Datenschutz *konkret*

ALTHAMMER & KILL

Das Kundenmagazin von Althammer & Kill
Ausgabe 2/2018

Liebe Leserin, lieber Leser,

am 25. Mai 2018 ist Sie in Kraft getreten: die Datenschutz-Grundverordnung. Ziel der Verordnung ist es, den Datenschutz innerhalb der Europäischen Union einheitlich zu regeln. Irgendwie passend hierzu, kamen vor kurzem diverse Missbräuche von personenbezogenen Daten ans Licht wie z. B. im Fall Facebook oder der Deutschen Post.

Ein wesentlicher Aspekt in der Prüfung der Ursache sind die Unternehmensprozesse, bei denen personenbezogene Daten verarbeitet werden. Welche Daten werden erhoben, wer ist an dem Prozess beteiligt und wie sehen die Löschfristen aus? Diese und weitere Informationen müssen von Unternehmen in dem s. g. Verzeichnis von Verarbeitungstätigkeiten dokumentiert werden, sodass zum einen Sie als Unternehmen um die Prozesse wissen und zum anderen die Aufsichtsbehörden bei einer Prüfung Einblick erhalten können. Weitere Informationen zu diesem Thema finden Sie im Beitrag ab Seite 3.

Wir wünschen eine aufschlussreiche Lektüre.

Thomas Althammer & Niels Kill

Datenrisiken 2018: Mit welchen IT-Bedrohungen müssen wir rechnen?

2018 ist ein spannendes Jahr für den Datenschutz. Nicht nur die Datenschutz-Grundverordnung erwartet uns, auch die IT bringt viele Neuheiten. Leider sind damit zugleich neue Risiken verbunden.

Vielleicht haben Sie schon in der einen oder anderen Computer-Zeitschrift von den Prognosen für die Datensicherheit 2018 gelesen. Kaum ein IT-Anbieter lässt die Chance ungenutzt, seine Einschätzung dazu zu veröffentlichen. Virenschutz-Hersteller berichten naturgemäß von neuen Computer-Schädlingen, die uns 2018 bedrohen. Anbieter im Bereich

In dieser Ausgabe:

E-Mail-Sicherheit weisen auf die steigende Gefahr durch Phishing-Angriffe hin, die es auf Passwörter der Opfer abgesehen haben. Hier soll jedoch nun nicht eine weitere Liste der neuen IT-Gefahren folgen, sondern es geht um den richtigen Umgang mit neuen Risiken

Mehr als Malware-Attacken

Die Vielzahl der Prognosen für 2018 kann verwirrend sein. Einige der Vorhersagen stimmen überein, andere führen IT-Bedrohungen auf, von denen man als Nutzer vorher noch nie gehört hat. Wichtig ist, sich weder davon beirren zu lassen noch sich vor den Meldungen über neue Gefahren zu verschließen. Die IT-Risiken für personenbezogene Daten sind so vielseitig wie die IT selbst. Mit jeder neuen App können neue Schwachstellen verbunden sein, jede zusätzliche Vernetzung mit dem Internet kann eine weitere Hintertür für Hacker öffnen.

Wenn Angriffe auf Schwachstellen treffen

Gefährlich für den Schutz der Privatsphäre wird es immer dann, wenn ein Angriff eine Schwachstelle in der IT ausnutzen kann. Wir werden 2018 sowohl bei den Attacken als auch bei den Schwachstellen auf Neuheiten stoßen.

Wir müssen uns darauf einstellen, dass die Angreifer neue Wege suchen, um an vertrauliche Daten zu gelangen. Das kann etwa die Smartwatch sein, die man mit ins Büro bringt und dort über Bluetooth oder WLAN mit dem Tablet verknüpft, um den morgendlichen Lauf abzuspeichern. Dazu muss die Fitness-App ins Internet. Gibt es in der Smartwatch, dem Betriebssystem der Uhr oder den Watch-Apps Sicherheitslücken, können Angreifer diese ausnutzen.

In aller Regel bringen neue Geräte auch neue Schwachstellen mit (wobei die alten Geräte ebenfalls bekannte und unbekannte Sicherheitslücken haben). Jedes neue Gerät, jede neue Anwendung, jede neue Betriebssystem-Version macht somit eine neue Risikoanalyse und eine neue Risikoabwehr erforderlich.

