Datenschutz ist Chefsache

Handreichung für die Geschäftsleitung von Unternehmen

SACHSEN-ANHALT

Landesbeauftragter
für den Datenschutz

Datenschutz ist Chefsache –
Handreichung für die Geschäftsleitung von Unternehmen

Auflage: 1. Auflage, Februar 2015
Herausgeber: Der Landesbeauftragte für den Datenschutz
Sachsen-Anhalt

Inhalt

Anhang

Vorwort

Liebe Leserin, lieber Leser,

Sie sind Unternehmer, Geschäftsführer, gehören dem Vorstand eines Unternehmens an oder befinden sich in einer ähnlich verantwortlichen Position? Dann sind Sie Ansprechpartner zum Thema „Datenschutz ist Chefsache“.

Datenschutz ist ein komplexes Thema, das jedes Unternehmen betrifft. Oftmals wird sich mit dem Thema Datenschutz zu spät oder nur unzureichend auseinandergesetzt. Datenschutz ist Grundrechtsschutz! Die Verantwortung zur Einhaltung der Normen zum Datenschutz trägt die Geschäftsleitung, auch wenn die Umsetzung notwendiger Maßnahmen durch entsprechende Mitarbeiter ausgeführt wird.

Sie als Mitglied der Geschäftsleitung sind dafür verantwortlich, dass in Ihrem Unternehmen der Datenschutz Beachtung findet, eingehalten und umgesetzt wird. Der Landesbeauftragte für den Datenschutz Sachsen-Anhalt unterstützt und berät Sie dabei gern. Er ist Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich.

Datenschutz scheint Kosten zu verursachen, führt jedoch grundsätzlich zu erheblichen Vorteilen. Denn Datenschutz schafft Vertrauen bei Kunden und Geschäftspartnern sowie bei den Beschäftigten. Dies schafft positive Öffentlichkeitswirkung, stärkt die Kundenbindung und trägt zur Wettbewerbsfähigkeit Ihres Unternehmens bei.

Diese Handreichung soll Ihnen als Orientierungshilfe bei der Durchführung notwendiger Maßnahmen zur Umsetzung von Datenschutz und Datensicherheit sowie als Leitfaden zur Selbstüberprüfung dienen.

Die Broschüre wird Ihnen nicht den Blick in das Bundesdatenschutzgesetz (BDSG) oder vorrangige Gesetze, die besondere datenschutzrechtliche Sachverhalte regeln, ersparen. Im Gegenteil: Die Handreichung soll Sie animieren, sich dem Datenschutz offensiv zu widmen und zu prüfen, welche Vorschriften speziell in Ihrem Unternehmen zu beachten und umzusetzen sind. Letztlich zum Wohle Ihres Unternehmens.

Dr. Harald von Bose
Landesbeauftragter für den Datenschutz Sachsen-Anhalt

In der Broschüre werden am Seitenrand die zutreffenden Paragrafen aus den jeweils anzuwendenden Gesetzen angezeigt. Die Lesart der Abkürzung „§ 1 II 3 BDSG“ lautet „Paragraf 1 Absatz 2 Satz 3 des Bundesdatenschutzgesetzes“.

1 Schutz von personenbezogenen Daten

Welche Ziele hat der Datenschutz?

Das Grundgesetz der Bundesrepublik Deutschland sichert jedermann das allgemeine Persönlichkeitsrecht zu. Dazu gehört das Grundrecht auf informationelle Selbstbestimmung. Jeder kann über Preisgabe und Verwendung seiner persönlichen Daten grundsätzlich selbst entscheiden. Zweck des Bundesdatenschutzgesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Datenschutz gewährleistet insofern, dass nur zulässige Daten natürlicher Personen auf sparsame Weise für die vorgesehenen (Geschäfts-)Zwecke sicher verwaltet werden.

§ 1 I BDSG

Was sind personenbezogene Daten?

§ 3 I BDSG

Personenbezogene Daten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.

§ 3 IX BDSG

§ 28 VI-IX BDSG

Für den Umgang mit besonderen Arten personenbezogener Daten gelten zusätzliche Beschränkungen. Diese sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

Was ist Datenverarbeitung?

§ 3 II BDSG

§ 3 III BDSG

§ 3 IV BDSG

Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von IT-Systemen. Erheben ist das Beschaffen von Daten über den Betroffenen. Verarbeiten ist nach dem Erheben das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Speichern ist das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung. Verändern ist das inhaltliche Umgestalten gespeicherter personenbezogener Daten. Übermitteln ist das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten, sodass die Daten entweder weitergegeben werden oder zur Einsicht oder zum Abruf bereit-

gehalten werden. Sperren ist das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken. Löschen ist das Unkenntlichmachen gespeicherter Daten. *§ 3 IV BDSG*

Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person 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. *§ 3 VI BDSG* *§ 3 VIa BDSG*

Wer ist verantwortlich?

Jedes Unternehmen, das personenbezogene Daten insbesondere *automatisiert* erhebt, verarbeitet und nutzt, hat die Bestimmungen zum Datenschutz einzuhalten und ist verantwortliche Stelle im Sinne des Gesetzes bei der Anordnung und Umsetzung von Datenschutzmaßnahmen und deren Kontrolle. Zugleich sind auch die Beschäftigten, die mit der Verarbeitung der personenbezogenen Daten betraut sind, in gewissem Maße mitverantwortlich. *§ 3 VII BDSG* *§ 5 BDSG*

Wer kontrolliert die Einhaltung?

Der Betroffene als Träger des Grundrechts auf informationeller Selbstbestimmung übt im Rahmen der *Eigenkontrolle* seine Rechte aus, indem er Auskunft über seine Daten beantragt und Berichtigung, Sperrung oder Löschung seiner Daten erwirkt. *§ 34 BDSG* *§ 35 BDSG*

Das Unternehmen trägt im Rahmen der *Selbstkontrolle* die Verantwortung, organisiert den Datenschutz, bedient sich dabei gegebenenfalls des betrieblichen Datenschutzbeauftragten und schützt die personenbezogenen Daten entsprechend den gesetzlichen Vorgaben, insbesondere des Bundesdatenschutzgesetzes. *§ 4f BDSG*

Der Landesbeauftragte berät die Unternehmen in Datenschutzfragen. Als Aufsichtsbehörde überprüft er im Rahmen der *Fremdkontrolle* die Einhaltung der Datenschutzvorschriften, unterbindet unzulässige Verfahren und kann Bußgelder verhängen oder Strafanträge stellen. *§ 38 I BDSG* *§ 38 V BDSG* *§§ 43, 44 BDSG*

2 Pflichten der verantwortlichen Stelle

Generell haben Unternehmensleitungen darauf zu achten, dass der gesamte Umgang mit personenbezogenen Daten rechtmäßig ist. Dazu sind besonders wichtige Grundsätze einzuhalten.

