STIFTUNG DATENSCHUTZ

BESCHÄFTIGTEN DATENSCHUTZ

EINE HANDREICHUNG

THEMEN

VORWORT

LIEBE LESERINNEN, LIEBE LESER,

Seit Mai 2018 ist die EU-Datenschutz-Grundverordnung verbindlich anzuwenden. Seither nehmen viele Organisationen, Einrichtungen, Privatpersonen und Unternehmen den Schutz personenbezogener Daten viel wichtiger als vorher.

Eine Vielzahl von personenbezogenen Daten über Beschäftigte und BewerberInnen fällt in den Personalabteilungen der Unternehmen an. Diese Daten sind oft besonders sensibel, betreffen sie doch meist auch die Privatsphäre der Menschen: Familienverhältnisse, Erkrankungen, und überhaupt Informationen, die manche nicht gern mit Vorgesetzten und ArbeitskollegInnen teilen möchten. Dazu kommt, dass Beschäftigungsverhältnisse für die Einzelnen besonders wichtig sind, weil sie die wirtschaftliche Existenz sichern. Daher sind Beschäftigungsverhältnisse auch im Rahmen des Arbeitsrechts besonders geschützt.

Umso verwunderlicher ist es, dass es noch kein spezielles Recht für den Beschäftigtendatenschutz gibt, obwohl dies schon seit vielen Jahren von DatenschutzexpterInnen, Personalprofis, Betriebsräten und anderen gefordert wird. Dies hat sich auch mit der EU-Datenschutz-Grundverordnung nicht geändert.

Die vorliegende Handreichung trägt die wichtigsten Grundsätze und Regeln zusammen, die für den Datenschutz in Beschäftigungsverhältnissen gelten. Sie wendet sich vor allem an Personalverantwortliche in kleinen und mittelständischen Unternehmen, aber auch an Betriebsräte und ganz allgemein an Beschäftigte. Ihr Ziel ist es, Leitlinien für den praktischen Unternehmensalltag zu vermitteln. Dabei ersetzt diese Handreichung natürlich nicht den Austausch mit dem/der Datenschutzbeauftragen, oder – in komplizierteren Fällen – mit einer spezialisierten Rechtsanwaltskanzlei. Wir haben uns um eine klare und verständliche Sprache bemüht.

Eine ausführlichere Version mit vielen Links zu den Veröffentlichungen der Aufsichtsbehörden finden Sie auf unserer Infoplattform und unter diesem Link: https://sds-links.de/Dossier-BS-DS

Wenn Sie Verbesserungsvorschläge haben, schreiben Sie uns: mail@stiftungdatenschutz.org

Und schließlich möchten wir Sie noch auf unsere allgemeine Handreichung zum „Datenschutz im Betrieb“ hinweisen, die Sie auf unserer Website finden.

Freundliche Grüße von

Frederick Richter
Vorstand der Stiftung Datenschutz

GRUNDSÄTZLICHES

WELCHE GESETZE REGELN DEN DATENSCHUTZ FÜR BESCHÄFTIGTE?

Die EU-Datenschutz-Grundverordnung (DSGVO) ist seit Mai 2018 in allen EU-Ländern verbindlich anzuwenden und regelt wesentliche Punkte der Verarbeitung personenbezogener Daten. Dazu gehören

- die Pflichten der Unternehmen, Einrichtungen und Organisationen, welche die Daten verarbeiten („verantwortliche Stellen"),
- die Rechte der Personen, deren Daten verarbeitet werden (die „Betroffenen"),
- die Benennung von Datenschutzbeauftragten und –aufsichtsbehörden,
- die Übermittlung von Daten an Dritte und in Drittländer,
- das Vorgehen und die Sanktionen bei Datenschutzverstößen und viele andere Aspekte.

Die DSGVO ermöglicht es den EU-Mitgliedsländern, bestimmte allgemeine Vorschriften an ihre speziellen Bedürfnisse anzupassen. Eine solche sogenannte Öffnungsklausel gibt es auch für den Beschäftigtendatenschutz. Deutschland hat das Bundesdatenschutzgesetz (BDSG) an die DSGVO angepasst und dabei die „alte" Regelung in den § 26 BDSG übernommen[1]. Ein eigenes Gesetz, das den Schutz der personenbezogenen Daten in Beschäftigungsverhältnissen umfassend regelt, gibt es bislang nicht.

Neben der Datenschutz-Grundverordnung und dem Bundesdatenschutzgesetz enthalten zahlreiche andere gesetzliche Regelungen Vorschriften für den Datenschutz. So ist die Verschwiegenheitspflicht von medizinischem Personal im Strafgesetzbuch, der Umgang mit Briefen im Postgesetz und der Umgang mit Gesundheitsdaten bei Versicherungen im Sozialgesetzbuch V geregelt.

FÜR WEN GELTEN DIE REGELUNGEN DES § 26 BDSG?

Das Gesetz gilt für „Beschäftigte". Das bedeutet im Sinne des Datenschutzes:

- Arbeitnehmerinnen und Arbeitnehmer
- Leiharbeitnehmerinnen und Leiharbeitnehmer (im Verhältnis zum entleihenden Unternehmen)
- Auszubildende
- TeilnehmerInnen an Leistungen zur Teilhabe am Arbeitsleben sowie RehabilitandInnen
- Menschen, die in anerkannten Werkstätten für behinderte Menschen beschäftigt sind,
- Freiwillige nach dem Jugendfreiwilligendienstgesetz oder dem Bundesfreiwilligendienstgesetz
- arbeitnehmerähnliche Personen (z. B. in Heimarbeit Beschäftigte)
- BewerberInnen für ein Beschäftigungsverhältnis
- Personen, deren Beschäftigungsverhältnis beendet ist
- Beamtinnen und Beamte des Bundes, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende (sofern nicht bundes- und landesspezifische Regelungen gelten).

In Kürze: Das Bundesdatenschutzgesetz und die DSGVO gelten für alle Beschäftigungsverhältnisse, einschließlich Leiharbeits- und Ausbildungsverhältnisse; für BewerberInnen und ehemals Beschäftigte. Für Bedienstete und Beschäftigte bei Behörden und öffentlichen Stellen des Bundes, der Länder und der Kommunen, gelten besondere (u.a. beamtenrechtliche) bundes- und landesspezifische Regelungen.