Empfehlung: Prognosen als Weckruf sehen

Es wäre deshalb falsch, die Prognosen für 2018 als Liste zu verstehen, für die man nur die passenden IT-Sicherheitslösungen braucht. Stattdessen sind solche Vorhersagen eine Erinnerung daran, dass es laufend neue IT-Risiken gibt. Es gilt, die Augen offenzuhalten, welche neuen Gefahren drohen, nicht nur zu Beginn des Jahres. Das betrifft sowohl die Anschaffung privater IT-Geräte als auch die Planung neuer Verfahren und Prozesse im Unternehmen, bei denen personenbezogene Daten verarbeitet werden sollen. &

Impressum

Redaktion/V. i. S. d. P.:
Niels Kill, Thomas Althammer

Gestaltung:
Ralf Winternheimer
www.winternheimer.net

Fotos mit Mini-Figuren:
© Katja Borchhardt
www.miniansichten.de

Anschrift:
Althammer & Kill GmbH & Co. KG
Thielenplatz 3 · 30159 Hannover
Tel. +49 511 330603-0

Schutzgebühr Print-Ausgabe: 10,– €

Das Verzeichnis von Verarbeitungstätigkeiten

„Verzeichnis" – das hört sich nach Bürokratie und Arbeit an. Und was bitte bedeutet der seltsame Begriff „Verarbeitungstätigkeiten"? In jedem Fall sollten Sie wissen: Unternehmen droht Ärger, wenn sie kein solches Verzeichnis haben. Also helfen Sie mit, es zu erstellen, wenn man Sie darum bittet.

Unternehmen müssen ab 25. Mai 2018 die Europäische Datenschutz-Grundverordnung (DSGVO) beachten. Sie ist ein EU-Gesetz. Das hat sich herumgesprochen. Weniger bekannt ist den meisten, dass die DSGVO neue Formalien mit sich bringt. Kernstück ist dabei das „Verzeichnis von Verarbeitungstätigkeiten".

Das Ziel: Überblick

Dieses Verzeichnis muss in jedem Unternehmen vorhanden sein. Es soll einen Überblick schaffen, mit welchen personenbezogenen Daten das Unternehmen umgeht und was es mit den Daten tut. Dabei wird es oft um Daten von Kunden gehen. Aber auch Daten von Arbeitnehmern sind erfasst. Ebenso Daten von Lieferanten, wenn dabei Namen von Personen auftauchen.

Pflicht zur Vorlage des Verzeichnisses

Die Datenschutzaufsicht kann jederzeit verlangen, dass ihr ein Unternehmen das Verzeichnis vorlegt. Ansonsten droht ein Bußgeld. Und wenn ein Betroffener Auskunft über seine Daten verlangt, hilft das Verzeichnis dabei, diese Daten zu finden. Es ist also sinnvoll, dieses Verzeichnis sorgfältig zu erstellen. Ab und zu muss es auch aktualisiert werden.

Formular mit oft banalen Antworten

Nehmen Sie es deshalb ernst, wenn Sie mithelfen sollen, für eine gute Qualität des Verzeichnisses zu sorgen! Normalerweise bedeutet das, dass Sie ein Formular ausfüllen müssen, sei es elektronisch oder auf Papier. Dort wird zum Beispiel gefragt,

– welche personenbezogenen Daten Sie am Arbeitsplatz verarbeiten,

– zu welchem Zweck Sie das tun und

– wie lange die Daten aufbewahrt werden.

Die Antworten darauf wirken manchmal recht banal. Beispielsweise ist jedem klar, dass eine Versandabteilung Kundendaten verwendet, um Bestellungen zu bearbeiten. Aber das muss eben festgehalten werden. Im Übrigen zeigt das Beispiel, dass das Formular oft schnell ausgefüllt ist. Der Aufwand hält sich also meistens in Grenzen.

Zögern Sie nicht lange!

Lassen Sie entsprechende Anfragen nicht lange liegen! Denn alle Meldungen aus dem Unternehmen zu einem Verzeichnis zusammenzuführen – das braucht durchaus etwas Zeit. Und seit dem 25. Mai 2018 muss das Verzeichnis fix und fertig vorliegen. Sonst kann es für das Unternehmen Ärger geben.

„Verarbeitungen auf Papier"

Eines wundert viele: In das Verzeichnis müssen auch „Verarbeitungen" aufgenommen werden, bei denen keine EDV zum Einsatz kommt. Klar: Diese Fälle werden seltener. Aber da und dort gibt es immer noch Hängeregistraturen, die alphabetisch nach den Namen geordnet sind, um nur ein typisches Beispiel zu nennen. Auch das ist dann eine „Verarbeitung", die in das Verzeichnis muss. Dasselbe würde natürlich für Karteikarten gelten, die nach Namen geordnet sind.

Überflüssige Datenträger entsorgen!

Eine solche Kartei steht zwar noch herum, wird aber gar nicht mehr benutzt? Das hilft nichts, sie muss trotzdem in das Verzeichnis. Vielleicht ein guter Anlass, die Kartei endlich einmal zu entsorgen. Doch fragen Sie bitte vorher genau nach, ob sie wirklich weg kann oder aus irgendwelchen Gründen doch noch aufgehoben werden muss. Das kann durchaus vorkommen, etwa weil die Steuergesetze das vorschreiben.