Zulässigkeit

§ 4 I BDSG

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, wenn der Betroffene eingewilligt hat oder eine Rechtsvorschrift dies erlaubt. Soweit keine Erlaubnisvorschriften aus speziellen Gesetzen angewendet werden können, sind die des Bundesdatenschutzgesetzes zu prüfen. Ein Umgang mit Daten, der weder durch Rechtsvorschriften noch durch eine Einwilligung erlaubt wird, ist unzulässig.

Datensparsamkeit

§ 3a BDSG

Es sind so wenig personenbezogene Daten zu erheben, zu verarbeiten oder zu nutzen, wie zur Durchführung der Unternehmenstätigkeiten benötigt werden. Wenn möglich, sind Daten zu anonymisieren oder pseudonymisieren. Daten, die nicht mehr gebraucht werden, müssen gelöscht werden, wenn dem keine Aufbewahrungsfristen entgegenstehen.

§ 35 II BDSG

Zweckbindung

Der Grundsatz der Zweckbindung soll gewährleisten, dass Daten nur für den Zweck verarbeitet werden, für den sie erhoben worden sind. Daher ist die *anlasslose* Sammlung personenbezogener Daten auf Vorrat unzulässig. Der Zweck der jeweiligen Datenerhebung ist festzustellen und sollte aus Beweisgründen schriftlich dokumentiert werden. Eine Verarbeitung abweichend vom ursprünglichen Zweck ist möglich, wenn eine Einwilligung des Betroffenen vorliegt oder das Gesetz es ausdrücklich zulässt. In der Praxis ist Vorsicht immer dann geboten, wenn unterschiedliche Bestände von personenbezogenen Daten verknüpft werden sollen.

§ 4a BDSG

§ 28 II BDSG

Direkterhebung

§ 4 II BDSG

Personenbezogene Daten sind mit wenigen Ausnahmen direkt beim Betroffenen selbst zu erheben.

Informationspflichten

Datenschutz erfordert Transparenz. Daher legt das Bundesdatenschutzgesetz Informationspflichten an unterschiedliche Adressaten fest. Im Fall der Direkterhebung ist der Betroffene über die verantwortliche Stelle und den Zweck der Erhebung, Verarbeitung und Nutzung zu unterrichten. Häufig ist der Betroffene unverzüglich zu informieren, wenn seine Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten zur Kenntnis gelangt sind und dadurch schwerwiegende Beeinträchtigungen für seine Rechte oder schutzwürdige Interessen drohen. In diesen Fällen ist zusätzlich der Landesbeauftragte für den Datenschutz zu informieren, insbesondere auch über im Unternehmen getroffene Abhilfemaßnahmen.

§ 4 III BDSG

§ 42a BDSG

Auskunftsanspruch des Betroffenen

Auf Verlangen des Betroffenen ist sein allgemeiner Auskunftsanspruch zu beachten. Danach hat die verantwortliche Stelle unentgeltlich Auskunft zu erteilen über die zu seiner Person gespeicherten Daten und weitere im Gesetz näher ausgeführte Umstände, wie den Datenempfänger und den Speicherungszweck.

§ 34 BDSG

Berichtigung, Löschung und Sperrung

Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Zu löschen sind sie insbesondere dann, wenn sie für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich sind und keinen Aufbewahrungspflichten unterliegen. Daten, die für den ursprünglichen Zweck nicht mehr erforderlich sind, aber nicht gelöscht werden dürfen, müssen gesperrt werden.

§ 35 BDSG

§ 257 HGB

Leistung von Schadensersatz

Das Bundesdatenschutzgesetz enthält eine eigenständige Haftungsnorm, die neben vertraglichen und anderen gesetzlichen Haftungsnormen gilt. Sie setzt eine unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung personenbezogener Daten voraus. Die Ersatzpflicht trifft die verantwortliche Stelle. Sie entfällt, wenn diese darlegen und ggf. beweisen kann, dass sie kein Verschulden trifft.

§ 7 BDSG

§ 823 BGB

3 Datenschutzmanagement

Datenschutz als Führungsaufgabe

In allen Wirtschaftsunternehmen – unabhängig von Größe und Branche – stellt sich die Frage, ob die Wahrnehmung der Aufgaben des Datenschutzes intern so organisiert und geregelt ist, dass die gesetzlichen Vorgaben des Datenschutzes eingehalten werden. Bei den Unternehmensleitungen liegt die Gesamtverantwortung. Datenschutz ist insoweit Führungsaufgabe und damit Chefsache. Zu klärende Einzelfragen sind z. B.:

§ 3 VII BDSG

- Sind die Zuständigkeiten im Unternehmen in Bezug auf Datenschutz und Datensicherheit geklärt?
- Muss oder sollte ein betrieblicher Datenschutzbeauftragter bestellt werden? Kann die Aufgabe ein Unternehmensangehöriger wahrnehmen oder muss ein externer Datenschutzbeauftragter bestellt werden?

§ 4f BDSG

- Ist sichergestellt, dass die gesetzlich geforderten Dokumentationen erstellt und vorgehalten werden?
- Ist sichergestellt, dass die Beschäftigten, die mit Datenverarbeitung befasst sind, auf das Datengeheimnis verpflichtet wurden und sind sie für ihre Aufgabe ausreichend geschult?

§ 5 BDSG

- Sind ausreichende Kontrollmechanismen implementiert?

Meldepflicht und Verfahrensverzeichnis

§ 4d BDSG
§ 4e BDSG

Verfahren automatisierter Verarbeitungen sind vor Inbetriebnahme der Aufsichtsbehörde zu melden. Die Einzelangaben der Meldepflicht ergeben sich aus dem Bundesdatenschutzgesetz. Diese Meldepflicht kann in Kleinstbetrieben oder bei Bestellung eines betrieblichen Datenschutzbeauftragten entfallen. Allerdings muss das Unternehmen in diesem Fall die Angaben dem betrieblichen Datenschutzbeauftragten vorlegen. Dieses *Verfahrensverzeichnis* dient der internen Selbstkontrolle und soll dem Datenschutzbeauftragten seine Prüf- und Kontrolltätigkeiten erleichtern. Außerdem ermöglicht es ihm, wesentliche Angaben für jedermann auf Antrag verfügbar zu machen.

