Newsletter

Ausgabe September 2022

Liebe Leserin, lieber Leser,

unser aktueller Newsletter befasst sich heute unter anderem mit dem Thema Auskunftsrecht. Wir geben Ihnen einen guten Überblick, wie Sie bei einem Auskunftsersuchen vorgehen müssen und haben Ihnen Hinweise zum Umgang mit Auskunftsersuchen von betroffenen Personen zusammengestellt. Diese erhalten Sie als PDF-Dokument anbei und stellen im Arbeitsalltag ein nützliches Hilfsmittel dar.

Des Weiteren möchten wir darauf hinweisen, dass im Namen der Industrie- und Handelskammer (IHK) Phishing-E-Mails verschickt werden. In diesen E-Mails werden Unternehmens- oder auch Kontodaten abgefragt. Die IHK rät, auf keinen Fall auf die E-Mails zu reagieren und im Zweifel Rückfrage bei der IHK zu halten.

Unsere Themen und Quellen im Überblick:

- **Recht auf Auskunft – Art. 15 DS-GVO**
  https://lfd.niedersachsen.de/download/132198

- **Persönliche Haftung von Geschäftsführerinnen und Geschäftsführern für mangelnde Datenschutz Compliance**
  https://www.anwalt.de/rechtstipps/persoenliche-haftung-von-geschaeftsfuehrerinnen-und-geschaeftsfuehrern-fuer-mangelnde-datenschutz-compliance-203878.html

- **„Alte“ Standardvertragsklauseln ab Ende Dezember ungültig**
  https://www.datenschutz-notizen.de/alte-standardvertragsklauseln-ab-ende-dezember-unguel-tig-2238080/

- **WhatsApp: Sicherheitsrisiko beim Einsatz im Unternehmen**
  https://www.dr-datenschutz.de/whatsapp-sicherheitsrisiko-beim-einsatz-im-unternehmen/

- **Urteile**

- **weitere interessante Links**

Viel Spaß beim Lesen,

freundliche Grüße

Mario Barthel

➢ Recht auf Auskunft – Art. 15 DS-GVO

Das Auskunftsrecht ist das am häufigsten in Anspruch genommene Betroffenenrecht. Um Auskunft über die über den Betroffenen gespeicherten personenbezogenen Daten zu erhalten, braucht die betroffene Person keinen Grund. Da für die Beantwortung von Auskunftsersuchen eine Frist von einem Monat vorgesehen ist, ist es für Unternehmen ratsam, auf Auskunftsersuchen vorbereitet zu sein.

Die Auskunftsanfrage kann mündlich, schriftlich oder elektronisch erfolgen und somit bei jedem Mitarbeitenden im Unternehmen eingehen. Aus diesem Grund ist es von besonderer Bedeutung, dass alle Mitarbeiter informiert und geschult sind, wie mit einem Auskunftsersuchen umzugehen ist.

Im ersten Schritt ist zu prüfen, **ob** über die betroffene Person Daten verarbeitet oder gespeichert werden. Ist dies nicht der Fall, ist in einer sogenannten „Negativauskunft“ darauf hinzuweisen. Liegen Daten vor, hat der Betroffene ein Recht auf Auskunft, **welche** Daten vorliegen.

Ablauf eines Auskunftsersuchens:

1. Anfrage liegt vor
   Eingang dokumentieren
2. Identität prüfen
   Ist der Betroffene der, für den er sich ausgibt? Möglichkeiten der Prüfung finden sie in unseren angefügten Hinweisen zum Umgang mit Auskunftsersuchen. Bei Zweifeln an der Identität, nicht ohne weitere Auskunft erteilen!
3. Bei vielen Daten: Um Spezifizierung bitten
   Welche Daten genau? Werden wirklich alle vorliegenden Daten benötigt?
4. Auskunft erteilen
   Vorausgesetzt, die Identität konnte festgestellt werden. Bei schriftlichen Anfragen (auch per E-Mail) ist der Versand an die bekannte Adresse der sicherste Weg (s. beigefügte Hinweise).
5. Auf Wunsch: Kopie der Daten

Damit Sie und Ihre Mitarbeiter wissen, was bei einem Auskunftsersuchen zu tun ist, haben wir Ihnen Hinweise zum Umgang mit Auskunftsersuchen von betroffenen Personen in übersichtlicher Form erstellt. Diese erhalten Sie als PDF zu unserem Newsletter!

Bei der Bearbeitung von Auskunftsersuchen stellt sich immer wieder die Frage, wie weit dies reicht. Grundsätzlich muss alles, was einer betroffenen Person zugeordnet werden kann, beauskunftet werden. Dies umfasst auch interne Vermerke oder Kommunikation zwischen der betroffenen Person und dem Verantwortlichen (auch E-Mail.) Hierzu haben wir Ihnen ein paar interessante Urteile zusammengestellt, die Sie weiter unten finden.