Kein Einsichtsrecht für Betroffene

Dürfen eigentlich Betroffene Einsicht in das Verzeichnis nehmen? Dürfte also beispielsweise ein Kunde verlangen, dass er hineinschauen darf? Nein. So etwas gab es früher einmal. Jetzt ist das nicht mehr vorgesehen. Das Verzeichnis ist eine rein interne Angelegenheit.

Aufbewahrung des Verzeichnisses

Wo das Verzeichnis geführt wird, kann das Unternehmen selbst festlegen. Oft liegt es beim Datenschutzbeauftragten. Eine Aufbewahrung durch eine andere Stelle ist aber auch möglich. Für den Datenschutzbeauftragten ist das Verzeichnis wichtig, weil er einen Überblick haben muss, wo personenbezogene Daten liegen.

Zulässige Sprachen: Deutsch und Englisch

Normalerweise ist das Verzeichnis in deutscher Sprache zu führen. Die Aufsichtsbehörden für den Datenschutz akzeptieren es aber auch, wenn Englisch verwendet wird. Hier hat das Unternehmen also die Wahl.

Manche Unternehmen legen dabei einen Katalog der englischen Begriffe fest, die verwendet werden dürfen. Das hat dann gute Gründe. Denn wenn eine Aufsichtsbehörde den Inhalt des Verzeichnisses sprachlich nicht versteht, kann sie eine Übersetzung fordern. Sprachliche Originalität ist deshalb hier fehl am Platz. &

Mitgliederlisten im Verein

Vereine spielen in der Gesellschaft eine wichtige Rolle – in Deutschland ganz besonders. In kleinen Vereinen kennen sich alle Mitglieder persönlich. In größeren Vereinen sieht das anders aus. Kann ein Vereinsmitglied dann fordern, dass es eine Liste aller anderen Mitglieder bekommt? Die Frage ist keineswegs banal, übrigens auch nicht für Unternehmen. Denn gerade kleine und mittelständische Unternehmen engagieren sich oft stark in regionalen Vereinen.

In einem Verein gibt es Spannungen. Fünf Mitglieder wünschen eine außerordentliche Mitgliederversammlung. Dort soll über die strittigen Punkte diskutiert werden. Der Vorstand des Vereins will von einer Mitgliederversammlung jedoch nichts wissen.

Mitgliederversammlung oder nicht?

Nun überlegt die „Fünferbande“, wie sie erreichen kann, dass eine Mitgliederversammlung stattfindet. Sie greift zur Satzung des Vereins. Dort heißt es: Eine Mitgliederversammlung muss einberufen werden, wenn 10 % der Mitglieder das schriftlich fordern. Das ernüchtert die Fünf. Der Verein hat nämlich fast genau 4.000 Mitglieder. Optimistisch betrachtet kennen die Fünf vielleicht 300 Mitglieder persönlich. Und viele davon halten nichts von einer außerordentlichen Mitgliederversammlung.

Der Wunsch: eine Liste aller Mitglieder

Einer der Fünf hat eine Idee. Er verlangt vom Vorstand, dass er eine Liste aller Vereinsmitglieder bekommt, mit Name und Anschrift. Soweit die E-Mail-Adresse bekannt ist, möchte er auch die Mail-Adresse haben. Der Vorstand will aber auch davon nichts wissen. Schließlich gebe es den Datenschutz, und damit sei der Wunsch nicht zu vereinbaren.

Recht klare Regeln der Rechtsprechung

Wer Mitglied eines Vereins ist, weiß es: Über solche Fragen wird öfter einmal gestritten. Da wundert es nicht, dass es einige Gerichtsentscheidungen dazu gibt, bis hinauf zum Bundesgerichtshof. Daraus lassen sich recht klare Regeln für solche Fälle ableiten:

- Eine solche Liste enthält personenbezogene Daten. Sie müssen auch in Vereinen geschützt werden.
- „Einfach so“ darf eine Mitgliederliste nicht herausgegeben werden.
- Der Wunsch, eine Mitgliederversammlung herbeizuführen, stellt ein berechtigtes Interesse dar. Schließlich gehört es zum Vereinsleben, dass man diskutiert und Beschlüsse dazu fasst, was im Verein geschehen soll.
- Ein Mitglied, das eine Mitgliederversammlung anstrebt, hat deshalb Anspruch auf eine Mitgliederliste.
- Diese Liste muss die Angaben enthalten, die notwendig sind, um die anderen Mitglieder zu kontaktieren.
- Dazu gehört auch die Mail-Adresse, aber selbstverständlich nur dann, wenn sie dem Verein vorliegt. Ein Verein muss also keine Mailadressen extra „einsammeln“.