§ 4g II BDSG

Datengeheimnis

Das Datengeheimnis beinhaltet das Verbot für die bei der Datenverarbeitung beschäftigten Personen, *unbefugt* personenbezogene Daten zu erheben, zu verarbeiten oder zu nutzen. Unternehmensleitungen haben dafür zu sorgen, dass dieser Personenkreis bei der Aufnahme seiner Tätigkeit auf das Datengeheimnis verpflichtet wird. Dies sollte zu Beweiszwecken schriftlich erfolgen. Auch Personen, die personenbezogene Daten lediglich zur Kenntnis nehmen können, sollten verpflichtet werden.

§ 5 BDSG

Risikoanalyse und Schutzbedarf

Wichtig ist, dass ein Unternehmen sich der eigenen Risiken bzgl. des Umgangs mit personenbezogenen Daten bewusst wird. Dazu ist eine Risikoanalyse erforderlich, die zunächst feststellt, in welchen Bereichen des Unternehmens mit welchen personenbezogenen Daten umgegangen wird. Anschließend muss ermittelt werden, wie die Daten geschützt sind. Bedarf das Unternehmen zur Feststellung der Gefährdungspotenziale der fachlichen Unterstützung oder kann es sie selbst feststellen? Ist der bestehende Schutz ausreichend oder sind weitere technische und organisatorische Maßnahmen erforderlich?

Bergen automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen, so ist vor Beginn der Verarbeitung in der Regel eine rechtliche und technische *Vorabkontrolle* durchzuführen. Dies gilt unter anderem bei besonderen Arten personenbezogener Daten.

§ 4d V BDSG

Interne Regelungen

Jedes Unternehmen hat eigene Geschäftsabläufe und Strukturen und verfügt über unterschiedliche personenbezogene Daten. Dafür sollten Unternehmensleitungen zur Konkretisierung gesetzlicher Vorgaben Regelungen treffen, die für die Mitarbeiter verbindlich sind und eindeutig den Umgang mit personenbezogenen Daten bestimmen. Aufgaben und jeweilige Verantwortlichkeiten sollten genau dokumentiert werden. Derartige Regelungen können durch Betriebsvereinbarungen unterstützt werden.

§ 77 BetrVG

4 Der betriebliche Datenschutzbeauftragte

Bestellung

§ 4f I BDSG

Unternehmen müssen einen Datenschutzbeauftragten bestellen, wenn personenbezogene Daten durch mindestens 10 Personen automatisiert oder durch mindestens 20 Personen auf andere Weise erhoben, verarbeitet oder genutzt werden. Unterliegen Verfahren einer Vorabkontrolle, ist ebenfalls ein betrieblicher Datenschutzbeauftragter zu bestellen. Dies gilt auch, wenn personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung automatisiert verarbeitet werden. In jedem Fall hat die Bestellung schriftlich zu erfolgen und nicht später als einen Monat nach Aufnahme der Tätigkeit. Wer diese Frist versäumt, begeht eine Ordnungswidrigkeit.

§ 43 I Nr. 2 BDSG

Fachkunde

§ 4f II BDSG

Zum betrieblichen Datenschutzbeauftragten darf nur bestellt werden, wer die erforderliche Fachkunde für diese Aufgabe besitzt. Er muss also das Bundesdatenschutzgesetz, die einschlägigen speziellen datenschutzrechtlichen Regelungen und die Spezialvorschriften seines Fachbereichs kennen und sicher anwenden können. Außerdem sollte er über grundlegende Kenntnisse über die Unternehmensorganisation und Informationstechnik verfügen. Diese Mindestkenntnisse müssen bereits bei seiner Bestellung vorliegen. Der betriebliche Datenschutzbeauftragte hat Anspruch auf Fortbildung.

§ 4f III BDSG

Interessenkonflikte

Der betriebliche Datenschutzbeauftragte ist Kontrollinstanz im Unternehmen und zugleich zur Verschwiegenheit verpflichtete Vertrauensperson als „Vermittler“ zwischen den Interessen der Geschäftsleitung, der Beschäftigten und der Betroffenen.

Diese Funktion kann kaum wahrgenommen werden, wenn der Datenschutzbeauftragte auch noch Aufgaben auf den Gebieten Personalverwaltung, Informationstechnik oder Verarbeitung besonders sensibler perso-

nenbezogener Daten erfüllt. Es ist vor der Bestellung zu prüfen, ob es zu solchen Interessenkonflikten kommen könnte.

Ausstattung

Der betriebliche Datenschutzbeauftragte hat, soweit dies für eine ordnungsgemäße Aufgabenerfüllung erforderlich ist, Anspruch auf geeignete Arbeitsräume, Einrichtungen und Mittel oder deren Mitnutzung. Bei der Ausübung seiner Tätigkeit hat ihn das Unternehmen zu unterstützen. Nach dem Gesetz ist ihm, wenn die Fülle seiner Aufgaben es gebietet, Hilfspersonal zur Verfügung zu stellen.

§ 4f V BDSG

Tätigkeit und Aufgaben

Durch Gesetz sind die Aufgaben des betrieblichen Datenschutzbeauftragten benannt: Vertrautmachen des Personals mit den einschlägigen datenschutzrechtlichen Vorschriften und Hinwirken auf die Einhaltung dieser Vorschriften, Überwachung der Datenverarbeitungsprogramme, mit denen personenbezogene Daten verarbeitet werden, Vorabkontrolle der für die Rechte der Betroffenen besonders risikoreichen Datenverarbeitungen, Verfügbarmachen des Verfahrensverzeichnisses für jedermann. In datenschutzrechtlichen Fragen kann er die Unternehmensleitung durch seine gezielte Beratung auch aktiv unterstützen. Dazu sollte der betriebliche Datenschutzbeauftragte von datenschutzrelevanten Planungen des Unternehmens rechtzeitig unterrichtet werden. Betroffene können sich jederzeit an ihn wenden.

§ 4g BDSG

§ 4f V BDSG

Verantwortung und Rechte

Der betriebliche Datenschutzbeauftragte ist der Unternehmensleitung direkt zu unterstellen und im Rahmen seiner Aufgabenwahrnehmung weisungsfrei. Er kann sich an den Landesbeauftragten wenden, der ihn berät und unterstützt.

