Geschäftsbereich
Recht, Zentrale Dienste

Nr. 05/2017

Newsletter Datenschutz

In dieser Ausgabe: Auftragsdatenverarbeitung

Vorbemerkung

Immer mehr Unternehmen lagern ihre Datenverarbeitung, um Kosten und Zeit zu sparen, aus. Hierbei werden personenbezogene Daten von externen Dritten weiterverarbeitet. Eine solche Auftragsverarbeitung unterliegt strengen Voraussetzungen. Auch in der DSGVO finden sich Regelungen dazu. Zentrale Vorschrift ist Art. 28 DSGVO, der den § 11 BDSG ablöst. Inhaltlich ergeben sich Unterschiede bzw. Neuerungen im Vergleich zur alten Regelung. An die Stelle der „Auftragsdatenverarbeitung" tritt die „Auftragsverarbeitung" und die beteiligten Personen werden nicht mehr „Auftraggeber" und „Auftragnehmer" genannt, sondern „Verantwortlicher" und „Auftragsverarbeiter". Der Auftragsverarbeiter wird zudem stärker in die Pflicht genommen.

Auftragsdatenverarbeitung - Was ist das?

Eine Auftragsdatenverarbeitung (ADV) liegt vor, wenn personenbezogene Daten im Auftrag für einen Verantwortlichen verarbeitet werden. Auftragsdatenverarbeitungen kommen insbesondere bei der Wartung von IT-Systemen oder im Bereich Personalverwaltung zum Einsatz.

Die Auftragsverarbeitung nach der DSGVO ist beschränkt „privilegiert". Die Verarbeitung stellt keine Übermittlung an einen Dritten dar. Auch nach der DSGVO bedarf die Übermittlung der Rechtfertigung. Eine Vorschrift, die die Beteiligten von dem grundsätzlich geltenden Verbotsprinzip befreit, gibt es - anders als im BDSG - in der DSGVO nicht. Eine Übermittlung wird jedoch regelmäßig aufgrund „berechtigter Interessen" zulässig sein. Alternativ kann auch Art. 28 DSGVO als eigenständige Befugnisnorm für die Verarbeitung der Daten angesehen werden. Sieht man die Verarbeitung als einheitlichen Vorgang der Datenverarbeitung, richtet sich die Rechtfertigung ebenfalls nach den berechtigten Interessen.

Neu ist, dass der Auftragsverarbeiter für die Verarbeitung der Daten **mitverantwortlich** ist. Bisher war ausschließlich der Auftraggeber für die Datenverarbeitung verantwortlich. Welche Pflichten sich für den Verarbeiter ergeben, erläutern wir Ihnen in diesem Newsletter.

Neu ist auch, dass eine Auftragsdatenverarbeitung auch außerhalb der EU stattfinden kann.

Welche Anforderungen bestehen an den Vertrag? Was muss geregelt sein?

Ein ADV-Vertrag ist nicht zwingend vorgeschrieben. Ausreichend ist auch ein anderer Rechtsakt wie beispielsweise eine einseitig bindende Verpflichtung. Der ADV-Vertrag (oder der Rechtsakt) muss **schriftlich** abgeschlossen werden. Die elektronische Form reicht aus. In ihm muss der Gegenstand und die Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt werden.

Der Auftragsverarbeiter muss - wie bisher auch - sorgfältig und unter Berücksichtigung der technischen und organisatorischen Maßnahmen ausgewählt werden.

Folgende Punkte müssen im Vertag geregelt sein:

1. Personenbezogene Daten dürfen nur auf Weisung des Verantwortlichen verarbeitet werden. Die Weisungen sind zu dokumentieren.

2. Für die Datenverarbeitung sind ausschließlich Personen einzusetzen, die sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

3. Der Auftragsverarbeiter muss alle technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO ergreifen.

4. Die Einschaltung von Subunternehmen bedarf der Genehmigung des Verantwortlichen. Mit dem Subunternehmen ist ebenfalls ein Vertrag abzuschließen. Der Auftragsverarbeiter steht für Datenschutzverstöße des Subunternehmers vollumfänglich ein.