Strikte Zweckbindung der Daten

Selbstverständlich darf die Liste nur für den Zweck verwendet werden, Unterstützung für eine Mitgliederversammlung zu finden. Eine Verwendung für andere Zwecke wäre ein schwerer Datenschutzverstoß.

Einschaltung eines Treuhänders oder nicht?

Nicht ganz einig sind sich die Gerichte darüber, ob die Mitgliederliste dem Mitglied, das sie wünscht, persönlich auszuhändigen ist. Manchmal verlangen die Gerichte, dass ein Treuhänder eingeschaltet wird. Das kann beispielsweise ein Rechtsanwalt oder Notar sein. Wichtig ist, dass der Treuhänder von Berufs wegen zur Verschwiegenheit verpflichtet ist.

Der Treuhänder erhält vom Verein die Mitgliederliste. Diese Liste verwendet er dazu, die anderen Mitglieder anzuschreiben. Das geschieht im Auftrag des Mitglieds, das eine Mitgliederversammlung anstrebt. Danach gibt der Treuhänder die Liste an den Verein zurück oder vernichtet sie. Diese Verfahrensweise ist besonders datenschutzkonform.

Die leidige Kostenfrage

Alle Kosten, die entstehen, muss natürlich das Mitglied tragen, das eine Mitgliederliste verlangt. Insgesamt kann dies bei größeren Vereinen ganz schön ins Geld gehen. Das gilt vor allem dann, wenn ein Treuhänder eingeschaltet werden muss. Denn selbstverständlich arbeitet auch ein Treuhänder nicht kostenlos.

Der Zweck eines Vereins

Manche wundern sich darüber, dass es offensichtlich relativ einfach ist, andere Vereinsmitglieder kontaktieren zu dürfen. Berücksichtigt man aber, wozu Vereine eigentlich da sind, ist das überhaupt nicht erstaunlich. Schließlich bildet ein Verein einen Zusammenschluss von Personen, die einen gemeinsamen Zweck verfolgen. Wer sich einem Verein anschließt, muss es deshalb akzeptieren, dass ihn andere Vereinsmitglieder um Kontakt bitten. Das gilt selbstverständlich nur im Rahmen des Vereinszwecks. &

Eigene Daten finden und löschen lassen

Umfrage zeigen, dass viele Verbraucher von dem Recht auf Vergessenwerden Gebrauch machen wollen. Trifft das auch auf Sie zu? Dann sollten Sie zuerst wissen, wie Sie Ihre Daten im Internet überhaupt finden können. Hier sind einige Tipps.

82 Prozent der Verbraucher in Europa wollen ihre neuen Rechte aus der Datenschutzgrundverordnung (DSGVO) ausüben und die Daten, die Unternehmen zu ihnen erfassen, einsehen, begrenzen oder löschen, so eine Umfrage von Pegasystems.

Sogar ganze 90 Prozent wollen sich darüber informieren, wie ihre Daten verwendet werden. Für mehr als die Hälfte (57 Prozent) ist es sehr wichtig, die Nutzung persönlicher Daten direkt zu kontrollieren. Für 31 Prozent ist dies zumindest noch wichtig.

Betroffenenrechte selbst nutzen

Die deutliche Mehrheit (93 Prozent) würde das Recht zur Datenlöschung nutzen, wenn Unternehmen ihre Daten auf eine Weise nutzen, mit der sie nicht einverstanden sind. 89 Prozent würden das Geschäftsverhältnis daraufhin ganz kappen. Über Dreiviertel der Befragten (78 Prozent) bevorzugen Unternehmen, die mit den Daten offen und transparent umgehen. Knapp die Hälfte der Befragten (47 Prozent) würde ihre Daten gelöscht haben wollen, wenn Unternehmen die Informationen mit anderen Unternehmen austauschen oder gar verkaufen würden.

Es stellt sich die Frage: Wie ist es mit Ihnen? Wollen auch Sie zum Beispiel das Recht auf Vergessenwerden nutzen? Doch wie geht das eigentlich?

Misstrauen ist weit verbreitet

In der Global-Trends-Studie von Ipsos gab jeder Zweite (54 Prozent) an, sich bei der Weitergabe seiner Daten unwohl zu fühlen. Nur jeder fünfte Internetnutzer (20 Prozent) in Deutschland hält seine Daten im Netz für sicher, wie eine weitere Befragung des Digitalverbands Bitkom ergab.

78 Prozent geben dagegen an, ihre Daten seien online eher (40 Prozent) oder völlig (38 Prozent) unsicher. Das höchste Vertrauen bei den Bürgern genießen beim Umgang mit ihren Daten der eigene Internet-Zugangsanbieter sowie der eigene E-Mail-Anbieter (je 49 Prozent). Das geringste Vertrauen wird den sozialen Netzwerken entgegengebracht (15 Prozent).

Welche Daten sind bereits im Internet?

