DS-GVO einen höheren Stellenwert als bisher ein.[8] Besonders hervorzuheben sind:

Sicherheitskonzept: Technische und organisatorische Maßnahmen zur Sicherheit müssen zukünftig u. a. den Stand der Technik ebenso berücksichtigen, wie die Risiken, die eine erlaubte wie auch eine unbefugte Verarbeitung der Daten für die betroffenen Personen mit sich bringen würde. Die Erstellung eines Sicherheitskonzepts, das die ausgewählten Maßnahmen begründet, wird notwendig, um die Auswahl der Maßnahmen begründen zu können. Da sich der Stand der Technik wie auch die Angriffsmöglichkeiten stetig verändern, muss ein Prozess zur Aktualisierung des IT-Sicherheitskonzepts und auch der Maßnahmen etabliert werden. Ein Blick auf das Betriebssystem Microsoft Windows zeigt die Problematik auf. Windows 10 ist die aktuelle Version, die sicherlich als Stand der Technik bezeichnet werden kann. Der Marktanteil im Januar 2016 lag bei 12,45 Prozent während Windows 7, das im Oktober 2009 auf den Markt kam, auf 42,58 Prozent kam.[9] Entspricht Windows 7 noch dem Stand der Technik?[10]

Wirksamkeitstests: Die DS-GVO verlangt einen Prozess zum regelmäßigen Testen der technischen und organisatorischen Maßnahmen auf ihre Wirksamkeit hin.[11]

Melde- und Informationspflichten bei Sicherheitsvorfällen: Alle Sicherheitsvorfälle müssen zukünftig ausnahmslos dokumentiert werden. Sobald ein Risiko für die Betroffenen vorhanden ist, muss die Datenschutzaufsichtsbehörde im Regelfall innerhalb von 72 Stunden über den Vorfall informiert werden. Bei hohen Risiken sind zusätzlich auch die betroffenen Personen zu informieren. Wenn die Information der Betroffenen einen unverhältnismäßigen Aufwand bedeuten würde, ist die Öffentlichkeit zu informieren. Dies könnte etwa durch eine Anzeige in einer überregionalen Zeitung umgesetzt werden. Lediglich wenige Ausnahmen begrenzen diese Informationspflicht. Die Datenschutzaufsichtsbehörde kann prüfen, ob die Information der Betroffenen zulässigerweise unterlassen wird.

Unter einem Sicherheitsvorfall versteht die DS-GVO eine „Verletzung des Schutzes personenbezogener Daten", die zur Folge

hat, dass personenbezogene Daten
- zufällig oder unrechtmäßig
  - zerstört werden,
  - verloren gehen,
  - verändert werden oder
- unbefugt
  - offenbart werden,
  - Zugang gewährt wird,
  - übermittelt werden,
  - gespeichert werden oder
  - anderweitig verarbeitet werden.[12]

3.5 Neuerungen im Outsourcing

Die Änderungen im Bereich des Outsourcings beschreibt Thomas Müthlein in seinem Beitrag „Auftragsverarbeitung nach der EU-Datenschutzgrundverordnung – ein neues Zeitalter für Dienstleister beginnt“ in diesem Heft.

3.6 Haftung & Bußgelder

Das BDSG billigt dem Betroffenen in § 7 einen Schadensersatzanspruch bei einer unzulässigen oder unrichtigen Verarbeitung personenbezogener Daten zu. Den Schadensersatzanspruch weitet die DS-GVO explizit auch auf immaterielle Schäden aus. Eine unzulässige Datenverarbeitung stellt regelmäßig auch eine Grundrechtsverletzung dar, die als immaterieller Schaden aufgefasst werden kann. Damit können zukünftig nicht nur Arbeitnehmer[13], sondern auch Kunden, Verbraucher, Bewerber usw. Schadensersatz verlangen. Im Rahmen des Outsourcings mittels Auftragsdatenverarbeitung nach Art. 26 DS-GVO haften Auftraggeber und Auftragnehmer in bestimmten Grenzen gesamtschuldnerisch.[14]

Mit der DS-GVO erhöht sich der Bußgeldrahmen auf bis zu 10 Mio. Euro oder zwei Prozent des weltweiten Jahresumsatzes des Vorjahres. Für ausgewählte Verstöße, wie z. B. die Datenverarbeitung ohne Rechtsgrundlage oder die fehlerhafte Einholung einer Einwilligung, sind es 20 Mio. oder vier Prozent des weltweiten Vorjahresumsatzes. In beiden Fällen ist der jeweils höhere Wert maßgeblich.