5. Der Auftragsverarbeiter ist zu verpflichten, den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen zu unterstützen, wenn Betroffene ihre Rechte geltend machen.

6. Der Auftragsverarbeiter ist zu verpflichten, den Verantwortlichen dabei zu unterstützen, seine technischen und organisatorischen Maßnahmen zu erfüllen, Datenpannen zu melden und eine Datenschutz-Folgenabschätzung durchzuführen.

7. Nach Abschluss der Verarbeitung sind alle personenbezogenen Daten entweder zu löschen oder zurückzugeben.

8. Der Verarbeiter muss dem Verantwortlichen Überprüfungen/Kontrollen ermöglichen.

Wer haftet bei Datenschutzverstößen?
Nach Art. 82 DSGVO haftet der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter für materielle oder moralische Schäden auf Schadensersatz, die aufgrund eines Verstoßes gegen die DSGVO entstanden sind. Grundsätzlich haften der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter gemeinsam. Die Haftung des Auftragsverarbeiters beschränkt sich auf Verstöße gegen speziell dem Auftragsverarbeiter auferlegte Pflichten. Er kann sich jedoch von einer Haftung freistellen, wenn er nachweisen kann, dass er für den Umstand, durch den der Schaden eingetreten ist, nicht verantwortlich ist.

Bei Verstößen gegen die DSGVO drohen dem Auftragsverarbeiter Geldbußen von bis zu 10 Millionen Euro oder 2 % des gesamten weltweit erzielten Jahresumsatzes. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag werden in jedem Einzelfall unter anderem die Art, Schwere und Dauer des Verstoßes berücksichtigt, ob der Verstoß fahrlässig oder vorsätzlich erfolgte und den Grad der Verantwortung.

Welche Pflichten hat der Auftragsverarbeiter?
Auch der Auftragsverarbeiter unterliegt den gesetzlichen Pflichten und muss die Grundsätze der DSGVO einhalten. Er hat einen Vertreter in der EU zu bestellen, wenn der Auftragsverarbeiter keine Niederlassung in der Union hat. Er muss - genau wie der Verantwortliche - Verfahrensverzeichnisse führen und mit der Aufsichtsbehörde zusammenarbeiten. Der Auftragsverarbeiter hat die Pflicht, technische und organisatorische Maßnahmen zu ergreifen und einen betrieblichen Datenschutzbeauftragten zu bestellen. Verletzungen des Schutzes personenbezogener Daten sind nach Bekanntwerden unverzüglich dem Verantwortlichen zu melden. Wie bislang auch ist der Auftragsverarbeiter grundsätzlich verpflichtet bei der Datenverarbeitung ausschließlich auf Weisung des Verantwortlichen zu handeln.

Welche Pflichten hat der Auftraggeber?
Der Auftraggeber muss, wie bislang auch, seinen Auftragnehmer sorgfältig auswählen. War der Auftraggeber nach dem BDSG ausschließlich für die Datenverarbeitung verantwortlich, so ist nunmehr auch der Auftragnehmer mit in die Verantwortung für die Verarbeitung der Daten genommen worden (siehe oben). Der Auftraggeber hat bei der Auftragsverarbeitung zwar Kontrollrechte, aber keine Kontroll- oder Dokumentationspflichten mehr wie nach dem BDSG. Die entsprechenden Vorschriften aus dem BDSG wurden durch die DSGVO nicht übernommen.

Praxistipp: Durch die Datenschutzgrundverordnung sind für den Auftragsverarbeiter neue Pflichten hinzugekommen, die insbesondere im Vertrag festgehalten werden müssen. Beim Abschluss von Neuverträgen sollte die zum 25.05.2018 eintretende Rechtslage jetzt schon beachtet werden. Altverträge sollten bis Mai 2018 an die neuen Regelungen angepasst werden.

E-Privacy-Verordnung: Änderungen dringend erforderlich
Die EU-Datenschutz-Grundverordnung schafft ein einheitliches Datenschutzniveau in der Europäischen Union. Die EU-Kommission will dies mit der E-Privacy-Verordnung nun für Kommunikation via Telefon, Internet, Messaging, E-Mails oder Internet-Telefonie ergänzen und präzisieren. Die Verordnung wird derzeit im Europäischen Parlament diskutiert und soll voraussichtlich gemeinsam mit der Datenschutz-Grundverordnung im Mai 2018 in Kraft treten.