Wenn Sie selbst nun Ihre Daten zum Beispiel bei sozialen Netzwerken oder anderen Online-Diensten löschen lassen, also von Ihrem Recht auf Vergessenwerden Gebrauch machen wollen, stehen Sie vor einer Herausforderung: Wer hat Ihre Daten bekommen, und zwar von Ihnen selbst? Das ist weitaus schwieriger zu beantworten, als man im ersten Moment glauben mag. Bei der Vielzahl an Online-Diensten und Apps, die man nutzt, und mehr noch bei der enormen Zahl der Dienste, bei denen man sich einmal angemeldet hat und die man nicht oder nicht mehr nutzt: Wer hat da noch die Übersicht?

Tipp: Suchmaschinen und spezielle Tools können helfen

Aus Sicht des Datenschutzes lautet die Empfehlung natürlich Datensparsamkeit, die Datenschutz-Grundverordnung spricht von Datenminimierung. So wichtig es auch ist, sich an dieses Prinzip zu halten: Sind die Daten bereits im Internet veröffentlicht, hilft Datenminimierung auch nicht mehr. Stattdessen müssen Sie auf Datensuche gehen, Sie müssen sich also selbst im Internet suchen. Hier erweisen sich Suchmaschinen wie ixquick.de oder duckduckgo.com als hilfreich. Über diese Tools können Sie nach Ihren eigenen Daten suchen, ohne die bei Suchmaschinen üblichen Nutzerspuren zu erzeugen.

Hat man möglichst viele seiner Daten gefunden, beginnt das Verfahren, entsprechende Löschanfragen zu erstellen. Hier bieten spezielle Tools und Dienste ihre Hilfe an. Sie suchen die Daten des Nutzers und helfen bei den Anfragen zur Löschung bei den jeweils verantwortlichen Stellen. Ein Beispiel für einen solchen Dienst ist Privacy Audit (http://privacyaudit.me/en/). Der Dienst listet die gefundenen Daten des Nutzers, bewertet die Risiken der Veröffentlichung und unterstützt bei den Löschanfragen. &

Haben Sie Ihre Daten im Griff? Testen Sie sich!

Frage: Wenn Google Daten aus seinem Datenbestand löscht, sind sie aus dem Internet verschwunden. Stimmt das?

a. Nein, die Daten wären dann nur bei Google gelöscht.
b. Ja, was man bei Google nicht findet, ist nicht mehr im Internet.

Lösung: Die Antwort a. ist richtig. Löschanfragen bei Google entfernen die Daten nicht dort, wo Google sie gefunden hat, also zum Beispiel nicht bei Webseiten oder sozialen Netzwerken, die Daten über einen Nutzer haben. Man muss jeweils die verantwortliche Stelle kontaktieren.

Frage: Das Recht auf Vergessenwerden garantiert die Umsetzung eines jeden Löschwunsches. Stimmt das?

a. Nein, die DSGVO enthält genaue Bedingungen dafür.
b. Ja, denn nur so kann man im Internet wirklich vergessen werden.

Lösung: Die Antwort a. ist auch hier richtig. Nicht jeder Wunsch auf Datenlöschung muss umgesetzt werden. Der Artikel 17 der DSGVO enthält einen Kriterienkatalog. Das Recht auf Vergessenwerden gilt zum Beispiel dann nicht, wenn die Verarbeitung der Daten erforderlich ist zur Ausübung des Rechts auf Freie Meinungsäußerung und Information oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Joint Control in der Datenschutz-Grundverordnung

Die am 25. Mai 2018 in Kraft tretende Datenschutz-Grundverordnung (DSGVO) hat vieles aus dem Bundesdatenschutzgesetz alte Fassung übernommen. Eine vollkommen neue Regelung findet sich in Art. 26 DSGVO. Danach legen zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel der Verarbeitung personenbezogener Daten fest und werden damit „gemeinsam Verantwortliche", auch Joint Controller genannt.

Als Folge der gemeinsamen Festlegung entsteht eine gemeinsame Verantwortung. In einem Vertrag ist zu dokumentieren, welcher Verantwortliche welche Verpflichtungen aus der DSGVO übernimmt.

Mehrere Verantwortliche wirken arbeitsteilig zusammen

Ein Beispiel: Ein Reisebüro, eine Fluggesellschaft und eine Hotelkette betreiben eine gemeinsame Online-Buchungsplattform, über die alle gemeinsam Daten erheben und verarbeiten. Die Daten eines dort registrierten Nutzers können jeweils für eigene Zwecke verarbeitet werden (Buchung einer Reise; Buchung von Flügen; Buchung von Hotelzimmern). Die Daten der registrierten Nutzer könnten zusätzlich für gemeinsame Marketing-Aktionen verarbeitet werden.