§ 4f III BDSG

§ 4g I BDSG
§ 38 I BDSG

Er darf wegen seiner Aufgabenwahrnehmung nicht benachteiligt werden. Seine Kündigung ist nur aus wichtigem Grund möglich.

§ 4f III BDSG

5 Auftragsdatenverarbeitung

Viele Unternehmen bedienen sich zur Abwicklung des Umgangs mit personenbezogenen Daten externer Dienstleister. Werden solche tätig, sind datenschutzrechtlich zwei Konstellationen möglich. Es handelt sich entweder um eine Auftragsdatenverarbeitung oder um eine Funktionsübertragung.

Wenn dem Dienstleister eigenständige rechtliche Zuständigkeiten zugewiesen werden, liegt eine *Funktionsübertragung* vor. Beispiel: Eigenständige Kundenbefragungen durch Institute. Bei der Funktionsübertragung wird der Dienstleister verantwortliche Stelle im Sinne des Bundesdatenschutzgesetzes. Der Datenaustausch darf hier nur erfolgen, wenn die rechtlichen Voraussetzungen einer Datenübermittlung erfüllt sind.

Im Auftrag der verantwortlichen Stelle

§ 11 BDSG

Eine eigentliche *Auftragsdatenverarbeitung*, die nicht an die hohen Voraussetzungen einer Datenübermittlung gebunden ist, liegt nur dann vor, wenn der Auftraggeber Herr der Daten bleibt und der Auftragnehmer bzgl. der Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten ausschließlich weisungsgebunden handelt. Der Auftragnehmer darf hierbei die Daten nicht zu eigenen Zwecken erheben, verarbeiten oder nutzen.

§ 3 VII BDSG

Bei der Auftragsdatenverarbeitung bleibt allein der Auftraggeber die verantwortliche Stelle. Beispiel: Archivieren von Daten; Entsorgung von Daten durch Löschen oder Vernichten; Auslagerung der Gehaltsabrechnung.

Rahmenbedingungen

Im Falle der Auftragsdatenverarbeitung hat der Auftraggeber den Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig

§ 11 II BDSG

auszuwählen. Der Auftrag ist schriftlich zu erteilen und muss diverse Festlegungen enthalten, insbesondere über Umfang und Zweck, den Kreis der Betroffenen, die Schutzmaßnahmen, die Pflichten des Auftragnehmers und die Kontrollrechte des Auftraggebers. Vor Beginn der Datenverarbeitung und sodann regelmäßig hat der Auftraggeber den Auftragnehmer auf Einhaltung erforderlicher technischer und organisatorischer Maßnahmen zu kontrollieren.

Unternehmen, die Fernwartungsarbeiten durchführen, sind wie Auftragnehmer einer Auftragsdatenverarbeitung zu behandeln, soweit der Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. *§ 11 V BDSG*

Auftragnehmer im Ausland

Befindet sich der Auftragnehmer im Ausland, ist zu unterscheiden, ob er sich innerhalb der Europäischen Union (EU) bzw. des Europäischen Wirtschaftsraumes (EWR) oder in einem sogenannten Drittstaat befindet. Innerhalb der EU bzw. des EWR sind die Vorschriften des Bundesdatenschutzgesetzes anzuwenden. Bei Auftragsvergabe an Auftragnehmer in Drittstaaten sind besondere Bedingungen zu beachten. Wichtig ist insbesondere, sicherzustellen, dass in dem Drittstaat ein angemessenes Datenschutzniveau gewährleistet wird.

§ 4b I BDSG

§ 4b II BDSG
§ 4c BDSG

Cloud Computing als Spezialfall

Ein spezieller Fall der Auftragsdatenverarbeitung ist das Cloud Computing, welches eine Bereitstellung von IT-Infrastruktur, wie z. B. Speicherkapazität, und Software als Serviceleistung beinhalten kann.

Zu warnen ist insbesondere vor der Nutzung von Cloud-Diensten, die einer breiten Öffentlichkeit ohne individuelle vertragliche Gestaltung zur Verfügung stehen und damit keine Möglichkeit eines schriftlichen Vertrags im Sinne der Auftragsdatenverarbeitung eröffnen.

Bei Cloud-Anbietern aus Drittstaaten ist oft nicht klar, in welchen Staaten die Server stehen, auf denen die Daten gespeichert sind. Damit ist auch ungewiss, welchem Datenschutzniveau die Infrastruktur unterliegt. Es sollten daher nur Cloud-Anbieter genutzt werden, die verlässliche Auskunft darüber geben können, wo der Server steht, sich vertraglich binden und kontrollieren lassen.

6 Maßnahmen zur Datensicherheit

§ 9 BDSG

Nachfolgend werden die in der Anlage zum Bundesdatenschutzgesetz erwähnten erforderlichen technischen und organisatorischen Mindest-Maßnahmen bei der automatisierten Datenverarbeitung beschrieben. Die Aufzählung ist nicht abschließend. Angesichts der Risiken durch moderne Datenverarbeitung sind weitergehende Sicherheitsmaßnahmen oftmals geboten.

Zutrittskontrolle

Anl. § 9 Nr. 1 BDSG

Unbefugten ist der Zutritt zu den Datenverarbeitungsanlagen zu verwehren, z. B. durch den Einsatz von Alarmanlagen, Schließsystemen oder die Überwachung der Räume und ihren Eingangsbereichen.

Zugangskontrolle

Anl. § 9 Nr. 2 BDSG

Die unbefugte Nutzung der Datenverarbeitungssysteme ist zu verhindern, z. B. durch die Authentifikation mit sicheren Passwörtern oder biometrischen Merkmalen sowie den Einsatz von Virenschutzlösungen und Firewalls. Die Verschlüsselung von Inhalten und Datenträgern kann die vorgenannten Maßnahmen verstärken.

Zugriffskontrolle

Anl. § 9 Nr. 3 BDSG

Nur berechtigte Personen sollen die ihnen freigegebenen personenbezogene Daten verarbeiten und nutzen können, währenddessen Unberechtigte diese Daten weder lesen noch verändern dürfen. Dies wird z. B. erreicht durch das Erstellen von Berechtigungskonzepten, die Verwaltung der Nutzerrechte von wenigen Systemadministratoren, die Durchsetzung strenger Passwortrichtlinien mit regelmäßigem Passwortwechsel, den Einsatz von Verschlüsselungsverfahren, die Protokollierung von Datenzugriffen sowie die sichere Aufbewahrung und Vernichtung von Datenträgern.

