ZEIT AKADEMIE
BUSINESS

DSGVO

Ihr Fahrplan für die praktische Umsetzung

Rechtsanwälte
für Datenschutzrecht
Sebastian Herting
und David Oberbeck

HERTING
OBERBECK
DATENSCHUTZKANZLEI

ZEIT AKADEMIE

DSGVO

Ihr Fahrplan für die praktische Umsetzung

Rechtsanwälte für Datenschutzrecht Sebastian Herting und David Oberbeck

Inhalt

Lektion 1

Einführung
Welche Bedeutung hat Datenschutz in einer digitalisierten Welt?

Noch vor zehn Jahren war der Datenschutz ein totales Nischenthema. Doch heute ist er hochrelevant geworden. Ein Grund dafür ist die neue Datenschutz-Grundverordnung, kurz DSGVO. Damit macht sich das Datenschutzrecht fit für die Herausforderungen einer digitalisierten Welt.

Wie bei den meisten Gesetzesänderungen kommen auch durch die DSGVO neue Anforderungen auf die Unternehmen zu. Neben umfassenden Dokumentationspflichten müssen diverse interne Prozesse geprüft und angepasst werden. Bei Umsetzungsdefiziten oder Verstößen drohen empfindliche Bußgelder, die durch Datenschutz-Aufsichtsbehörden verhängt werden können.

Bei einem so jungen Gesetz fehlen zuweilen bewährte Konzepte, und Beispiele aus der Praxis sind rar. Dieses Seminar schließt die Lücke und unterstützt Sie aktiv bei der Umsetzung der DSGVO. Sie erhalten eine **Anleitung**, wie Sie das Thema Datenschutz in Ihrem Unternehmen angehen können. Dazu bekommen Sie **Erklärungen** und konkrete **Hilfestellungen.**

Die Grundlagen des europäischen Datenschutzrechts

Der Datenschutz hat seine Wurzeln in den Europäischen Grundrechten. Speziell in Deutschland ist der Datenschutz als das »Recht auf informationelle Selbstbestimmung« ein aus dem Grundgesetz abgeleitetes fundamentales Recht. Die Datenschutzgesetze sind letztlich Ausprägungen dieser Grundrechte.

In Europa verfolgt das Datenschutzrecht von Beginn an eine doppelte Zielsetzung. Zum einen sollen die Grundrechte der Menschen auf den Schutz ihrer persönlichen Daten gewahrt werden, zum anderen soll aber auch der freie Verkehr personenbezogener Daten gewährleistet sein, um ungehindert Waren und Dienstleistungen austauschen zu können. Datenschutzrecht soll nämlich auch Verarbeitungen möglich machen.

Aus diesem Grund muss Datenschutz aus zwei unterschiedlichen Perspektiven betrachtet werden. Auf der einen Seite steht der einzelne Mensch: Ich als Person möchte Herr meiner Daten sein und bleiben. Ich möchte selbst entscheiden, mit wem ich meine Daten teile und zu welchem Zweck meine Daten zum Beispiel durch Unternehmen verarbeitet werden dürfen.

Auf der anderen Seite stehen Unternehmen. Für sie ist eine Leistungserbringung ohne die Verarbeitung personenbezogener Daten in der Regel nicht mehr möglich. Denken Sie nur an die Auftragsabwicklung, den Zahlungsverkehr oder den Versand – überall werden Daten gebraucht. Häufig sind unsere Daten aber auch der Rohstoff ganzer Geschäftsmodelle. Sie haben für sich gesehen einen zunehmenden Wert, und entsprechend hoch sind die Begehrlichkeiten. Dieses System funktioniert nur, wenn Kunden und Nutzer darauf vertrauen können, dass ihre Daten in guten Händen sind.

Das Datenschutzrecht stellt die Spielregeln auf, nach denen personenbezogene Daten verarbeitet werden dürfen. Es regelt den Umgang mit diesen Daten und die Möglichkeiten des Einzelnen, die Kontrolle über seine Daten zu behalten. Der physische Schutz von Daten, zum Beispiel durch Maßnahmen der IT-Sicherheit, ist nur ein Teilaspekt davon.