WAS SIND ÜBERHAUPT PERSONENBEZOGENE DATEN?

Personenbezogene Daten sind alle Informationen über eine natürliche Person, die sich der Person unmittelbar oder mittelbar zuordnen lassen.

- Unmittelbar zuzuordnen ist der Person ihr Name.
- Unmittelbar der Person zuzuordnen kann auch ihre Funktion sein, wenn es zum Beispiel nur eine IT-Leiterin im Unternehmen gibt.

1 https://sds-links.de/v78

- Mittelbar zuzuordnen ist der Person ihre Personalnummer: Zwar weist die Personalnummer an sich noch nicht auf die konkrete Person hin, der Personenbezug kann jedoch hergestellt werden, wenn bekannt ist, welcher Name zu welcher Personalnummer gehört.
- Mittelbar kann unter bestimmten Umständen auch eine IP-Adresse einer Person zugeordnet werden.

Diese Beispiele zeigen, dass vor allem beim mittelbaren Personenbezug der Zusammenhang betrachtet werden muss, wenn es darum geht zu entscheiden, ob es sich um personenbezogene Daten handelt.

Personenbezogene Daten können auch bloße Annahmen und Vermutungen sein. Wenn eine Auskunftei die Kreditwürdigkeit einer Person mit Hilfe eines Score-Wertes berechnet, ist dieser Wert eine Annahme über die Zahlungsfähigkeit oder -bereitschaft des Kunden bzw. über die Ausfallwahrscheinlichkeit des Kredits in der Zukunft. Auch solche Einschätzungen gehören zu den personenbezogenen Daten.

Darüber hinaus gibt es sogenannte **„besondere Kategorien personenbezogener Daten“** (Artikel 9 Absatz 1 DSGVO). Das sind Daten, die besonders sensibel und daher schutzwürdig sind, weil aus ihnen die ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder eine Gewerkschaftszugehörigkeit hervorgehen, sowie genetische und biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben oder der geschlechtlichen Orientierung einer natürlichen Person. Für deren Verarbeitung gibt es besondere Vorschriften.

GILT DIE DSGVO NICHT NUR FÜR DIE AUTOMATISIERTE DATENVERARBEITUNG?

Die Datenschutz-Grundverordnung gilt für alle Formen der Verarbeitung personenbezogener Daten gleichermaßen, ob sie teilweise oder ganz automatisiert oder auch gar nicht automatisiert ist.

§26 Abs.7 BDSG schreibt ergänzend vor, dass die DSGVO (im Beschäftigtendatenschutz) auch auf nicht-strukturierte personenbezogene Daten anzuwenden ist, zum Beispiel handschriftliche Notizen.

Unter „Verarbeitung“ werden alle vorstellbaren Handlungsformen verstanden, tatsächliche Handlungen wie das Erheben und Speichern ebenso wie Beobachtungen, mündliche Äußerungen oder handschriftliche Notizen über Beschäftigte.

DAS PRINZIP DER ZWECKBINDUNG

Das Prinzip der Zweckbindung[2] verlangt, dass Beschäftigtendaten nur für festgelegte, eindeutige und legitime Zwecke erhoben und verarbeitet werden dürfen. Dies muss der Arbeitgeber nachweisen können[3]. In Betriebsvereinbarungen müssen dazu Regelungen getroffen werden, die möglichst konkret, klar und abschließend die Zwecke der Datenverarbeitung festlegen. Allgemeine Beschreibungen sind zu vermeiden.

Beispiel

- Zu allgemein: „Die Datenverarbeitung dient der Urlaubsplanung“
- Ausreichend konkret: „Die Unternehmenssoftware ‚HappyHolidays‘ dient der Erfassung und Prüfung der Urlaubsanträge der Beschäftigten auf Basis ihres Urlaubsanspruchs.“

DIE ROLLE DES BETRIEBSRATS

Dem Betriebsrat werden im Zuge seiner Tätigkeit eine Reihen von personenbezogenen Daten, auch solche aus den besonders geschützten Kategorien, bekannt. Ob der Betriebsrat damit zu eine verantwortlichen Stelle im Sinne von Artikel 4 Nr. 7 DSGVO ist oder ob er – wie unter bisherigem Recht – Teil der verantwortlichen Stelle, also des Unternehmens, bleibt, ist derzeit noch umstritten. Damit ist auch offen, ob er der Kontrolle durch den betrieblichen Datenschutzbeauftragten sowie der Aufsichtsbehörden unterliegt.

Unbestritten ist jedoch, dass der Betriebsrat bei seiner Tätigkeit die üblichen gesetzlichen Regelungen befolgen muss. Bei der Erarbeitung von Betriebsvereinbarungen ist zu beachten, dass deren Schutzniveau nicht unter das der DSGVO fallen darf.

2 https://sds-links.de/jy7 (Artikel 5 Abs.1 Buchstabe b) DSGVO)
3 https://sds-links.de/jy7 (Artikel 5 Abs.2 DSGVO)

WANN IST DIE DATENVERARBEITUNG ZULÄSSIG?

Die DSGVO und das BDSG sind Verbotsgesetze mit Erlaubnisvorbehalt. Das bedeutet, dass jede Verarbeitung personenbezogener Daten zunächst unzulässig ist; es sei denn, es gibt einen sogenannten „Erlaubnisgrund", der die Datenverarbeitung erlaubt. Die wichtigsten Erlaubnisgründe sollen hier kurz dargestellt werden.

DIE DATENVERARBEITUNG IST ERFORDERLICH.

Personenbezogene Daten über Beschäftigte dürfen verarbeitet werden, sofern dies erforderlich ist, um das Arbeitsverhältnis zu begründen, durchzuführen und zu beenden. Weiterhin kann die Datenverarbeitung erforderlich sein, um Pflichten zu erfüllen und/oder Rechte auszuüben, die sich aus Gesetzen, Tarifverträgen und Betriebs- oder Dienstvereinbarungen ergeben. Dabei bedeutet das Merkmal der Erforderlichkeit, dass mit der Datenverarbeitung ein legitimer Zweck verfolgt wird, und dass dieser Zweck ohne Datenverarbeitung nicht erreicht werden kann. Auch besonders sensible Daten dürfen verarbeitet werden, wenn dies erforderlich ist.