Joint Control bietet also die Möglichkeit, dass mehrere Verantwortliche arbeitsteilig zusammenwirken. Das an sich ist eine gute Sache. Problematisch ist allerdings, dass auch die Auftragsverarbeitung nach Art. 28 DSGVO genau dies ermöglicht. Deshalb muss im Einzelfall geklärt werden, ob es sich bei der Datenverarbeitung mehrerer Verantwortlicher um einen Fall von Joint Control oder um einen Fall der Auftragsverarbeitung handelt. Im Fall der Auftragsverarbeitung ist ein Beteiligter lediglich der „verlängerte Arm" des anderen, führt für ihn im Auftrag eine Dienstleistung aus und ist von ihm weisungsabhängig.

Bußgeld kann drohen

Die Frage der Fragen ist damit klar: Wann werden Zwecke und Mittel gemeinsam festgelegt? Die Abgrenzung ist nicht rein akademischer Natur. Je nach Einordnung muss

ein unterschiedlicher Vertrag abgeschlossen werden. Sollte es sich um einen Fall von Joint Control handeln und die Beteiligten haben das Verhältnis als Auftragsverarbeitung deklariert, liegt ein Verstoß vor, der mit einem Bußgeld geahndet werden kann.

Da das Gesetz auf die gestellte Frage keine Antwort gibt, haben sich die Datenschutzbehörden nun erstmals dem Thema angenähert. Eine gemeinsame Festlegung über die Zwecke und Mittel der Verarbeitung soll voraussetzen, dass jeder der Beteiligten einen bestimmenden tatsächlichen Einfluss auf die Zwecke und die wesentlichen Elemente der Mittel der Datenverarbeitung ausübt.

Klar ist dennoch längst nicht alles

Ist damit nun alles geklärt? Nein, es wird viele Fallgestaltungen geben, bei denen man darüber streiten kann, ob ein Beteiligter ein gewisses Maß an Entscheidungsbefugnis und Einfluss hat oder ob er doch nur weisungsabhängiger „Befehlsempfänger“ eines anderen Beteiligten ist, möglicherweise sogar mit einem gewissen Entscheidungsspielraum. Im oben genannten Beispiel ist die Lösung ausnahmsweise mal einfach: Alle drei Beteiligten üben einen tatsächlichen Einfluss auf die Zwecke und die wesentlichen Elemente der Mittel aus und haben damit die Zwecke und Mittel gemeinsam festgelegt. Sie sind gemeinsam Verantwortliche bzw. Joint Controller.

Auch was den Vertrag und dessen Inhalte angeht, tappt man derzeit ein wenig im Dunkeln. Es findet sich lediglich die Vorgabe, dass geregelt sein muss, welcher Verantwortliche sich um die Betroffenenrechte kümmert und wer den Informationspflichten nachkommt. Beide Vorgaben betreffen das Außenverhältnis. Es ist dringend anzuraten, dass die Verantwortlichen darüber hinaus weitere Inhalte vereinbaren, die das Innenverhältnis betreffen. So sollte sich in dem Vertrag eine Regelung zum Haftungsausgleich im Innenverhältnis finden, da die Verantwortlichen der betroffenen Person gegenüber als Gesamtschuldner haften.

Was ist das Wesentliche?

Damit die Betroffenen wissen, wer zu welchem Zweck personenbezogene Daten verarbeitet, müssen die Joint Controller das Wesentliche des Vertrages den betroffenen Personen zur Verfügung stellen. „Wesentlich“ ist zumindest eine nachvollziehbare Beschreibung des Zusammenwirkens und der Rollen der Beteiligten und ihrer jeweiligen Beziehung zur betroffenen Person sowie die Angabe, welcher der gemeinsam Verantwortlichen welche Betroffenenrechte und Informationspflichten erfüllen soll.

Der genaue Anwendsbereich muss noch definiert werden

Stand heute bleibt die weitere Entwicklung zur Abgrenzung zwischen Joint Control und Auftragsverarbeitung abzuwarten. Es ist zu hoffen, dass mit Inkrafttreten der DSGVO ab dem 25. Mai 2018 der Anwendungsbereich von Joint Control präziser herausgearbeitet und definiert wird. &

Benötigen Sie weitere Informationen?

Haben Sie Fragen oder benötigen Sie Unterstützung im Bereich Datenschutz oder Informationssicherheit? Wir freuen uns über Ihre Kontaktaufnahme:
info@althammer-kill.de

Verpflichtung auf das Datengeheimnis

Die EU-Datenschutz-Grundverordnung (DSGVO) beschert ganz Europa viele Änderungen. Auch betroffen ist die Verpflichtung auf das Datengeheimnis – oder etwa doch nicht?

„Ist eine Verpflichtung meiner Mitarbeiter auf das Datengeheimnis notwendig?“ – diese Frage stellen sich zurzeit viele Unternehmen.