Datenschutzgesetze gab es auch schon vor der DSGVO. Das alte Datenschutzrecht der EU basierte auf der sogenannten EU-Datenschutz-Richtlinie von 1995. Das Besondere an einer EU-Richtlinie ist, dass sie von jedem Mitgliedsstaat erst noch in nationales Recht umgesetzt werden muss. Hier hatten die Mitgliedsstaaten also einen gewissen Entscheidungsspielraum, der unterschiedlich genutzt wurde und im Ergebnis zu einem Flickenteppich unterschiedlicher Datenschutzgesetze führte. So war das deutsche Bundesdatenschutzgesetz (BDSG) schon immer recht streng, im Gegensatz zu den Regelungen zum Beispiel in Irland oder Schweden.

Bei der DSGVO, die ab dem 25.05.2018 gilt, handelt es sich nun um eine **EU-Verordnung.** Anders als eine **EU-Richtlinie** wirkt eine Verordnung unmittelbar in allen Mitgliedsstaaten, ohne dass es eines nationalen Umsetzungsakts mehr bedarf. Der Datenschutz wird also vereinheitlicht.

Neben der DSGVO wird es in den Mitgliedsstaaten aber weiterhin nationale Datenschutzgesetze geben. Das gilt zum einen für spezialgesetzliche Regelungen, beispielsweise im Bereich der Telekommunikation, zum anderen aber auch im Rahmen sogenannter Öffnungsklauseln, die die DSGVO enthält. Öffnungsklauseln sollen den Mitgliedsstaaten die Möglichkeit geben, nationale Regelungen einzubinden. Aus diesem Grund wird es in Deutschland weiterhin ein BDSG geben. Darin finden sich unter anderem Regelungen zum Beschäftigtendatenschutz und zum betrieblichen Datenschutzbeauftragten. Letztlich hat der deutsche Gesetzgeber mithilfe des neuen BDSG einige Regelungen der alten Rechtslage durch die Hintertür einfach beibehalten.

In diesem Seminar wird auf eine detaillierte Gegenüberstellung der alten mit der neuen Rechtslage verzichtet. Der Fokus liegt in den folgenden Lektionen auf den neuen Anforderungen für Unternehmen. Wenn Sie in der Vergangenheit bereits aktiven Datenschutz betrieben haben und die Vorgaben des alten BDSG einhalten, werden Sie feststellen, dass sich die tatsächlichen Änderungen in Grenzen halten.

Eine maßgebliche Änderung ist der neue Bußgeldkatalog – hier ist jetzt deutlich mehr Zug drin. Durch Bußgelder von bis zu 20 000 000 Euro oder gar vier Prozent des weltweiten Konzernumsatzes, je nachdem was höher ist, sollen die Regelungen auch in der datengetriebenen Wirtschaft genügend Beachtung finden. Die Aufsichtsbehörden sollen sicherstellen, dass Bußgelder im Einzelfall wirksam, verhältnismäßig und abschreckend sind.

Adressat des Datenschutzrechts ist erst mal jede natürliche oder juristische Person, aber auch Behörden, Einrichtungen oder andere Stellen, die in der EU niedergelassen sind. In Deutschland ansässige Unternehmen sind daher nahezu vollständig vom Geltungsbereich der DSGVO erfasst. Die Größe oder Rechtsform des Unternehmens spielt dabei keine Rolle. Die DSGVO gilt also gleichermaßen für Freiberufler, Selbstständige sowie Personen- und Kapitalgesellschaften.

Darüber hinaus gilt aber auch das sogenannte Marktortprinzip: Auch für Datenverarbeiter, die keine Niederlassung in der EU betreiben, gilt die DSGVO, wenn sie ihre Waren und Dienstleistungen in der EU anbieten. Das Marktortprinzip bewirkt, dass sich auch Unternehmen wie Amazon, Google oder Facebook an europäisches Datenschutzrecht halten müssen, wenn sie hier Geschäfte machen. Das Datenschutzrecht greift immer dann, wenn personenbezogene Daten verarbeitet werden.