Beispiel
Durchführung des Arbeitsverhältnisses

In der Personalakte wird die Religionszugehörigkeit (= personenbezogenes Datum) gespeichert (= verarbeitet), weil der Arbeitgeber per Gesetz verpflichtet ist, im Rahmen der Gehaltszahlungen die Kirchensteuer an das Finanzamt abzuführen (= legitimer Zweck). Dies wäre ohne die Verarbeitung des Datums „Religionszugehörigkeit" nicht möglich. Daher ist die Datenverarbeitung erforderlich und damit zulässig.

Beispiel
Daten, die bei der Computernutzung anfallen

Es wird gespeichert, wer sich wann an einem Computersystem anmeldet. Die Anmeldenamen sind im Zusammenhang mit dem Passwort als personenbezogene Daten zu betrachten. Die Datenverarbeitung kann aus Sicherheitsgründen oder zur Dokumentation erforderlich sein (legitimer Zweck). Das Protokollieren aller Tastatureingaben wäre jedoch nicht zulässig, weil damit kein legitimer Zweck verfolgt werden kann; damit fehlt die Erforderlichkeit.

Für die Feststellung der Erforderlichkeit zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes muss stets eine Interessenabwägung stattfinden. Dabei wird das Interesse des Arbeitsgebers an der Datenverarbeitung dem schutzwürdigen Interesse der Beschäftigten gegenüber gestellt, die Daten nicht zu verarbeiten. Die Verarbeitung ist nur dann zulässig, wenn kein Grund zu der Annahme besteht, dass das Interesse der Beschäftigten an dem Ausschluss der Verarbeitung überwiegt. Dies gilt auch für die Verarbeitung besonders sensibler Daten.

ES LIEGT EINE EINWILLIGUNG VOR.

Die Datenschutz-Grundverordnung regelt, dass die Einwilligung einer betroffenen Person (also derjenigen Menschen, deren personenbezogene Daten verarbeitet werden sollen) die Verarbeitung erlaubt, wenn keine anderen Gründe dagegen sprechen. (Andere Erlaubnisgründe sind zum Beispiel die Erforderlichkeit zur Vertragsdurchführung oder das Vorliegen von entsprechenden gesetzlichen Vorschriften, siehe oben.) Diese Einwilligung muss immer informiert und freiwillig erfolgen, d.h. die betroffene Person muss wissen, welche Daten in welchem Umfang von wem zu welchem Zweck verarbeitet werden, und es darf ihr kein Nachteil aus einer Ablehnung entstehen.

Diese Aspekte machen es schwierig, in Beschäftigungsverhältnissen mit einer wirksamen Einwilligung zu arbeiten, denn für die allermeisten Menschen ist das Beschäftigungsverhältnis die Grundlage ihrer wirtschaftlichen Existenz. Daher, und wegen der bestehenden Weisungsrechte, bestehen fast immer so unterschiedliche Machtverhältnisse, dass die Freiwilligkeit einer Einwilligung schwer nachzuweisen ist.

Beispiel

In der Bäckerei Hermann treten immer wieder Kassenfehlbeträge auf. Hermann möchte daher die Bäckereifachverkäuferinnen bei ihrer Arbeit per Video

überwachen, und bittet diese um ihre Einwilligung. Silke Streusel ist noch in der Probezeit und fürchtet, entlassen zu werden, wenn sie nicht einwilligt.

Das bedeutet jedoch nicht, dass die Datenverarbeitung auf der Grundlage einer Einwilligung im Beschäftigungsverhältnis ausgeschlossen ist. Von einer freiwilligen Einwilligung kann ausgegangen werden, wenn für die Beschäftigten durch die Datenverarbeitung ein rechtlicher oder wirtschaftlicher Vorteil entsteht, oder wenn Arbeitgeber und Beschäftigte übereinstimmende Interessen verfolgen.

Auch die Verarbeitung besonders sensibler personenbezogener Daten ist mit einer Einwilligung möglich, wenn sich die Einwilligung ausdrücklich auf diese Daten bezieht

Beispiel

Der Installateurbetrieb Warmwasser stattet seine Installateure mit Mobiltelefonen aus, damit sie währen der Arbeit beim Kunden erreichbar sind, und gestattet die uneingeschränkte private Nutzung. Die Beschäftigten benötigen kein privates Mobiltelefon, dadurch entsteht ihnen ein wirtschaftlicher Vorteil. Daher ist davon auszugehen, dass ihre Einwilligung in die Datenverarbeitung, die ihre private Telefonnutzung betrifft, wirksam erteilt werden kann.

Die Einwilligung im Arbeitsverhältnis muss grundsätzlich schriftlich erteilt werden. Damit die Einwilligung auch „informiert“ ist, müssen Beschäftigte über Zweck und Umfang der Datenverarbeitung in Kenntnis gesetzt werden; ebenso darüber, dass die Einwilligung jederzeit widerrufen werden kann. Der Widerruf macht die Datenverarbeitung aber nicht rückwirkend unzulässig, sondern nur für die Zukunft.

ES SOLLEN STRAFTATEN AUFGEDECKT WERDEN.

Beschäftigtendaten dürfen verarbeitet werden, wenn dadurch bereits begangene Straftaten aufgedeckt werden sollen. Dazu muss ein begründeter Verdacht gegen bestimmte Beschäftigte dokumentiert sein.

Eine vorsorgliche Datenverarbeitung zur Verhinderung von Straftaten oder zur Aufdeckung von Ordnungswidrigkeiten ist nicht zulässig.

Nicht gesetzlich geregelt ist, ob eine Datenverarbeitung bei Verdacht auf eine schwerwiegende Pflichtverletzung, die keine Straftat darstellt, in Betracht kommen kann, wie unerlaubte Konkurrenztätigkeit oder das Vortäuschen von Arbeitsunfähigkeit, wenn die Umstände des Einzelfalls berücksichtigt sind. Im Einzelfall kann auch die Beauftragung einer Detektei gerechtfertigt sein.

Auf jeden Fall muss an die Zulässigkeit von Überwachungsmaßnahmen zur Aufdeckung schwerer Pflichtverletzungen strenge Maßstäbe angelegt werden.

UND DIE „BERECHTIGTEN INTERESSEN“?