DIN 66399

Weitergabekontrolle

Anl. § 9 Nr. 4 BDSG

Bei der Übertragung und Speicherung dürfen personenbezogene Daten nicht gelesen, kopiert, verändert oder entfernt werden können. Der Empfänger dieser Daten muss jederzeit bekannt sein. Dies wird z. B. erreicht

durch den Einsatz von virtuellen privaten Netzwerken (VPN), die Weitergabe der Daten in anonymisierter oder pseudonymisierter Form, die Verwendung einer Transport- oder Inhaltsverschlüsselung vor der Übertragung. Beim Transport von Datenträgern sind sichere Transportbehälter und zuverlässiges Transportpersonal vorzusehen.

Eingabekontrolle

Die Kontrolle der Eingabe, Veränderung und Entfernung von personenbezogenen Daten wird z. B. erreicht durch das Erstellen individueller Benutzerkennungen zusammen mit der Protokollierung aller Lese-, Schreib- und Löschvorgänge in Logdateien.

Anl. § 9 Nr. 5 BDSG

Auftragskontrolle

Die Sicherstellung der Auftragsdatenverarbeitung nach Weisung des Auftraggebers wird z. B. erreicht durch die Prüfung der Dokumentation der getroffenen Sicherheitsmaßnahmen, die Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis, die Sicherstellung der Datenvernichtung nach Auftragsbeendigung.

Anl. § 9 Nr. 6 BDSG

§ 11 II BDSG

Verfügbarkeitskontrolle

Daten müssen gegen zufällige Zerstörung oder Verlust geschützt werden, z. B. durch den Einsatz von Klimaanlagen, unterbrechungsfreier Stromversorgung, Feuer- und Rauchmeldeanlagen, die Erstellung eines Datensicherungs- und Wiederherstellungskonzepts sowie eines Notfallplans, die Aufbewahrung von Sicherungskopien an einem geschützten Ort. Nach Möglichkeit sollte redundante IT-Infrastruktur vorgehalten werden.

Anl. § 9 Nr. 7 BDSG

Datentrennung

Die Gewährleistung der getrennten Verarbeitung von zu unterschiedlichen Zwecken erhobenen Daten wird z. B. erreicht durch physikalisch getrennte Speicherung auf gesonderten Infrastrukturen oder getrennte Datenverarbeitung in mandantenfähigen Umgebungen mit strenger Rechtevergabe im Datenbankmanagementsystem.

Anl. § 9 Nr. 8 BDSG

7 Kunden und Geschäftspartner

§§ 27 ff. BDSG

Kunden und Geschäftspartner haben einen gesetzlichen Anspruch darauf, dass die Mitarbeiter der Unternehmen die maßgeblichen datenschutzrechtlichen Vorschriften kennen, beachten und anwenden. Diese befinden sich vor allem im dritten Abschnitt des Bundesdatenschutzgesetzes.

Umgang mit Kundendaten

§ 28 I BDSG

Der Umgang mit personenbezogenen Daten der Kunden ist grundsätzlich immer dann zulässig, wenn und soweit jedes einzelne Kundendatum zur Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dem Kunden im Rahmen der Erfüllung eigener Geschäftszwecke erforderlich ist. Weitere Möglichkeiten einer zulässigen Verwendung von Kundendaten ergeben sich aus dem Gesetz.

Umgang mit Daten von Geschäftspartnern

§ 28 I BDSG

Die Befugnis des Umgangs mit Kundendaten lässt sich nicht gänzlich auf den Umgang mit Daten der Geschäftspartner übertragen. Aber auch jeder weitere Gebrauch personenbezogener Daten, z. B. der Mitarbeiter der Geschäftspartner, muss von einer datenschutzrechtlichen Vorschrift gedeckt sein. Firmendaten ohne Personenbezug unterliegen nicht dem Datenschutz.

Werbung

Abhängig davon, ob Bestands- oder Neukunden beworben oder ob per Briefpost oder per E-Mail geworben werden sollen, ist eine Vielzahl von Vorschriften zu beachten.

§ 28 III BDSG

Grundsätzlich darf ein Kunde bzw. potentieller Kunde nicht ohne seine Einwilligung zum Zwecke der Werbung angesprochen werden. Die Einwilligung sollte schriftlich erfolgen und beweiskräftig dokumentiert sein. Erfolgt sie elektronisch, sollte eine zusätzliche elektronische Bestätigung zur Feststellung der Identität eingeholt werden.

§ 28 III 2 BDSG

Bei listenmäßig oder sonst zusammengefassten Daten einer Personengruppe (Name, Adresse, Titel, akademischer Grad, Anschrift, Geburtsjahr, Berufs-, Branchen- und Geschäftsbezeichnung sowie einem hinzu zu spei-

chernden Datum) ist die Nutzung und Weitergabe insbesondere für Briefwerbung auch ohne Einwilligung möglich, solange der Empfänger nicht widerspricht oder der Werbung seine schutzwürdigen Interessen entgegenstehen. Auf das Widerspruchsrecht ist der Kunde spätestens bei der Ansprache zur Werbung hinzuweisen. Widerspricht der Kunde der Verarbeitung oder Nutzung seiner Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung, ist diese unzulässig.

§ 28 III 6 BDSG

§ 28 IV 2 BDSG

§ 28 IV 1 BDSG

Werbung per E-Mail und Telefax wird grundsätzlich als „unzumutbare Belästigung" eingestuft und ist daher nur mit ausdrücklicher Einwilligung erlaubt. Eine Ausnahme besteht im Falle der E-Mail-Werbung, wenn Bestandskunden für eigene ähnliche Produkte beworben werden. Sie müssen bei Erhebung und jeder Verwendung der E-Mail-Adresse auf ihr Widerspruchsrecht hingewiesen werden und dürfen nicht schon widersprochen haben.

§ 7 II UWG

§ 7 III UWG

Werbung per Telefon gegenüber Verbrauchern ist ausschließlich zulässig bei vorheriger ausdrücklicher Einwilligung. Telefonate zu Zwecken der Markt- und Meinungsforschung dürfen nicht mit der Frage nach der Einwilligung in die Telefonwerbung verbunden werden.

§ 7 II UWG

Kundenrechte

Wenn ein Unternehmen personenbezogene Daten über potentielle Kunden ohne ihre Kenntnis, z. B. im Adresshandel, speichert, ist es in der Regel verpflichtet, den Kunden darüber zu benachrichtigen. Weitere Kundenrechte sind das Recht auf Auskunft und das Recht auf Berichtigung, Löschung und Sperrung.