Keine eigene Regelung notwendig
Die Datenschutz-Grundverordnung gilt für alle personenbezogenen Daten. Sie umfasst damit auch die Informationen, die durch Telekommunikation anfallen. Eine eigene Verordnung wäre also unnötig. Sie könnte vielmehr Geschäftsmodelle, die nach der Datenschutz-Grundverordnung zulässig wären, rechtlich unmöglich machen.

Kein einheitliches Datenschutzniveau
Die Datenschutz-Grundverordnung sorgt für einen starken Datenschutz. Der zusätzliche Vorschlag der Kommission geht jedoch noch darüber hinaus. Bisher gilt für die Verwendung von Cookies, die Nutzungsprofile auf pseudonymer Basis erstellen, die sogenannte Opt-out-Lösung. Danach reicht es aus, dass Unternehmen beim Aufruf der Webseite hierüber in der Datenschutzerklärung informieren und den Nutzern eine Widerspruchsmöglichkeit einräumen. Diese Regelung will die EU-Kommission ersatzlos streichen. Wer weiterhin Nutzungsprofile erstellen möchte, braucht dafür künftig vorher die ausdrückliche Zustimmung des Nutzers. Eine Ausnahme bilden

lediglich Cookies für Konfigurationszwecke und für die Warenkorbfunktion beim Online-Shopping.

Kein eindeutiger Anwendungsbereich
Für die Unternehmen, die unter die E-Privacy-Verordnung fallen - und das sind fast alle - ist der Niveauunterschied unverständlich. Betrieben wird es damit erschwert, die neuen Datenschutzanforderungen umzusetzen. Der Entwurf der E-Privacy-Verordnung betrifft nicht nur die reine Telekommunikation. Sie gilt auch für Daten, die zwar auf dem Telekommunikationsweg übermittelt werden, aber keinerlei Personenbezug haben - wie zum Beispiel Maschine-zu-Maschine-Kommunikation. Wenn Unternehmen auch für diese Datenübermittlungen die strengen Regeln des Entwurfs einhalten müssen, behindert das die Entwicklung von Wirtschaft 4.0 - ohne dass dadurch der Datenschutz gestärkt würde. Zudem behält sich die EU-Kommission vor, den Anwendungsbereich der Verordnung noch weiter zu konkretisieren. Damit werden Unternehmen erst nach und nach erkennen können, ob sie unter den Anwendungsbereich der Verordnung fallen und zusätzlich Geld investieren müssen, um die Anforderungen einzuhalten. Sie stehen aber bereits durch die Datenschutz-Grundverordnung ohnehin vor erheblichen Herausforderungen organisatorischer und technischer Art.

Umsetzung dennoch rechtzeitig angehen
Die E-Privacy-Verordnung enthält zudem - ebenso wie die Datenschutz-Grundverordnung - Öffnungsklauseln, die es den EU-Mitgliedstaaten ermöglichen, eigene ergänzende datenschutzrechtliche Regelungen aufzustellen. Daran wird bereits parallel gearbeitet. Was gut gemeint ist, führt zu Datenschutz-Wirrwarr und hilft deshalb den Unternehmen nicht weiter. In jedem Fall sind Unternehmen gut beraten, sich rechtzeitig mit den neuen Datenregeln zu beschäftigen. Denn bei Missachtung drohen Bußgelder von bis zu 20 Millionen Euro oder bis zu vier Prozent des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs.

Autorinnen: Annette Karstedt-Meierrieks, DIHK Berlin, Katrin Sobania, DIHK Berlin

Papier zur Pseudonymisierung formuliert

Eine Arbeitsgruppe aus Vertretern von Unternehmen, Verbänden, Wissenschaft und Aufsichtsbehörden hat für den letzten IT-Gipfel ein Papier zur Pseudonymisierung nach der EU-Datenschutz-Grundverordnung verfasst.
Link: https://www.gdd.de/aktuelles/startseite/whitepaper-zur-pseudonymisierung

VERANSTALTUNGEN

GDD-Datenschutz-Erfa-Kreis Saarland-Pfalz
Dienstag, 24.10.2017, 13.00 - 16.00 Uhr, Raum 3, Saalgebäude, IHK Saarland, Franz-Josef-Röder-Str. 9, 66119 Saarbrücken.