Wie die Erforderlichkeit und die Einwilligung sind auch die sogenannten „berechtigten Interessen“ nach der DSGVO ein Erlaubnisgrund für die Datenverarbeitung. Ob „berechtigte Interessen“ auch im Rahmen von Beschäftigungsverhältnissen die Datenverarbeitung erlauben, ist im Moment noch umstritten. Daher empfehlen wir, auf die berechtigten Interessen als Erlaubnisgrund zu verzichten, zumal der Arbeitgeber verpflichtet ist, im Streitfall die Rechtmäßigkeit der Datenverarbeitung nachzuweisen.

BELEHRUNGS- UND INFORMATIONSPFLICHTEN

Die Verarbeitung von personenbezogenen Daten im Beschäftigungsverhältnis erfordert vom Arbeitgeber, das die Beschäftigten über die Datenverarbeitung belehrt und informiert werden. Zu Dokumentationszwecken empfehlen wir, dies stets schriftlich zu tun oder zumindest eine schriftliche Bestätigung über die mündliche Belehrung einzuholen.

VERPFLICHTUNG AUF DAS DATENGEHEIMNIS

Beschäftigte, die personenbezogene Daten verarbeiten, sollten auf das Datengeheimnis verpflichtet werden. Das ist zwar in der DSGVO nicht ausdrücklich vorgesehen, aber der Arbeitgeber muss die Rechtmäßigkeit der Datenverarbeitung nachweisen. Ein Muster bietet die bayrische Aufsichtsbehörde auf ihrer Website an[4]; mehr zu allgemeinen Grundsätzen der Datenverarbeitung findet sich in der Broschüre der Stiftung Datenschutz „Datenschutz im Betrieb“.[5]

INFORMATIONSPFLICHTEN GEGENÜBER DEN BESCHÄFTIGTEN

Die DSGVO regelt, dass von der Datenverarbeitung betroffene Personen eine Reihe von Rechten gegenüber der verantwortlichen Stelle ausüben können. Dies gilt auch im Beschäftigtenverhältnis.

Zu den Betroffenenrechten zählen unter anderem der Anspruch auf Information darüber, welche Daten zu welchem Zweck verarbeitet werden und wer – im Falle einer Datenweitergabe – Empfänger dieser Daten ist.

Beispiel
Lohnbuchhaltung: Informationspflichtige Angaben

- Verarbeitete Daten: Name, Anschrift, Bankverbindung, Geburtsdatum, Steuerklasse, Zeugnisse, aber auch Arbeitszeiten, Gehaltsdaten, Kranken- oder Urlaubszeiten
- Verarbeitungszwecke: Lohnbuchhaltung, Entgeltauszahlung,
- Erlaubnisgrund: Erforderlichkeit zur Durchführung des Arbeitsverhältnisses
- Empfänger der Datenweitergabe: Krankenversicherung, sonstige Sozialversicherungsträger, Finanzämter

4 https://sds-links.de/dg4
5 https://sds-links.de/infomaterial

ANWENDUNGEN IN DER BETRIEBLICHEN PRAXIS

HEIMLICHE VIDEOÜBERWACHUNG

Eine heimliche Überwachung ist ein schwerer Eingriff in das allgemeine Persönlichkeitsrecht der Beschäftigten. Aber auch der Arbeitgeber kann sich auf grundrechtlich geschützte Positionen berufen (Eigentumsrecht und Berufsausübungsfreiheit). Derzeit ist umstritten, ob eine heimliche Videoüberwachung unter der Datenschutz-Grundverordnung zulässig ist. Argumente, welche dagegen sprechen, sind das in der DSGVO verankerte Transparenzgebot sowie die fehlende gesetzliche Legitimationsgrundlage, da die heimliche Videoüberwachung im BDSG nicht ausdrücklich genannt wird.

Im Zuge der Interessenabwägung ist nach der bisherigen Rechtsprechung des Bundesarbeitsgerichts eine heimliche Videoüberwachung nur im absoluten Ausnahmefall als letztes Mittel zulässig, wenn ein konkreter Verdacht einer strafbaren Handlung oder einer anderen schwerwiegenden Verfehlung besteht. Durch eine unzulässige Videoüberwachung gewonnene Beweise dürfen nicht gerichtlich verwertet werden.

OFFENE VIDEOÜBERWACHUNG

Nach der Rechtsprechung des Bundesarbeitsgerichts ist auch eine *offene* Videoüberwachung nur in Ausnahmefällen zulässig. Mitentscheidend ist insbesondere die Intensität des Eingriffs für die Beschäftigten, die von den Bildaufnahmen erfasst sind, und ob die Maßnahme erforderlich ist oder der Zweck auch im Wege einer weniger einschneidenden Maßnahme erreicht werden kann. Zu prüfen ist, ob die Beschäftigten einem ständigen Überwachungsdruck ausgesetzt sind und damit in schwerwiegender Weise in das allgemeine Persönlichkeitsrecht eingegriffen wird und dadurch auch ein Anpassungsdruck erzeugt werden kann.

Die Intimsphäre muss unter allen Umständen unangetastet bleiben. In Umkleidekabinen oder Sanitärbereichen ist Videoüberwachung grundsätzlich unzulässig. Abgeschlossene Schränke oder Schubladen gehören zwar nicht zur Intimsphäre, dürfen jedoch allenfalls im Beisein der Beschäftigten bzw. gegebenenfalls im Beisein einer Vertrauensperson (Betriebsrat, Datenschutzbeauftragte) geöffnet werden.

Die Videoüberwachung unterliegt hohen formalen Anforderungen, so dass wir empfehlen, solche Maßnahme mit Hilfe spezieller Datenschutz-Expertise zu planen und durchzuführen. Diese Anforderungen umfassen

- das Verzeichnis von Verarbeitungstätigkeiten
- eine Datenschutz-Folgenabschätzung
- die Berücksichtigung des Prinzips „Datenschutz durch Technik“
- die Erfüllung von Informationspflichten gegenüber den Betroffenen
- die Prüfung der zeitlichen Beschränkung der Maßnahmen

Insgesamt muss die Zulässigkeit einer Videoüberwachung pro Betrieb und im Einzelfall bewertet werden. In jedem Fall unterliegt die Videoüberwachung der Mitbestimmung durch den Betriebsrat, wenn vorhanden. In diesem Fall sollte die Durchführung und Auswertung der durch Videoüberwachung erzeugten Aufnahmen in einer Betriebsvereinbarung geregelt werden.