§ 33 I BDSG

§ 34 BDSG

§ 35 BDSG

Bonitätsanfragen

Bonitätsanfragen zu (potentiellen) Kunden bzw. Geschäftspartnern an eine Auskunftei müssen für ein konkretes Geschäft erforderlich sein. Ihr Gegenstück, die Weitergabe von Kundendaten über eine nicht erfüllte Forderung an Auskunfteien, ist nur zulässig, soweit die geschuldete Leistung trotz Fälligkeit nicht erbracht wurde, die Übermittlung zur Wahrung berechtigter Interessen erforderlich ist und weitere im Gesetz genannte Voraussetzungen erfüllt sind.

§ 28 I BDSG

§ 28a I BDSG

8 Beschäftigtendatenschutz

§ 32 BDSG
§ 77 BetrVG

Die grundlegende gesetzliche Regelung zum Umgang mit Beschäftigtendaten findet sich im Bundesdatenschutzgesetz. Betriebsvereinbarungen sind ein wichtiges ergänzendes Instrument zur Ausgestaltung des gesetzlichen Rahmens der Beschäftigtendatenverarbeitung. Eine Einwilligung des Beschäftigten zum Umgang mit seinen Daten kann in wenigen Fällen zugrunde gelegt werden, wenn sie auf einer freien Entscheidung beruht. Die Entscheidungsfreiheit ist wegen der existenziellen Bedeutung des Arbeitsverhältnisses jedoch oft nicht gegeben. Die Einwilligung kann nur dann wirksam sein, wenn dem Mitarbeiter für den Fall der Versagung der Einwilligung keine Nachteile drohen und kein „Druck" ausgeübt wird.

§ 4a BDSG

Rechtsgrundlagen der Datenverarbeitung

§ 32 I BDSG

Die Begründung, Durchführung oder Beendigung von Beschäftigungsverhältnissen erfordert eine begrenzte Datenverwendung. Allgemein erlaubt ist die Erhebung, Verarbeitung oder Nutzung von Daten von Bewerbern oder Beschäftigten als Grundlage der Personalverwaltung und Personalwirtschaft.

§ 28 VI BDSG
§ 3 IX BDSG

Die Erhebung, Verarbeitung und Nutzung besonderer Arten personenbezogener Daten, z. B. Gesundheitsdaten, ist nur in engen Grenzen zulässig.

Erforderlichkeit der Daten

§ 32 I BDSG

Die Erforderlichkeit ergibt sich aus einer umfassenden Abwägung der legitimen Interessen des Arbeitgebers und der schutzwürdigen Interessen des Arbeitnehmers. Zulässig ist die Datenverwendung für eigene Zwecke des Arbeitgebers zur Erfüllung des konkreten Arbeitsverhältnisses. Der Zweck wird u. a. bestimmt durch den Arbeitsvertrag, Tarifregelungen und gesetzliche Anforderungen.

Vom Fragerecht des Unternehmers an einen Bewerber ausgeschlossen sind unspezifische Fragen nach strafrechtlichen Ermittlungsverfahren. Fragen nach Verurteilungen wegen Straßenverkehrsdelikten wären zulässig, wenn ein Kraftfahrer gesucht wird. Fragen nach Vermögensdelikten in Bezug auf einen Einsatz als Kassierer wären ebenfalls zulässig. Daten zum Bewerber oder Beschäftigten dürfen nur bedingt bei Dritten erhoben wer-

den. Die Erkundigung bei ehemaligen Arbeitgebern kann unter besonderen Voraussetzungen zulässig sein. Recherchen in sozialen Netzwerken sind dagegen zumeist bedenklich.

Daten können erhoben, verarbeitet und genutzt werden für Entgeltberechnungen, Leistungsbeurteilungen oder zur Feststellung von Krankheitstagen, Eingruppierungen, Umsetzungen oder im Rahmen weiterer sozialer, personeller, organisatorischer bzw. betrieblicher Maßnahmen. Ein legitimes Anliegen des Arbeitgebers kann unter Umständen eine nach Ankündigung erfolgte stichprobenartige Leistungskontrolle zur Qualitätssicherung sein. Nicht vom Verarbeitungszweck erfasst sind in der Regel telefonische Auskünfte zu Personaldaten an Verwandte, Freunde und Bekannte oder die Nutzung der Privatanschrift des Mitarbeiters für Werbung.

Veröffentlichung von Mitarbeiterdaten

Vor der Veröffentlichung von Mitarbeiterdaten im Internet sollte der Betroffene die Möglichkeit erhalten, persönliche Belange dagegen vorzutragen. Denn die Konsequenzen einer weltweiten Veröffentlichung sind für den Einzelnen nicht immer absehbar. Grundsätzlich gilt, dass Daten von Mitarbeitern der Leitungsebene und von Mitarbeitern mit Außenkontakten im dafür erforderlichen Maße veröffentlicht werden dürfen. Diese Daten umfassen in der Regel den Namen, die Funktion sowie betriebliche Telefonnummer und E-Mail-Adresse. Persönliche Daten wie z. B. der berufliche Werdegang und insbesondere Fotos dürfen dagegen grundsätzlich nur mit Einwilligung des Betroffenen veröffentlicht werden. Bei Fotos gilt das Recht am eigenen Bild.

§ 22 KunstUrhG

Ermittlungen

Ermittlungstätigkeiten des Arbeitgebers sind nur begrenzt zulässig. Die Erhebung bzw. Verarbeitung von Beschäftigtendaten ist möglich, wenn der Beschäftigte aufgrund zu dokumentierender tatsächlicher Anhaltspunkte einer Straftat im Beschäftigungsverhältnis verdächtig ist. Das Vorgehen des Arbeitgebers muss insgesamt verhältnismäßig sein. Dies gilt insbesondere für präventive Kontrollvorhaben, die mit betroffenen Persönlichkeitsrechten abzuwägen sind.

§ 32 I 2 BDSG

Mitarbeiterüberwachung

Eine permanente Überwachung ist grundsätzlich verboten.

§ 6b BDSG

§ 28 BDSG

§ 32 BDSG

Eine Videoüberwachung der Mitarbeiter in öffentlich zugänglichen Räumen kann in engen Grenzen zulässig sein. Ebenfalls in sehr engen Grenzen kann eine Beobachtung in nicht öffentlich zugänglichen Räumen möglich sein. Unter Berücksichtigung des Verhältnismäßigkeitsprinzips (Überwachungsdruck, Intensität der Beobachtung) sind in Einzelfällen überwiegende Arbeitgeberinteressen (Sicherheit, Arbeitsorganisation) denkbar, wenn weniger einschneidende Maßnahmen nicht in Betracht kommen. Eine Beobachtung ist kenntlich zu machen.