Was ändert sich mit der Datenschutz-Grundverordnung?

Eine rasche Antwort fand man bisher in § 5 Bundesdatenschutzgesetz alte Fassung: „Ja, es ist notwendig!“. Spätestens bei der Neuausrichtung auf die DSGVO sucht man diesen Passus jedoch vergebens. Doch bedeutet dies nun, dass neue Mitarbeiter nicht mehr verpflichtet werden müssen?

Für Auftragsverarbeiter ist diese Frage schnell zu verneinen. Art. 28 Abs. 3 lit. b DSGVO schreibt explizit vor, dass der Auftragsverarbeiter im Auftragsverarbeitungsvertrag (AV-Vertrag) gewährleisten muss, dass seine Mitarbeiter bei der Verarbeitung von personenbezogenen Daten zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. An dieser Stelle wird nun nicht mehr vom Datengeheimnis, sondern von Vertraulichkeit gesprochen, welches uns die Augen für den folgenden Absatz öffnen wird.

Der Begriff der „Vertraulichkeit“

Die Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 DSGVO) gelten gleichermaßen für alle Unternehmen, ungeachtet davon, ob es sich um Auftraggeber, Auftragsverarbeiter oder schlichtweg um Unternehmen handelt, die personenbezogenen Daten verarbeiten.

In Art. 5 Abs. 1 lit. f wird man (liest man den Gesetzestext von Anfang an) erstmalig auf den Begriff der „Vertraulichkeit“ aufmerksam gemacht:

„Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“)“ – so der Wortlaut.

Mitarbeiter müssen nach Vorgaben handeln

Blättert man im Gesetzestext einige Seiten weiter, stolpert man unweigerlich über Art. 24 und Art. 32 DSGVO, die final Antwort geben, ob eine Verpflichtung notwendig ist.

Art. 24 DSGVO verlangt, dass der Verantwortliche geeignete technische und organisatorische Maßnahmen umsetzt und nachweisen kann, dass die Verarbeitung im Einklang mit der DSGVO erfolgt - maßgeblich also nach den oben erwähnten Grundsätzen für die Verarbeitung personenbezogener Daten aus Art. 5 DSGVO.

Art. 32 Abs. 4 DSGVO verlangt darüber hinaus, dass der Verantwortliche sicherstellt, dass die Mitarbeiter nach seinen Vorgaben handeln.

Der Kreis schließt sich

Und hier schließt sich der Kreis: Mittels einer Verpflichtung auf die Vertraulichkeit kann der Verantwortliche seinen Pflichten aus den oben genannten Artikeln nachkommen und sicherstellen, dass jeder neue Mitarbeiter Kenntnis über den datenschutzkonformen Umgang von personenbezogenen Daten erlangt.

Für Unternehmen bedeutet dies: Alte Verpflichtungen auf das Datengeheimnis sind nach den Artikeln der DSGVO auszurichten. Das Kind bekommt einen neuen Namen, faktisch geändert hat sich jedoch wenig. &

11 **Datenschutz** *konkret* –
Das Kundenmagazin von Althammer & Kill
Ausgabe 2/2018

ALTHAMMER & KILL

News

Aus unserem aktuellen Newsletter:

Risikomanagement unter der Datenschutz-Grundverordnung
https://www.althammer-kill.de/news-detail/risikomanagement-unter-der-datenschutz-grundverordnung/

Digitalisierung: Chancen durch Gesetzesreform nutzen
https://www.althammer-kill.de/news-detail/digitalisierung-chancen-durch-gesetzesreform-nutzen/

Datenschützer in Sorge! GPS-Sender soll Schulkinder ortbar machen und andere Verkehrsteilnehmer warnen.
https://www.althammer-kill.de/news-detail/datenschuetzer-in-sorge/

Interview: Datenschutz-Grundverordnung im „Wirtschaftsbrief Gesundheit“
https://www.althammer-kill.de/news-detail/interview-datenschutz-grundverordnung/

Cyber-Versicherungen: Was zu beachten ist und wann sich eine Cyber-Versicherungen lohnt
https://www.althammer-kill.de/news-detail/cyber-versicherungen/

Anmeldemöglichkeiten zum Newsletter finden Sie unter:
www.althammer-kill.de

Termine

Wir freuen uns auf persönliche Begegnungen –
zum Beispiel im Rahmen der folgenden Veranstaltungen:

11. – 15.06.2018, Hannover
CeBIT 2018
Die CeBIT 2018 - Wir freuen uns auf Ihren Besuch!

11.07.2018, Online (stifter-helfen.de)
Kostenloses Webinar Datenschutz „Auftragsverarbeitungsverträge“ für Non-Profit-Organisationen
Durch die Verabschiedung der EU-Datenschutz-Grundverordnung (DSGVO) hat sich die datenschutzrechtliche Situation in Deutschland wesentlich geändert. In unserem Webinar lernen Sie die rechtlichen Hintergründe und die Bedeutung von Auftragsverarbeitungsverträgen.