EINSTELLUNGSTESTS

Auch in Bezug auf Einstellungstests im Rahmen eines Personalauswahlverfahrens oder ärztliche Eignungsuntersuchungen gilt der Grundsatz der Erforderlichkeit, wenn kein milderes Mittel zur Verfügung steht. So können beispielsweise ärztliche Bescheinigungen über die gesundheitliche Eignung erforderlich sein, wenn diese Eignung eine wichtige Voraussetzung darstellt, um den Beruf ausüben zu können, (z. B. Lehrer, Pilotin).

Eignungstests (Arbeitsprobe, Leistungstest, Intelligenztest, Assessments,...) müssen nachweisbar geeignet und erforderlich sein, die Eignung des Bewerbers für die vakante Position festzustellen. Allgemeine Intelligenz- oder Persönlichkeitstests zur Erfassung der Gesamtpersönlichkeit des Beschäftigten sind nicht erforderlich und damit unzulässig.

Es muss sich grundsätzlich um einen wissenschaftlich anerkannten Test handeln, der fachkundiger Ausführung bedarf. So müssen psychologische Tests von Psychologen durchgeführt werden, die aufgrund ihrer Schweigepflicht dem Arbeitgeber nur das Gesamtergebnis der Tests übermitteln dürfen (Eignung oder Nichteignung). Das Verfahren muss für die BewerberInnen transparent sein.

Eignungstests im Bewerbungsverfahren auf der Erlaubnisgrundlage der Einwilligung sind zu vermeiden, weil erhebliche Bedenken im Hinblick auf die Freiwilligkeit der Einwilligung naheliegen.

KONZERNINTERNE DATENÜBERMITTLUNG

Sollen personenbezogene Beschäftigtendaten innerhalb eines Konzerns übermittelt werden, ist eine solche Übermittlung grundsätzlich nicht privilegiert; auch hierfür ist eine Rechtsgrundlage notwendig. Innerhalb einer Unternehmensgruppe kann allerdings auch ein berechtigtes Interesse dahingehend bestehen, personenbezogene Daten für interne Verwaltungszwecke zu übermitteln, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten. Hierfür ist eine Interessenabwägung erforderlich. Wird die Datenübermittlung in einer Betriebsvereinbarung geregelt, muss diese rechtmäßig sowie für die Betroffenen nachvollziehbar (transparent) sein und der Zweckbindungsgrundsatz umgesetzt werden.

FAZIT

Für viele Menschen ist das Beschäftigungsverhältnis die Grundlage ihrer wirtschaftlichen Existenz. In diesem Verhältnis werden zahlreiche, teils sensible, personenbezogene Daten erhoben und verarbeitet. Beschäftigte müssen sich darauf verlassen, dass dies im Einklang mit den gesetzlichen Vorschriften geschieht. Ziel der vorliegenden Handreichung ist es, für den vorschriftsmäßigen Umgang mit personenbezogenen Daten in der betrieblichen Praxis zu sensibilisieren. Dazu haben wir die wichtigsten Begriffe erklärt und typische Situationen erläutert. Wir wollten häufige Fragen beantworten und Unklarheiten ausräumen. Ob uns das gelungen ist, können Sie beurteilen, wenn Sie die folgenden Fallbeispiele betrachten.

Wir freuen uns auf Ihre Rückmeldungen und Verbesserungsvorschläge:

mail@stiftungdatenschutz.org

BESCHÄFTIGTEN DATENSCHUTZ

FALLBEISPIELE

THEMEN

IM BEWERBUNGSVERFAHREN

Constanze ist Personalleiterin der Spedition „HappyTrans“. Unter welchen Voraussetzungen darf sie personenbezogene Daten über Bewerberinnen und Bewerber erheben und verarbeiten? Zum Bewerbungsverfahren bei „HappyTrans“ gehört ein umfassender Online-Fragebogen.

Personenbezogene Daten einer Bewerberin oder eines Bewerbers dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses erforderlich ist. Die Fragen des Bewerbungsbogens sind stets unter dem Aspekt stellen, ob diese für die Begründung des konkreten Beschäftigungsverhältnisses erforderlich sind.

Darf Constanze in dem Bewerbungsbogen nach einer Schwerbehinderung fragen? Nach einer Schwangerschaft? Oder nach einer Vorstrafe?

Die Frage nach einer Schwerbehinderung stellt einen Eingriff in das allgemeine Persönlichkeitsrecht der Bewerberin oder des Bewerbers dar und verletzt damit das informationelle Selbstbestimmungsrecht. Diese Wertung ergibt sich auch aus dem Allgemeinen Gleichbehandlungsgesetz (AGG). Ziel dieses Gesetzes ist es, Benachteiligungen unter anderem aus Gründen einer Behinderung oder aufgrund des Geschlechts zu verhindern. Der Arbeitgeber darf danach pauschal keine Auskunft darüber verlangen, ob eine Behinderung vorliegt. Constanze könnte allenfalls fragen, ob die Bewerberin oder der Bewerber an gesundheitlichen, seelischen oder anderen Beeinträchtigungen leidet, die der Erfüllung der erwarteten arbeitsvertraglichen Pflichten entgegenstehen, und zwar wenn dies gerade die wesentliche Voraussetzung für den konkreten Arbeitsplatz darstellt.

Aus den gleichen Gründen darf auch nicht nach einer bestehenden oder geplanten Schwangerschaft gefragt werden. Die pauschale Frage nach einer Schwerbehinderung oder nach einer Schwangerschaft ist demnach unzulässig.

Nach Vorstrafen darf bei der Einstellung nur insofern gefragt werden, wie die Art des zu besetzenden Arbeitsplatzes dies erfordert. Künftige Kurierfahrerinnen dürfen also nach Verkehrsdelikten gefragt werden oder Buchhalter nach Betrugsdelikten.

Ein polizeiliches Führungszeugnis darf ebenfalls nicht pauschal verlangt werden, weil dies auch Vorstrafen enthält, die im Bundeszentralregister bereits getilgt sind und daher nicht mehr angegeben werden müssen.

Zur Jahresmitte hat Constanze die Stelle eines Kuriers besetzt. Sie weiß, dass zum Weihnachtsgeschäft zahlreiche Kuriere gebraucht werden und speichert die Daten der abgelehnten BewerberInnen in einer Datenbank, um sie später anzuschreiben.