Ob und vor allem inwieweit eine Lokalisierung von externen Mitarbeitern durch Ortung von Handys oder mittels GPS in Fahrzeugen zulässig ist, hängt vom Arbeitsvertrag, den konkreten Arbeitsbedingungen, besonderen Anforderungen (Fahrzeiten und Anwesenheitszeiten für Abrechnungen, Transportplanung usw.) und hinreichender Einschränkung zum Schutz der Mitarbeiter (keine Erfassung von Privatem, keine Rundumkontrolle, nur zeitweise Einschaltung usw.) ab. Eine heimliche Ortung ist unzulässig.

§ 31 BDSG

Protokolldaten der Internet- und E-Mail-Nutzung sowie der Anmeldung im Netzwerk oder der Arbeit im Dokumentenmanagementsystem dürfen nicht zur Verhaltens- oder Leistungsüberwachung der Mitarbeiter verwendet werden. Allerdings ist bei tatsächlich vorliegenden Anhaltspunkten für einen Verstoß gegen die Nutzungsgrundsätze eine Kontrolle im Einzelfall möglich.

9 Videoüberwachung

Die Beobachtung öffentlich zugänglicher Räume mit Videotechnik ist nur unter bestimmten Bedingungen erlaubt, damit es nicht zu einer Verletzung des Persönlichkeitsrechts des Einzelnen durch eine ständige Beobachtung kommt. Dabei ist es zunächst unerheblich, ob dabei eine Aufzeichnung erfolgt. *§ 6b BDSG*

Der öffentlich zugängliche Raum

Unter öffentlich zugänglichen Räumen sind nicht nur öffentliche Gebäude, Plätze und Straßen zu verstehen, sondern auch Teile von Privatgrundstücken und -gebäuden, die dafür vorgesehen sind, von beliebigen Personen betreten zu werden, wie z. B. Geschäfte, Banken, Tankstellen, Parkhäuser, Hotels, Restaurants, Wartezimmer usw. Dabei ist es unerheblich, ob die Person ein Entgelt zum Betreten zu entrichten hat, z. B. als Gast im Kino. Zu beachten ist, dass Wege, die zu einer Klingel oder einem Briefkasten führen, in der Regel als öffentlich zugängliche Räume anzusehen sind. Alle anderen Bereiche eines als solchen erkennbaren Privatgrundstücks oder Firmengeländes, insbesondere Räume hinter geschlossenen Türen, wie z. B. Produktionsstätten, sind keine öffentlich zugänglichen Räume.

Zweck, Verhältnismäßigkeit, Kennzeichnung

Eine Videoüberwachung öffentlich zugänglicher Räume ist nur zur Geltendmachung des Hausrechts oder für konkret festgelegte Zwecke zur Wahrnehmung eines berechtigten Interesses zulässig, z. B. zum Beweis von Sachbeschädigung oder Diebstahl. Das berechtigte Interesse muss dabei belegbar sein, z. B. durch Nachweis wiederholter Schädigungen. Eine Beobachtung ist nur zulässig, wenn keine milderen Mittel das Schutzziel gewährleisten können. Bei der Einrichtung einer Videoüberwachung ist zudem das Interesse des Betroffenen am Schutz der Privatsphäre gegenüber den verfolgten Zwecken des Beobachters abzuwägen. Bei zulässiger Videoüberwachung hat eine geeignete Kennzeichnung, z. B. durch Hinweisschilder, unter Benennung der verantwortlichen Stelle zu erfolgen. Aufgezeichnete Videosignale sind umgehend zu löschen, wenn sich keine Erkenntnisse aus den Aufzeichnungen für die verfolgten Zwecke ergeben. Die Beobachtung eines höchstpersönlichen Bereiches wie Umkleidekabinen oder Toiletten ist generell untersagt.

§ 6b I Nr. 2 BDSG
§ 6b I Nr. 3 BDSG
§ 6b III BDSG
§ 6b II BDSG
§ 6b V BDSG
§ 201a StGB

10 Das Unternehmen im Internet

Die Unternehmenswebseite

Viele Unternehmen präsentieren sich mit einer eigenen Webseite im Internet. Unabhängig davon, ob nur das Unternehmen beworben wird oder direkt Waren oder Dienstleistungen über das Internet angeboten werden, sind verschiedene rechtliche Vorgaben zu beachten.

§ 5 I TMG

Das auch als Anbieterkennzeichnung bezeichnete *Impressum* dient dazu, den Nutzer der Webseite über den Anbieter der Webseite zu informieren. Dazu sind unter anderem Name und Anschrift des Unternehmens, bei juristischen Personen zusätzlich die Umsatzsteueridentifikationsnummer, die Rechtsform und der Vertretungsberechtigte zu nennen. Auch Angaben, die eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation ermöglichen, einschließlich der Adresse der elektronischen Post, gehören dazu und sind leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten.

§ 13 I TMG

Immer dann, wenn über den Internetauftritt personenbezogene Daten erhoben werden, ist eine *Datenschutzerklärung* erforderlich. Diese muss den Nutzer genau darüber informieren, welche personenbezogenen Daten zu welchem Zweck gespeichert oder verwendet werden. Werden Cookies verwendet, die eine spätere Identifizierung ermöglichen, ist der Nutzer ebenfalls zu unterrichten. Der Inhalt der Unterrichtung muss jederzeit abrufbar sein. Personenbezogene Daten dürfen nur dann erhoben und verwendet werden, wenn dies entweder durch Gesetz ausdrücklich erlaubt ist oder der Nutzer eingewilligt hat.

§ 12 I TMG

Vor der Verwendung *externer Links*, die auf fremde Internetangebote verweisen, sollten diese genau auf strafrechtlich relevante Inhalte geprüft und die Prüfung in regelmäßigen Abständen wiederholt werden. Außerdem sind externe Links entsprechend zu kennzeichnen, damit der Nutzer die Weiterleitung zu einem anderen Diensteanbieter erkennen kann.

§ 13 V TMG

Soziale Netzwerke

Soll das Unternehmen in sozialen Netzwerken präsentiert werden, um breitere Kundenkreise zu erreichen, ist jedoch auch hier zu beachten, dass die gesetzlichen Regelungen des Telemediengesetzes und des Bundesdatenschutzgesetzes eingehalten werden müssen. Das ist insbesondere bei den großen sozialen Netzwerken mit Sitz außerhalb Europas nicht immer möglich.