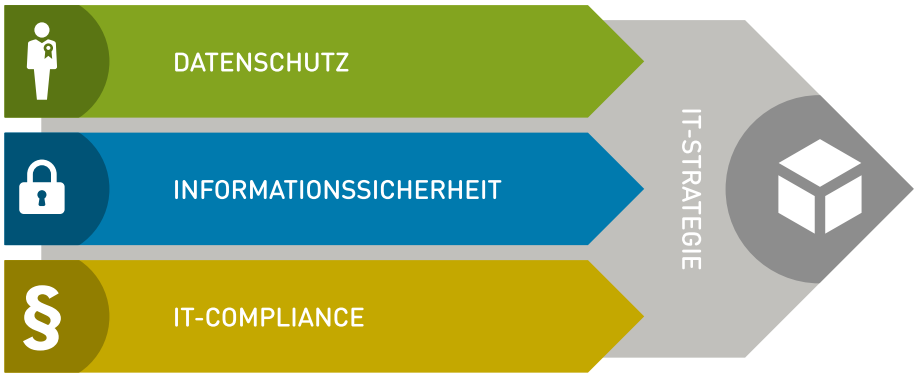
18.07.2018, Hannover
Privacy by Design: Datenschutz nimmt Anbieter und Administratoren stärker in die Pflicht
Spätestens mit der EU Datenschutz-Grundverordnung (DSGVO) sollten Unternehmen bereits bei der Auswahl von IT-Lösungen berücksichtigen, inwieweit diese datenschutzrechtlichen Anforderungen genügen.

24.07.2018, Online (stifter-helfen.de)
Kostenloses Webinar „EU-Datenschutz-Grundverordnung“ für Non-Profit-Organisationen
Durch die Verabschiedung der EU-Datenschutz-Grundverordnung (DSGVO) hat sich die datenschutzrechtliche Situation in Deutschland wesentlich geändert. In unserem Webinar lernen Sie den Status quo von Änderungen, Auswirkungen und Umsetzung kennen.

Termin verpasst? Anruf oder E-Mail genügt und wir lassen Ihnen gern weitere Informationen zukommen.

Althammer & Kill – Wir schützen Ihre Daten.

Althammer & Kill ist ein auf Datenschutz, Informationssicherheit und IT-Compliance spezialisiertes Unternehmen. Unsere Mitarbeiter sind zertifizierte Datenschutzbeauftragte, IT-Sicherheitsexperten, ausgebildete IT-Compliance-Beauftragte und IT-Berater.



Datenschutz

Durch unsere langjährige Erfahrung in unterschiedlichsten Branchen können wir praxisgerechte Lösungen für Ihr Unternehmen entwickeln. Sei es im Rahmen eines konkreten Projektes oder als langfristige Begleitung Ihres Unternehmens z. B. in der Funktion als externer Datenschutzbeauftragter.

Informationssicherheit

Sind Ihre Systeme sicher? In unserer vernetzten Welt fällt es immer schwerer, den Durchblick zu behalten. Angriffe von außen oder ungewollter Informationsverlust: die Risiken sind vielfältig. Wir begleiten Sie zu Security-Fragen, prüfen die Sicherheit Ihrer Systeme und stellen den IT-Sicherheitsbeauftragten.

IT-Compliance

Gesetze, Verordnungen, Normen – da fällt es nicht immer leicht, Compliance-Verstöße zu verhindern. Wir begleiten branchenorientiert und liefern passende Konzepte für einen rechtssicheren Betrieb Ihres Unternehmens, z. B. im Rahmen des Risiko- und Notfallmanagements.

IT-Strategie

Welche Ziele möchten Sie mithilfe der Informationstechnologie in Ihrem Unternehmen erreichen? Wo liegen Möglichkeiten, Nutzen und Wertschöpfung? Wir orientieren unsere Arbeit an Ihren Zielen und begleiten bei der Auswahl und Gestaltung passender Strategien.

Wir sind Mitglied der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD), des Berufsverbandes der Datenschutzbeauftragten Deutschlands e. V. (BvD) und des Fachverbands Informationstechnologien in Sozialwirtschaft und Sozialverwaltung e. V. (FINSOZ).

Althammer & Kill GmbH & Co. KG

Standort Hannover:
Thielenplatz 3 · 30159 Hannover
Tel. +49 511 330603-0

Standort Düsseldorf:
Neuer Zollhof 3 · 40221 Düsseldorf
Tel. +49 211 936748-0

info@althammer-kill.de
www.althammer-kill.de

Mitglied im:

FINSOZ e.V. · GDD Mitglied · BvD e.V. Mitglied · Hannover IT