In vielen Fällen handelt es sich bei Auskunftsersuchen um kurze gezielte Informationen, die abgefragt werden. Ein Auskunftsersuchen kann jedoch auch sehr umfangreich sein oder gar auf einem zugrunde liegenden Konflikt gestellt werden. Wir sind Ihnen hierbei gerne behilflich. Wichtig ist hierbei, uns frühzeitig in die Bearbeitung einzubeziehen.

➢ Persönliche Haftung von Geschäftsführerinnen und Geschäftsführern für mangelnde Datenschutz Compliance

Die „Sorgfalt eines ordentlichen Geschäftsmannes“ verpflichtet den Geschäftsführer, unternehmensinterne Regelungen für die Einhaltung gesetzlicher und interner Vorgaben für die Beschäftigten aufzustellen und zu kontrollieren. Ansonsten haftet der Geschäftsführer persönlich gegenüber der GmbH. Diese Sorgfalt ist bekannt und wurde durch die Rechtsprechung über die Jahre weiter konkretisiert.

Mit einem Urteil des Landgerichts München I wurde bereits 2013 für Vorstandsmitglieder einer AG klargestellt, dass nur die Einführung funktionierender Compliance-Systeme die persönliche Haftung des Vorstands verhindern kann.

Das Urteil *Az. 12 U 1520/19* des Oberlandesgerichts Nürnberg vom 30. März 2022 bestätigt dies nun auch für Geschäftsführer einer GmbH. Der im Rahmen der Sorgfaltspflicht bestehende „weitreichende Beurteilungsspielraum“ für Geschäftsführer endet hiernach, wenn ein *„hohes Risiko“* eines Schadens unabweisbar ist und keine „vernünftigen“ geschäftlichen Gründe ersichtlich sind, das Risiko dennoch einzugehen. Nach dem Urteil bedeutet dies, eine Organisationsstruktur zu schaffen, die die Rechtmäßigkeit und Effizienz der Gesellschaft gewährleistet.

Mit Blick auf den Datenschutz können Verstöße gegen die DSGVO zu hohen Bußgeldern oder Schadensersatz führen und bergen somit ein hohes Risiko. Daher ist es für Geschäftsführer wichtig, das Risiko durch geeignete Maßnahmen und Richtlinien im Rahmen eines Datenschutzmanagementsystems zu minimieren. Dies kann Schritt für Schritt erfolgen – gerne unterstützen wir Sie dabei.

➢ „Alte“ Standardvertragsklauseln ab Ende Dezember ungültig

Mit unserem Newsletter 06/2021 haben wir Sie bereits im letzten Jahr auf die Notwenigkeit „neuer“ Standardvertragsklauseln bis zum 27. Dezember 2022 hingewiesen, wenn Sie personenbezogene Daten in Drittstaaten übermitteln.

Übermittlungen personenbezogener Daten an Länder außerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraumes dürfen danach nicht mehr auf „alte“ Standardvertragsklauseln gestützt werden. Unter Umständen kann dies zu Bußgeldern seitens der Aufsichtsbehörden führen.

Was ist zu tun?

- Überprüfen Sie, ob die Liste mit Dienstleistern in unsicheren Drittstaaten aktuell ist oder ob weitere Datenübermittlungen in unsichere Drittstaaten erfolgen.
- Finden Sie heraus, welche Konstellationen bei Ihnen vorliegen und welche Module der neuen EU-Standarddatenschutzklauseln geschlossen werden müssen.
- Nehmen Sie Kontakt mit den betroffenen Dienstleistern auf und fordern Sie den Abschluss der neuen EU-Standarddatenschutzklausen.
- Erörtern Sie mit dem Dienstleister den Inhalt und die Durchführung der Datentransfer-Folgenabschätzung.
- Dokumentieren Sie das Ergebnis der Datentransfer-Folgenabschätzung und legen Sie mit dem Dienstleister einen Turnus für die nächste Prüfung fest.

➢ WhatsApp: Sicherheitsrisiko beim Einsatz im Unternehmen

Viele Unternehmen nutzen WhatsApp, wobei die Kommunikation intern, aber auch extern stattfindet. Auch wenn neben der Standardversion bereits eine Business Variante der App zur Verfügung steht, stellt sich die Frage, ob eine datenschutzkonforme Nutzung überhaupt möglich ist. Wir möchten Sie in diesem Zusammenhang auf die wichtigsten datenschutzrechtlichen Risiken hinweisen.