Anmeldungen bis **23.10.2017** unter E-Mail: rosemarie.kurtz@saarland.ihk.de

Krankheitsbedingte Kündigung
Dienstag, 07.11.2017, 18.00 - 20.00 Uhr, Raum 1 - 3, Saalgebäude, IHK Saarland, Franz-Josef-Röder-Str. 9, 66119 Saarbrücken.

Ein erkrankter Mitarbeiter kann nach dem deutschen Arbeitsrecht gekündigt werden. Die Krankheit des Arbeitnehmers kann unter bestimmten Voraussetzungen sogar Anlass für den Ausspruch einer krankheitsbedingten Kündigung sein. Arbeitgeber sind gut beraten, wenn sie wissen, welche Voraussetzungen erfüllt sein müssen, bevor sie sich von einem erkrankten Mitarbeiter trennen müssen.

Herr Rechtsanwalt Eric Schulien, Rechtsanwaltskanzlei Eric Schulien GmbH Rechtsanwaltsgesellschaft, Saarbrücken, wird in seinem Vortrag aufzeigen, welche Fallkonstellationen es bei der Kündigung wegen Krankheit gibt, wie ein betriebliches Eingliederungsmanagement (bEm) bei einer krankheitsbedingten Kündigung durchzuführen ist und welche Schritte zu beachten sind, wenn eine krankheitsbedingte Kündigung in die Wege geleitet werden muss.

Referent: Rechtsanwalt Eric Schulien, Rechtsanwaltskanzlei Eric Schulien GmbH Rechtsanwaltsgesellschaft, Saarbrücken

Anmeldungen bis **06.11.2017** unter E-Mail: rosemarie.kurtz@saarland.ihk.de

Tag der Immobilienwirtschaft
„Die Immobilienwirtschaft vor neuen rechtlichen Herausforderungen“
Mittwoch, 06.12.2017, 14.00 - 17.30 Uhr, Raum 1, Saalgebäude, IHK Saarland, Franz-Josef-Röder-Str. 9, 66119 Saarbrücken.

Anmeldungen bis **05.12.2017** unter E-Mail: rosemarie.kurtz@saarland.ihk.de

Verantwortlich und Redaktion:
Ass. iur. Heike Cloß, Tel.: (0681) 9520-600, Fax: (0681) 9520-690
E-Mail: heike.closs@saarland.ihk.de
IHK Saarland, Franz-Josef-Röder-Str. 9, 66119 Saarbrücken

Ihre Ansprechpartnerinnen:

Ass. iur. Heike Cloß
Tel.: (0681) 9520-600
Fax: (0681) 9520-690
E-Mail: heike.closs@saarland.ihk.de

Ass. iur. Kim Pleines
Tel.: (0681) 9520-640
Fax: (0681) 9520-690
E-Mail: kim.pleines@saarland.ihk.de

Die in dem Newsletter Datenschutz enthaltenen Angaben sind mit größtmöglicher Sorgfalt erstellt worden. Dennoch kann für Vollständigkeit, Richtigkeit sowie für zwischenzeitliche Änderungen keine Gewähr übernommen werden

Wir danken der AG Datenschutz, DIHK, für die Zurverfügungstellung des Newsletters.

Impressum:
IHK Saarland, vertreten durch Präsident Dr. jur. Hanno Dornseifer und Hauptgeschäftsführer Dipl.-Volkswirt Dr. Heino Klingen, Franz-Josef-Röder-Str. 9, 66119 Saarbrücken, E-Mail info@saarland.ihk.de, Tel. + 49 (0) 6 81/95 20-0, Fax + 49 (0) 6 81/95 20-8 88, UST.- Ident.- Nummer: DE 138117020