Das Bußgeld wird im Einzelfall bestimmt. Dabei sind verschiedene Bußgeld reduzierende Faktoren, wie z. B. Maßnahmen zur Schadensreduktion gegenüber den betroffenen Personen, sowie erhöhende Faktoren, bspw. Vorsatz, zu berücksichtigen. Einen Bußgeldkatalog, wie er aus dem Straßenverkehr bekannt ist, gibt es nicht.

Das BDSG sanktioniert nicht jeden Verstoß, sondern konzentriert sich auf unerlaubtes oder unterlassenes Handeln, bspw.

- Datenverarbeitung ohne Rechtsgrundlage,
- unterlassene Information der betroffenen Personen,
- unvollständige Verträge in der Auftragsdatenverarbeitung und
- unterlassene Bestellung eines Datenschutzbeauftragten.

Die DS-GVO sanktioniert stattdessen jeden Verstoß gegen eine Vorschrift, d. h. auch
- fehlende oder unvollständige Dokumentation,
- Überschreitung von Fristen und
- fehlende IT-Sicherheitsmaßnahmen.

Durch die Ausweitung der bußgeldbewehrten Tatbestände sowie den drastisch gestiegenen Bußgeldrahmen, stellen Datenschutzverstöße ein ernstzunehmendes Existenzrisiko für Unternehmen dar.

3.7 Datenschutzaufsicht

Heute kann jede Datenschutzaufsichtsbehörde unabhängig entscheiden, wie sie die Rechtslage auslegt. Die DS-GVO will die Auslegungs-, Genehmigungs- und Vollzugspraxis europaweit harmonisieren. Dazu müssen sich die nationalen Datenschutzaufsichtsbehörden in einem neuen Gremium, dem „Europäischen Datenschutzausschuss“, abstimmen. Die dort gefassten Beschlüsse binden die nationalen Datenschutzaufsichtsbehörden. Jedes Land hat in dem europäischen Datenschutzausschuss eine Stimme und einen Sitz. Die momentan existierenden 18 deutschen Datenschutzaufsichtsbehörden[15] überlegen, wie sie mit der neuen Situation umgehen wollen. Der deutsche Gesetzgeber wird hier noch tätig werden müssen.

Heute ist die Datenschutzaufsicht territorial in Deutschland und Europa geregelt. Unternehmen, die in verschiedenen Bundesländern oder EU-Staaten Niederlassungen haben, werden von mehreren Behörden beaufsichtigt. Die DS-GVO führt den „One-Stop-Shop“ ein, d.h. die Datenschutzaufsichtsbehörde am Unternehmenshauptsitz wird regelmäßig federführend zuständig sein.[16]

4 Paradigmenwechsel: Beweise die Unschuld

Mit der DS-GVO hat der Gesetzgeber einen Paradigmenwechsel vorgenommen. Bisher steht das rechtskonforme Handeln im Mittelpunkt. Verstöße müssen von der Datenschutzaufsichtsbehörde belegt werden. Zukünftig muss das Unternehmen faktisch belegen können, dass es die Vorschriften der DS-GVO eingehalten hat.[17] Ist es nicht in der Lage, das konforme Handeln zu belegen, liegt bereits ein bußgeldbewehrter Verstoß gegen die DS-GVO vor, auch wenn kein „gravierender“ Verstoß begangen wurde und kein Schaden entstanden ist!

Der Aufbau eines Datenschutzmanagementsystems ist nicht nur empfehlenswert, sondern auch von der DS-GVO gefordert[18], das insbesondere

- die Rechtsgrundlagen aller Datenverarbeitungsvorgänge dokumentiert,
- die Einhaltung der Informations- und Meldepflichten sicherstellt,
- die Umsetzung der Betroffenenrechte in den vorgeschriebenen Fristen gewährleistet,
- die sorgfältige Auswahl von Dienstleistern unterstützt,
- die Einhaltung der Datenschutzvorschriften dokumentiert,
- die technischen und organisatorischen (Sicherheits-)Maßnahmen konzipiert und ihre Umsetzung überwacht und
- die Einhaltung aller gesetzlichen Datenschutzvorschriften und betrieblichen Regelungen kontrolliert.

Markus Bormann © www.fotolia.de

Existenzielle Dinge: Bei Verstoß gegen die EU-Datenschutzgrundverordnung drohen dramatische Strafen.