Personenbezogene Daten und deren Verarbeitung

Im Datenschutzrecht dreht sich alles um den Begriff »personenbezogene Daten«. Nach dem Gesetz sind davon alle Informationen gemeint, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Geschützt sind also alle mit einem Menschen verbundene Daten, wie zum Beispiel der Name, ein Foto, die Post- oder E-Mail-Adresse.

Es liegen auch dann personenbezogene Daten vor, wenn der Bezug zu einem Menschen nur mit Zusatzwissen erzeugt werden kann. Hierzu zählen zum Beispiel Kennziffern wie Telefonnummern, Kfz-Kennzeichen, Kundennummern oder auch IP-Adressen. Der Anwendungsbereich der DSGVO endet erst da, wo eine solche Zuordnung auch mit größtmöglichem Aufwand nicht möglich ist. Nur dann sind die Daten anonym und nicht vom Datenschutzrecht erfasst.

Auch der Begriff der Datenverarbeitung ist sehr weit gefasst. Jeder vorstellbare Umgang mit personenbezogenen Daten ist von den Datenschutzgesetzen erfasst. Die DSGVO muss daher häufiger als gedacht beachtet werden.

Zur Datenverarbeitung gehört nach dem Gesetz:

1. das Erheben
2. das Erfassen
3. die Organisation
4. das Ordnen
5. die Speicherung
6. die Anpassung oder Veränderung
7. das Auslesen
8. das Abfragen
9. die Verwendung
10. die Weitergabe durch Übermittlung
11. die Verbreitung oder eine andere Form der Bereitstellung
12. der Vergleich oder die Verknüpfung
13. die Einschränkung
14. das Löschen oder die Vernichtung von Daten

Ausreichend ist dafür bereits das Zwischenspeichern im Cache eines Browsers. Einzig unstrukturierte Akten oder Aktensammlungen fallen aus dem Anwendungsbereich. Sie sind für die betriebliche Praxis aber kaum entscheidend.

Wenn ein Kunde bei Ihnen Waren bestellt und Sie deshalb Kontaktdaten in eine Datenbank oder Excel-Liste speichern, stellt dies eine Erhebung personenbezogener Daten dar. Denn über den Namen oder die E-Mail-Adresse des Kunden lässt sich ohne Probleme ein Rückschluss auf eine real existierende Person herstellen.

Vielleicht möchten Sie Ihren Kunden auch »besser kennenlernen« und speichern hierfür zusätzliche Informationen zu Hobbys oder Affinitäten zu bestimmten Themen oder auch Informationen zu vorherigen Arbeitgebern mit ab. Auch diese Informationen haben einen Bezug zu diesem Menschen und sind daher personenbezogene Daten. Eine Verarbeitung ist somit nur unter Beachtung der Datenschutzgesetze möglich.

Grundsätze der DSGVO

Die DSGVO stellt in ihrem Art. 5 Abs. 1 eine Reihe von Grundsätzen auf, die das neue Datenschutzrecht prägen. Diese Prinzipien der Datenverarbeitung sind keine bloßen Programmsätze, sondern verbindliche Vorgaben, die sich durch die ganze DSGVO ziehen. Sie müssen diese Grundsätze kennen und verstehen, um die Vorgaben der DSGVO korrekt umsetzen zu können.

Hinweis: Dieser Link führt zur Datenschutz-Grundverordnung als PDF

- **Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz:** Erlaubt sind natürlich nur rechtmäßige Datenverarbeitungen. Jede Verarbeitung muss nach Treu und Glauben und in einer Weise erfolgen, die für die betroffene Person nachvollziehbar ist. Diese Prinzipien verlangen einen fairen Umgang mit Daten und sollen Klarheit über die Verarbeitung schaffen. Dazu dienen insbesondere die Informationspflichten und Auskunftsrechte.
- **Zweckbindung**: Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben werden. Jede Weiterverarbeitung muss sich mit diesen Erhebungszwecken vereinbaren lassen. Eine Verarbeitung zu anderen Zwecken ist nur unter sehr engen Voraussetzungen möglich.
- **Datenminimierung:** Die Daten müssen auf das für den Zweck erforderliche Maß beschränkt bleiben.