Daten von Bewerbern und Bewerberinnen sollten nicht länger als vier Monate gespeichert und danach gelöscht werden[6]. Sofern Arbeitgeber oder Arbeitgeberinnen für zukünftige Stellenbesetzungen Interesse an einer längerfristigen Speicherung haben, muss die freiwillige und informierte Einwilligung der Bewerber und Bewerberinnen eingeholt werden

6 https://sds-links.de/ap1

Weil die Tätigkeit als Kurier besondere Zuverlässigkeit erfordert, schaut Constanze sich die Social-Media-Profile ihrer Bewerber an und fragt die Namen mit einer Suchmaschine ab. Außerdem ruft sie frühere Vorgesetzte der BewerberInnen an. Ist das zulässig?

Im Arbeitsrecht gilt stets der Grundsatz der Direkterhebung, so dass Daten beim Arbeitnehmer zu erfragen sind. Die Datenschutzaufsichtsbehörden vertreten die Auffassung, dass Recherchen in sozialen Netzwerken wie Facebook oder Twitter aus datenschutzrechtlicher Sicht stets unzulässig sind, es sei denn es handelt sich um überwiegend beruflich genutzte Netzwerken wie etwa XING oder LinkedIn. Eine Ausnahme besteht, wenn die Online-Präsenz der Bewerberin als Arbeitsprobe betrachtet werden können, die direkte Aufschlüsse auf deren berufliche Eignung zulässt, zum Beispiel bei Social Media Managern oder Website-Designern.

Die Informationsbeschaffung durch allgemein zugängliche Suchmaschinen wird außerdem für zulässig gehalten, wenn sie für die Einstellungsentscheidung erforderlich ist und ausschließlich Informationen betrifft, die vom Fragerecht umfasst sind. In diesem Falle muss dieser Umstand dem Bewerber bzw. der Bewerberin jedoch spätestens innerhalb eines Monats nach Erlangung der personenbezogenen Daten mitgeteilt werden und ebenso eine Information über die Quellen und die Rechtsgrundlage der Verarbeitung erfolgen.

Sollen bei einer früheren Stelle Erkundigungen eingeholt werden, kann dies wegen des Grundsatzes der Direkterhebung nur mit der freiwilligen Einwilligung der BewerberInnen erfolgen. Da die Freiwilligkeit im Arbeitsverhältnis schwierig zu belegen ist, empfiehlt es sich, die Bewerberinnen um die Angabe von Referenzen zu bitten, wenn Erkundigungen an früheren Arbeitsplätzen eingeholt werden sollen.

Aus Gründen der Effizienz möchte Constanze gern die Auswahlgespräche per Skype Video-Telefonat über das Internet führen. Wie ist dies zu beurteilen?

Die Aufsichtsbehörden empfehlen, die schutzwürdigen Belange der Bewerberinnen und Bewerber zu berücksichtigen und auf Video-Telefonate zugunsten persönlicher Auswahlgespräche zu verzichten. Dennoch kann ein solches Video-Telefonat zulässig sein, wenn die Betroffenen dies selbst wünschen. Dann kann von einer freiwillig erteilten Einwilligung ausgegangen werden, wenn die Betroffenen über den Verwendungszweck und die Weitergabe der Daten durch den Diensteanbieter informiert werden. (Skype zum Beispiel speichert bis zu 90 Tage lang die Chat-Protokolle auf den Servern des Mutterkonzerns Microsoft in den USA.)

Die Aufzeichnung von Auswahlgesprächen ist dagegen ein deutlich schwererer Eingriff in das Selbstbestimmungsrecht der BewerberInnen. Eine Zulässigkeit wird daher von den Aufsichtsbehörden grundsätzlich verneint.

Ferdinand ist Eigentümer der Firma „HappyTrans“ und fordert Constanze auf, bei sämtlichen Einstellungen routinemäßig einen Drogentest durchführen zu lassen. Er verweist darauf, dass er keine „Straftäter“ in seinem Betrieb beschäftigen wolle. Was wird Constanze ihm antworten?

Drogentests sind grundsätzlich zwar zulässig, wenn die Betroffenen wirksam schriftlich eingewilligt haben; sie müssen aber für die Besetzung der konkreten Stelle erforderlich sein. Der Test muss darauf gerichtet sein, eine Alkohol-oder Drogenabhängigkeit nachzuweisen; es darf nicht lediglich darum gehen, den Alkohol-oder Drogenkonsum zu ermitteln. Arbeitsplatzrelevantes Verhalten liegt allerdings nur vor, wenn die Beschäftigten durch ein abhängigkeitsbedingtes Fehlverhalten sich selbst, Leben und Gesundheit Dritter oder bedeutende Sachwerte des Unternehmens gefährden könnte[7].

7 https://sds-links.de/uw1

PERSONALVERWALTUNG

Malermeister Schwarz führt die Personalakten seiner Angestellen handschriftlich, die Blätter heftet er in einem Ordner ab. Neben den Stammdaten notiert er dort, dass Hassan eine Woche wegen eines Schnupfens krankgeschrieben war, und dass Henriette schon wieder an einem Montag zu spät zur Arbeit gekommen ist. Bei Aushilfe Herbert vermerkt Schwarz, dass dieser evangelisch ist. Darf er das?

Die Anwendbarkeit der Vorschriften der DSGVO und des BDSG setzt im Beschäftigtenverhältnis keine automatisierte bzw. IT-gestützte Verarbeitung von Personaldaten voraus. Auch Daten auf Papier unterliegen der DSGVO und dem BDSG[8].

Die Verarbeitung besonders sensibler Kategorien von Daten (z. B. Religionszugehörigkeit, Gesundheitsdaten) kann zur Erfüllung der Pflichten aus dem Arbeitsrecht oder des Sozialschutzes erforderlich sein. In diesem Falle braucht die Verarbeitung dieser sensiblen Daten keine Einwilligung der Beschäftigten; es sei denn, das Interesse des Beschäftigten an dem Ausschluss der Verarbeitung überwiegt. Zu berücksichtigen ist dabei, dass Angaben zur Religionszugehörigkeit nur für die Abführung von Kirchensteuer erhoben und genutzt werden dürfen.