Sogenannte Social Plugins wie der *Gefällt-mir*-Button von Facebook, der *g+1*-Button von Google+ oder der *Tweet*-Button von Twitter sollten nicht direkt in die Unternehmenswebseite eingebunden werden, da hierbei Nutzerdaten auch dann an Facebook, Google und Twitter übermittelt werden, wenn der Nutzer den Button gar nicht anklickt. Deshalb wird empfohlen, eine 2-Klick-Lösung einzusetzen, bei der zunächst deaktivierte Buttons auf der Webseite eingebunden werden, die keinen Kontakt mit den Servern sozialer Netzwerke, wie Facebook und Google+, herstellen. Erst wenn der Nutzer diese aktiviert und damit seine Zustimmung erklärt, werden die Buttons aktiv und stellen die Verbindung her.

Eine weitere Möglichkeit ist die Einbindung eigener, individuell gestalteter Buttons, bei denen die Kommunikation mit den sozialen Netzwerken ein auf dem Server des Webseitenbetreibers abgelegtes Skript übernimmt. Erst wenn der Nutzer einen Button betätigt, entsteht eine direkte Verbindung und Nutzerdaten werden übertragen.

E-Mail und Internet am Arbeitsplatz

Es ist auf jeden Fall zu empfehlen, die Nutzung von Internet und E-Mail am Arbeitsplatz intern, z. B. durch eine Betriebsvereinbarung, zu regeln. Dabei sollten die Grundsätze der Nutzung festgelegt werden, vor allem ob die Nutzung nur zu rein betrieblichen oder auch für private Zwecke zulässig ist. Erfahrungsgemäß werden u. a. aus Gründen der Datensicherheit solche Nutzungen protokolliert. Bei erlaubter privater Nutzung ist sowohl für die damit verbundene Protokollierung als auch für die Einsichtnahme des Arbeitgebers in das E-Mail-Postfach eine schriftliche Einwilligung von den Mitarbeitern einzuholen.

§ 4a BDSG

A Auswahl datenschutzrelevanter Vorschriften

§§ 201-203 StGB Das Strafgesetzbuch stellt u. a. die Verletzung der Vertraulichkeit und das Ausspähen von Daten sowie die Missachtung der Wahrung von Geheimnissen unter Strafe.

§ 305 BGB Im Bürgerlichen Gesetzbuch wird u. a. die Ausgestaltung allgemeiner Geschäftsbedingungen geregelt.

§ 35 SGB I Im Sozialgesetzbuch wird u. a. geregelt, dass jedermann einen Anspruch auf Wahrung des Sozialgeheimnisses hat.

§ 77 BetrVG Das Betriebsverfassungsgesetz benennt die Betriebsvereinbarungen als vertragliche Regelungen zwischen Unternehmen und Betriebsrat mit normativem Charakter.

§ 7 UWG Im Gesetz gegen den unlauteren Wettbewerb wird Werbung per E-Mail und Telefon in der Regel als unzumutbare Belästigung verboten.

§ 13 TMG Das Telemediengesetz regelt u. a. die Einwilligung und das Widerrufsrecht der Datenerfassung bei der Nutzung von Telemediendiensten.

§ 88 TKG Das Telekommunikationsgesetz regelt die Wahrung des Fernmeldegeheimnisses bei der Telekommunikation.

§ 22 KunstUrhG Das Kunsturhebergesetz regelt die Verbreitung und Veröffentlichung von Bildnissen der eigenen Person.

Weitere relevante Gesetze, die Regelungen zum Datenschutz enthalten, sind die Abgabenordnung (AO), das Genossenschaftsgesetz (GenG), das Handelsgesetzbuch (HGB), das Personalausweisgesetz (PAuswG), die Sozialgesetzbücher (insbesondere I und X) sowie das Versicherungsvertragsgesetz (VVG) u. v. m.

B Informationsquellen

Internetseiten

Der Landesbeauftragte für den Datenschutz Sachsen-Anhalt:
http://www.datenschutz.sachsen-anhalt.de

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit:
http://www.bfdi.bund.de

Virtuelles Datenschutzbüro der Datenschutzbeauftragten des Bundes und der Länder: http://www.datenschutz.de

Bundesamt für Sicherheit in der Informationstechnik:
https://www.bsi.bund.de

Themensammlung der Zeitschrift für Datenschutz:
http://rsw.beck.de/CMS/?toc=ZD.120

Arbeitskammer des Saarlandes – Datenschutz im Betrieb:
http://www.arbeitskammer.de/publikationen/online-broschueren/datenschutz-im-betrieb-stand-82012.html

Broschüren der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit – BfDI*

BfDI-Info 1: *Bundesdatenschutzgesetz – Text und Erläuterung,* 2014.

BfDI-Faltblatt: *Datenschutz – meine Rechte,* 2014.

BfDI-Info 4: *Die Datenschutzbeauftragten in Behörde und Betrieb,* 2011.

BfDI-Info 5: *Datenschutz und Telekommunikation,* 2013.

BfDI: *Adresshandel und unerwünschte Werbung*.

BfDI-Faltblatt: *Surfen Am Arbeitsplatz – Datenschutz-Wegweiser,* 2013.

* auch online verfügbar

Orientierungshilfe der Datenschutzbeauftragten des Bundes und der Länder zur Videoüberwachung

http://lsaurl.de/videooh

Eigene Notizen

Die Beiträge dieser Broschüre sind sorgfältig recherchiert und entsprechen dem aktuellen Stand. Abweichungen durch seit Drucklegung geänderte Gesetze sind nicht auszuschließen.

Impressum

Herausgeber:
Der Landesbeauftragte für den Datenschutz Sachsen-Anhalt

Leiterstr. 9, 39104 Magdeburg
PF 1947, 39009 Magdeburg

Tel. (0391) 81803-0
Fax (0391) 81803-33

www.datenschutz.sachsen-anhalt.de
poststelle@lfd.sachsen-anhalt.de

Druck: Der Landtag von Sachsen-Anhalt
PDF-Version: http://lsaurl.de/chefsache

Diese Handreichung ist eine Orientierungshilfe für Unternehmen bei der Umsetzung von Datenschutz und Datensicherheit sowie ein Leitfaden zur Selbstüberprüfung.

www.datenschutz.sachsen-anhalt.de
poststelle@lfd.sachsen-anhalt.de