- **Richtigkeit:** Daten müssen sachlich richtig sein. Daher müssen alle vertretbaren Schritte unternommen werden, damit unrichtige personenbezogene Daten gelöscht oder berichtigt werden. Diese Grundsätze werden flankiert von den Rechten der betroffenen Personen auf Berichtigung und Löschung.
- **Speicherbegrenzung:** Personenbezogene Daten dürfen nicht länger als nötig gespeichert werden. Die Speicherdauer ist daher bestenfalls schon bei Erhebung der Daten festzulegen. Wenn diese Fristen abgelaufen sind, sind die Daten wieder zu löschen.
- **Integrität und Vertraulichkeit:** Personenbezogene Daten müssen so verarbeitet werden, dass ihre Sicherheit und Vertraulichkeit gewährleistet ist. Dazu gehören gemäß Art. 25 und 32 DSGVO geeignete technische und organisatorische Maßnahmen der Datensicherheit.

Als Unternehmen müssen Sie die Verarbeitung personenbezogener Daten letztlich so organisieren, dass Sie die Einhaltung dieser Prinzipien nachweisen können. Art. 5 Abs. 2 DSGVO normiert eine entsprechende **Rechenschaftspflicht**, die ein aktives Datenschutz-Management erforderlich macht.

Mit der DSGVO müssen Unternehmen zahlreiche Pflichten zum Datenschutz beachten. Wenn diese Pflichten ignoriert oder übersehen werden, drohen empfindliche Bußgelder durch Aufsichtsbehörden. Außerdem können Wettbewerber und Verbraucherverbände Verstöße kostenpflichtig abmahnen. Und es besteht die Gefahr, dass betroffene Personen Schadensersatz von Ihnen fordern. Datenschutz ist heute ein wichtiger Vertrauenspunkt in der Beziehung zu Ihren Kunden. Der sachgemäße Umgang mit überlassenen Daten kann das Vertrauen in Ihr Unternehmen nachhaltig stärken.

Auf den Punkt

- Mit der DSGVO soll das Datenschutzrecht für die Herausforderungen einer digitalisierten Welt fit gemacht werden.
- Die Grundrechte der Menschen auf den Schutz ihrer persönlichen Daten soll zum einen gewahrt werden, zum anderen aber auch der freie Verkehr personenbezogener Daten gewährleistet sein.
- Die DSGVO von 2018 ist eine EU-Verordnung, die unmittelbar in allen Mitgliedsstaaten wirkt, ohne dass es eines nationalen Umsetzungsakts bedarf. Sie wird jedoch von weiteren Datenschutzregelungen flankiert, zum Beispiel aus dem neuen BDSG.
- Für Unternehmen ergeben sich zahlreiche neue Pflichten aus der DSGVO, bei deren Missachtung empfindliche Bußgelder drohen.

Impressum

Geschäftsführung: *Angela Broer, Nils von der Kall*
Wissenschaftliche Leitung: *Matthias Naß*
Autoren: *Sebastian Herting, David Oberbeck*
Redaktion: *Jennifer Knappheide, Stephanie Wilde*
Grafiken: *Simon Kondermann*
Cover & Umsetzung: *Ingrid Wernitz unter Verwendung eines Bildes von IStockPhoto/shulz*
Fotografie: *Felix Amsel*
Korrektorat: *Thomas Worthmann (Leitung)*

ZEIT AKADEMIE

www.zeitakademie.de

In Kooperation mit:

HERTING OBERBECK DATENSCHUTZKANZLEI

BAVARIA FILM INTERACTIVE