Bei einer längerfristigen Speicherung von Beschäftigtendaten, etwa beim Führen von Personalakten, gelten die Maßstäbe der Erforderlichkeit sowie der Verhältnismäßigkeit. Informationen zur Identität der Beschäftigten sind erforderlich (Name, Anschrift, Alter, Geschlecht, Familienstand, Schulabschluss und Ausbildung). Für die Beurteilung ist wesentlich, ob die langfristig gespeicherten Daten die Persönlichkeitsrechte der Beschäftigten beeinträchtigen. Eine Speicherung von Informationen zu konkreten Krankheitsgründen oder Notizen des Arbeitgebers über die Leistungen oder Nichtleistungen der Beschäftigten können einen Eingriff in das Persönlichkeitsrecht des Arbeitnehmers begründen. Eine Abmahnung hingegen darf als Dokumentation eines Fehlverhaltens in der Personalakte geführt werden. Von besonderer Bedeutung ist außerdem der Zugriffsschutz für die gespeicherten Daten. Ärztliche Gutachten, Gesundheitszeugnisse und ähnliche Dokumente müssen in einem verschlossenen Umschlag in der Personalakte liegen.

Ayse hat ihr Ausbildungsverhältnis bei der Deutschen Röhren AG begonnen. Kurz darauf bekommt sie Post von der „V.Traut"-Versicherung, welche dem gleichen Konzernverbund angehört. Das Versicherungsunternehmen bietet ihr 30% Rabatt an, wenn sie dort eine private Unfallversicherung abschließt. Auf Nachfrage bei ihrem Chef erhält Ayse die Auskunft, dass der Betriebsrat der Deutschen Röhren AG der Übermittlung ihrer Daten an die „V.Traut"-Versicherung zugestimmt hat. Außerdem sei die Datenweitergabe innerhalb des Konzernverbundes unkritisch. Die datenschutzfreundliche Ayse hat dennoch Bedenken. Zu Recht?[9]

Auszubildende fallen unter den Begriff der „Beschäftigten", daher ist hier die Datenschutz-Grundverordnung anzuwenden. Auch innerhalb eines Konzerns ist jedes rechtlich selbstständige Unternehmen im datenschutzrechtlichen Sinne „Dritter". Daher ist für die Datenweitergabe eine Rechtsgrundlage erforderlich.

Denkbar wäre, dass ein berechtigtes Interesse besteht, personenbezogene Daten für interne Verwaltungszwecke zu übermitteln. Bei Ayse und der „V.Traut"-Versicherung trifft dies jedoch nicht zu, weil es sich nicht um Verwaltungszwecke, die für die Durchführung des Ausbildungsverhältnisses erforderlich sind, handelt, sondern um Kundenwerbung.

Auch ein berechtigtes Interesse der „V.Traut" an der Kundenwerbung ist auszuschließen, weil eine Interessenabwägung ergeben müsste, dass Ayses Interesse daran überwiegt, dass ihre Daten nicht ohne ihr ausdrückliches Einverständnis weitergegeben werden.

8 https://sds-links.de/xoq
9 Siehe hierzu Gola/Reif, Praxisfälle Datenschutzrecht, 2. Auflage, S. 45

Die Zustimmung des Betriebsrats ist hier unwirksam, weil der Betriebsrat gar nicht zuständig ist. Eine entsprechende Betriebsvereinbarung wäre nichtig. Zudem muss der Betriebsrat die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer schützen und fördern. Im geschilderten Fall würde dagegen zusätzlich ein Eingriff in das Persönlichkeitsrecht der Beschäftigten vorliegen.

Konrad Controletti, der Inhaber einer Hausgerätereparaturwerkstatt, möchte sein Außendienstteam besser im Blick haben. Daher lässt er sämtliche Dienstfahrzeuge mit einem Ortungssystem ausstatten. Ist dies unter datenschutzrechtlichen Gesichtspunkten zulässig?

Nein. Die umfassende und anlasslose Überwachung von Arbeitnehmerinnen und Arbeitnehmern ist unzulässig.

Ändert sich etwas, wenn Konrad Controletti die Fahrzeuge vor Diebstahl schützen möchte und das Ortungssystem dazu dienen soll, Mitarbeiter- und Fahrzeugeinsätze besser zu koordinieren?

Die Verarbeitung der Ortungsdaten muss für die Durchführung des Beschäftigungsverhältnisses erforderlich sein. Ob „berechtigte Interessen“ als Erlaubnisgrund für die Datenverarbeitung im Beschäftigungsverhältnis in Betracht kommen, ist derzeit noch umstritten. Auf jeden Fall unterliegt eine solche Maßnahme der Mitbestimmung des Betriebsrats.

Das Verwaltungsgericht Lüneburg hat bezogen auf ein Gebäudereinigungsunternehmen entschieden, dass die ständige Erfassung der Fahrzeugposition weder als Diebstahlprävention noch für die Koordinierung der Arbeitseinsätze geeignet oder erforderlich ist. Als milderes Mittel für die Einsatzkontrolle stünde der Kontakt zu den Mitarbeitern per Mobiltelefon zur Verfügung. Allerdings könnte diese Beurteilung in anderen Branchen, zum Beispiel im Transportgewerbe, anders ausfallen.

Die Deutsche Röhren AG ist ein besonders kundenorientiertes Unternehmen möchte auf ihrer Unternehmenswebseite die Fotos und Kontaktdaten (Name, dienstliche Telefonnummer, dienstliche E-Mail-Adresse, Funktion) ihrer AbteilungsleiterInnen veröffentlichen.

Die Veröffentlichung der Kontaktdaten von Arbeitnehmern und Arbeitnehmerinnen, die im Rahmen ihrer Aufgaben für den Außenkontakt verantwortlich sind, ist auch ohne deren Einwilligung zulässig. Die Beschäftigten müssen darüber jedoch informiert werden. Die Veröffentlichung der Fotos ist jedoch davon nicht gedeckt.

Das Sommerfest der Firma „HappyTrans“ war wieder ein großer Erfolg. Social Media Manager Denis hat viele Fotos gemacht, und fragt seine Chefin, ober er eine Auswahl auf der Website und bei Facebook veröffentlichen darf.