Ein solches Datenschutzmanagementsystem baut auf dem betrieblichen Datenschutzbeauftragten als Datenschutzfachmann auf. Da Aufgaben wie z. B. Dokumentation oder IT-Sicherheit tief in fachliche Tätigkeiten und Verantwortungsbereiche hinein reichen, bietet sich die Einbeziehung der jeweiligen Fachabteilungen an. Unternehmen, die keinen Datenschutzbeauftragten bestellt haben, müssen die DS-GVO ebenfalls vollumfänglich einhalten. Die Bestellung eines externen oder internen Datenschutzbeauftragten hilft Geschäftsführern und Vorständen, den Vorwurf der groben Fahrlässigkeit bei Nichteinhaltung von Datenschutzgesetzen zu entkräften, um so eine persönliche Haftung zu vermeiden. Inhaber profitieren ebenfalls durch die Bestellung eines Datenschutzbeauftragten, da sie ihrer Aufsichtspflicht nachkommen.[19]

5 Fazit: Erste Schritte zur Umsetzung

Die DS-GVO wird die Art und Weise, wie Unternehmen personenbezogene Daten verarbeiten, stark verändern. Durch die Beweislastumkehr zu Lasten der Unternehmen, entscheidet die Qualität der Dokumentation, ob der „Unschuldsbeweis“ gelingt oder nicht.

Erste Schritte auf dem Weg zur Umstellung auf die DS-GVO sind

- Information der relevanten Organe und Akteure (Geschäftsführung, Fachabteilungen, IT, Betriebsrat)
- Aufbau oder Einkauf des Fachwissens zur DS-GVO
- Erhebung des Ist-Zustands u.a. mit
  - Prozessen und ihrer Beschreibung (z. B. QM-Handbücher),
  - Zwecken für jedes Datenfeld,
  - Rechtsgrundlagen für jedes Datenfeld und
  - Einschlägigen Löschfristen,
- Aufbau eines Datenschutzmanagementsystems,
- Aufbau oder Ausbau eines Dokumentationssystems,
- Prüfung und Anpassung der Rechtsgrundlagen an DS-GVO,
- Anpassung aller Verträge zur Auftragsdatenverarbeitung und
- Prüfung und Anpassung der IT-Sicherheitsmaßnahmen.

Angesichts des hohen Anpassungsbedarfs erscheint die zweijährige Übergangszeit eher kurz als zu lang.

1 Rat der Europäischen Union, http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CONSIL:ST_5455_2016_INIT&from=EN Die im Beitrag genannten Artikel aus der DS-GVO beziehen sich auf diese Fassung. Änderungen insbesondere in der Nummerierung können sich in der verabschiedeten Fassung ergeben.
2 Art. 4 Abs. 1 DS-GVO
3 Allgemein zugängliche, besondere personenbezogene Daten wie z. B. Angaben zur Gesundheit können verarbeitet werden.
4 Lepperhoff, Niels (2016): Personalrecruiting (bald) ein risikoreiches Geschäft? In: Recruiting Tomorrow 2017
5 Art. 18 DS-GVO
6 Art 28 Abs. 1 DS-GVO
7 Art 28 Abs. 2a DS-GVO
8 Eine ausführliche Darstellung findet sich bei Lepperhoff, Niels (2016): Neue gesetzliche Pflichten für IT-Verantwortliche. In: IT-Sicherheit, Nr. 2.
9 Statistica (2016): Marktanteile der führenden Betriebssystemversionen weltweit von Januar 2009 bis Januar 2016. URL: http://de.statista.com/statistik/daten/studie/157902/umfrage/marktanteil-der-genutzten-betriebssysteme-weltweit-seit-2009/. Letzter Zugriff: 2016-03-02.
10 Art. 30 Abs. 1 DS-GVO
11 Art. 30 Abs. 1 Lit. d DS-GVO
12 Art. 4 Abs. 9 DS-GVO
13 Das LAG Mainz hat wegen einer unzulässigen Videoüberwachung Mitarbeitern ein Schmerzensgeld zugesprochen (Az. 2 Sa 540/12 v. 23.05.2013 und Az. 2 Sa 12/13 v. 23.05.2013).
14 Art. 77 DS-GVO
15 Es gibt eine für den Bund und jeweils eine für jedes Bundesland außer für Bayern, das jeweils eine Aufsichtsbehörde für öffentliche Einrichtungen und eine für nicht-öffentliche Einrichtungen unterhält.
16 Art. 51a Abs. 1 DS-GVO
17 Vgl. z. B. Art. 5 Abs. 2 DS-GVO. Ähnliche Regelungen finden sich auch an anderen Stellen.
18 Art. 22 Abs. 1+2a DS-GVO
19 Die vorsätzliche oder fahrlässige Verletzung der Aufsichtspflicht kann mit einem Bußgeld belegt werden (§ 130 OwiG).

DR. NIELS LEPPERHOFF
Geschäftsführer der Xamit Bewertungsgesellschaft mbH und der DSZ Datenschutz Zertifizierungsgesellschaft mbH