Bildnisse dürfen nur mit Einwilligung des Betroffenen veröffentlicht werden. Möchte ein Arbeitgeber daher Fotos seiner Beschäftigten auf der Webseite veröffentlichen, muss er zuvor deren Einwilligung einholen. Die Einwilligung muss informiert und freiwillig sein. „Informiert“ bedeutet hier, dass die Betroffenen wissen müssen, wo, in welchem Kontext und für wie lange die Fotos veröffentlicht werden sollen, und dass sie ihre Einwilligung jederzeit widerrufen können. „Freiwillig“ bedeutet, dass den Betroffenen keinen negativen Konsequenzen drohen, falls sie ihre Einwilligung in die Veröffentlichung verweigern. Die Einwilligung sollte schriftlich eingeholt werden; der Arbeitgeber unterliegt den Informationspflichten der DSGVO.[10]

Dies gilt allerdings nur, wenn die Personen auf den Fotos erkennbar sind. Sind sie nur „Beiwerk“, ist die Einwilligung nicht erforderlich.

10 https://sds-links.de/xhp

NUTZUNG VON INFORMATIONS- UND KOMMUNIKATIONSTECHNIK

Konrad Controletti möchte gern die Telefonate seiner Angestellte ohne deren Wissen mithören. Wie ist dies rechtlich zu bewerten?

Strafrechtlich relevant ist lediglich das Aufnehmen des nicht-öffentlich gesprochenen Wortes oder die Zugänglichmachung an Dritte. Das reine Mithören ist strafrechtlich nicht relevant (zumindest nicht bei handelsüblichen bzw. gebräuchlichen Mithörvorrichtungen in privaten oder geschäftlichen Telefonanlagen). Zu berücksichtigen ist dennoch das Persönlichkeitsrecht der Beschäftigten: Das Recht am gesprochenen Wort ist geschützt und es liegt ein Eingriff in das Persönlichkeitsrecht der Beschäftigten vor, wenn der Arbeitgeber die Vertraulichkeit der Kommunikation verletzt. Dies gilt unabhängig davon, ob es sich um private oder geschäftliche Kommunikation handelt.[11]

Außerdem ist Controletti der Auffassung, dass er die Mails seiner Mitarbeiter und Mitarbeiterinnen jederzeit lesen darf, sofern es sich um betriebliche Kommunikation handelt. Die IT-Azubis Hakan und Charlotte haben Bedenken und weisen darauf hin, dass dies in einer Betriebsvereinbarung geregelt werden müsse.

Der dienstlich bereitgestellte Mail-Account zählt zu den Betriebsmitteln, über die der Arbeitgeber entscheidet und die seinem Direktionsrecht unterliegen. Er kann daher die private Nutzung verbieten und bei dienstlicher Kommunikation jederzeit Einsicht verlangen bzw. sich diese zeigen lassen, sofern nicht die Korrespondenz mit betrieblichen Vertrauensstellen (z. B. Betriebsrat, Betriebsarzt) betroffen ist.

Bei „HappyTrans“ sollen künftig die Beschäftigten WhatsApp auf den dienstlichen Telefonen nutzen. Das ist doch unproblematisch, das nutzen ja ohnehin alle privat?

WhatsApp teilt in seiner Nutzungsrichtlinie mit:

„Im Einklang mit geltenden Gesetzen stellst du uns regelmäßig die Telefonnummern in deinem Mobiltelefon-Adressbuch zur Verfügung, darunter sowohl die Nummern von Nutzern unserer Dienste als auch die von deinen sonstigen Kontakten.“

Allerdings: Die Personen, deren Kontaktdaten in den Adressbüchern gespeichert sind, haben keine Erlaubnis dafür erteilt, dass ihre Kontaktdaten an WhatsApp weitergegeben werden und auf Servern außerhalb Europas gespeichert dürfen. Darüber hinaus erhält WhatsApp Kenntnis von den Metadaten (Zeitpunkt und Dauer der Kommunikation, IP-Adresse, Geräte-ID, etc.), die Rückschlüsse auf die Beteiligten zulassen und Profilerstellung zulassen. Zudem ist die dauerhafte Verschlüsselung der Text- und Bilddaten fraglich. Eine datenschutzkonforme Nutzung von WhatsApp ohne Übertragung von Telefonnummern ist nur bei dauerhafter Deaktivierung des Zugriffs auf die Kontakte direkt nach der Installation möglich. Die deutschen Aufsichtsbehörden weisen darauf hin, dass der Einsatz von WhatsApp durch Unternehmen zur betrieblichen Kommunikation gegen die Datenschutz-Grundverordnung verstößt. Auf die Nutzung von WhatsApp sollte im betrieblichen Kontext verzichtet werden, zumal sichere, datenschutzkonforme Alternativen wie Threema, Signal oder Wire zur Verfügung stehen. Die private Nutzung fällt jedoch nicht unter das Datenschutzrecht.

11 Vgl. hierzu auch ausführlich Gola/Reif, Praxisfälle Datenschutzrecht, 2. Auflage, S. 150

WEITERE INFORMATIONSMATERIALIEN

Alle Beschäftigten sollten sich mit den Kernpflichten des Datenschutzes auskennen. Daher liegen unsere Broschüren für den Einsatz in Unternehmen, Praxen, Vereinen und anderen Organisationen vollständig überarbeitet und an die Anforderungen der EU-Datenschutz-Grundverordnung angepasst vor..

„Datenschutz im Betrieb – Eine Handreichung für Beschäftigte“ soll die notwendigen Hintergründe vermitteln und praxisnah die gesetzlich vorgeschriebenen Informationen darstellen. Die Broschüre umfasst 40 Seiten im DIN A5-Format.

„Datenschutz ganz kurz“ fasst die allerwichtigsten Punkte kurz und knapp zusammen. Für alle, die sich kompakt und praktisch über die Anforderungen des betrieblichen Datenschutzes informieren wollen, auf 20 Seiten im Format DIN lang.

„Das neue Recht auf Datenportabilität“: Mit Inkrafttreten der EU-Datenschutz-Grundverordnung bekam erstmals jede Person das „Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten“. Für die Anbieter von datenverarbeitenden Diensten wird es damit erforderlich, personenbezogene Daten so vorzuhalten, dass diese in einem gängigen Format „mitgenommen“ werden können. Was dies in der Praxis bedeutet, haben wir in zwei Broschüren zusammengetragen.

stiftungdatenschutz.org/themen/informationsmaterialien

STICHWORTVERZEICHNIS

IMPRESSUM

Herausgeber
Stiftung Datenschutz

Autorinnen
Prof. Dr. Anne Riechert
Antje Simon, M.A.

Version
1.0, Stand Juli 2019