Risiken der Standardversion:

- Im Gegensatz zur reinen privaten Nutzung fällt der Austausch von betrieblichen Angelegenheiten unter Kollegen (z. B. Krankmeldung) in den Anwendungsbereich der DSGVO. Allein die Billigung durch den Arbeitgeber kann ihn in die Rolle des Verantwortlichen rücken lassen.
- Beim Installieren der App muss der Nutzer den Zugriff auf das abgespeicherte Telefonbuch erteilen. WhatsApp synchronisiert dann das komplette Adressbuch (auch, wenn kein WhatsApp genutzt wird) und somit auch eventuelle geschäftliche Kontakte, die bei einem Diensthandy durchaus vorhanden sein sollten. Die Berechtigung kann man entziehen, schränkt jedoch die WhatsApp Nutzung sehr ein.
- Da WhatsApp ein US-amerikanisches Unternehmen ist handelt es sich um eine Datenübermittlung in einen Drittstaat.
- WhatsApp gibt Daten an weitere Meta-Unternehmen weiter, der sie für Profilbildungszwecke nutzt.

WhatsApp Business ist eine Version für Kleinunternehmen und ist kostenlos. Leider birgt diese Version die gleichen Risiken wie bereits die Standardversion. Zwar wird beim Erstellen eines Unternehmensaccounts ein Auftragsverarbeitungsvertrag (AVV) zur Verfügung gestellt, dieser ist jedoch sehr überschaubar. Ob beispielsweise eine rein weisungsgebundene Verarbeitung auch tatsächlich stattfindet, wozu sich WhatsApp in seinem AVV verpflichtet, kann nicht sicher beantwortet werden.

Insgesamt ist zu sagen, dass die aufgeführten Risiken nicht vollständig sind und der Datenschutz bei WhatsApp noch sehr intransparent ist.

Auf die kostenpflichtige Version WhatsApp Business Cloud API, die sich an mittelständische und Großunternehmen richtet wird aufgrund der sehr vielfältigen Funktionen hier nicht erläutert.

➢ Urteile

<u>Auch Vorbekanntes vom Auskunftsanspruch erfasst</u>

Ein DSGVO-Auskunftsanspruch ist nicht bereits deshalb ausgeschlossen, weil dem Anfragenden die Informationen bekannt sind.

Im Rahmen einer gerichtlichen Auseinandersetzung machte die Klägerin u.a. einen DSGVO-Auskunftsanspruch geltend. Die Beklagte wandte ein, dass der Anspruch bereits erfüllt sei, da die Daten bereits bekannt seien.

Dies sei für eine Erfüllung nicht ausreichend, so das LG Bonn in einem Hinweisbeschluss.

Hinweisbeschluss des Landgerichts Bonn vom 24. Mai 2022 - Az.: 9 O 158/21.

Auch unvollständige Auskünfte können u.U. Auskunftsanspruch nach Art. 15 DSGVO erfüllen

Das Verwaltungsgericht Bremen kam zu der Entscheidung, dass in gewissen Konstellationen auch eine unvollständige Auskunft gegenüber Betroffenen einen Auskunftsanspruch gemäß Art. 15 Datenschutz-Grundverordnung (DSGVO) erfüllen kann.

In diesem Fall hatte das verklagte Jugendamt der klägerischen Bürgerin eine DSGVO-Auskunft nach Art. 15 DSGVO erteilt. Diese war jedoch objektiv nicht vollständig, es fehlten u.a.:

- Hinweis auf Beschwerderecht
- Hinweise auf Berichtigung, Löschung oder Einschränkung der Verarbeitung
- automatisierte Entscheidungsfindung / Profiling

Gleichwohl bewertete das Gericht die DSGVO-Auskunft als erfüllt an. Zwar erbrachte die Beklagte einen Teil der Auskunft erst nach Klageerhebung, aber noch vor der mündlichen Verhandlung, was den maßgeblichen Zeitpunkt für das Gericht darstellt.

Insgesamt ist diese Entscheidung als Einzelfall einzustufen und sollte im Rahmen einer Auskunftserteilung nicht als Vorbild dienen. Schon gar nicht für privatwirtschaftliche Unternehmen, bei denen nicht selten strengere Maßstäbe herangezogen werden.

Urteil des Verwaltungsgerichts Bremen vom 22. Juni 2022 - Az.: 4 K 1/21

➢ Weitere interessante Links

Erklärvideos der Landesbeauftragten für den Datenschutz Niedersachsen
Die Landesbeauftragte für den Datenschutz Niedersachsen hat zum Thema Datenschutz verschiedene Erklärvideos (z. B. Datenschutz im Homeoffice) erstellt.
https://lfd.niedersachsen.de/startseite/infothek/erklarvideos/

E-Rezepte künftig auch mit elektronischer Gesundheitskarte (eGK) einlösbar – Wissenswertes rund um die eGK – Teil 1
Wie die elektronische Gesundheitskarte (eGK) genau funktioniert und wie man damit seine E-Rezepte abholen soll, wird in einem zweiteiligen Beitrag erläutert.
In diesem Teil 1 wird zunächst Allgemeines über die eGK erklärt.
https://www.datenschutzticker.de/2022/09/e-rezepte-kuenftig-auch-mit-elektronischer-gesundheitskarte-egk-einloesbar-wissenswertes-rund-um-die-egk-teil-1/

E-Rezepte künftig auch mit elektronischer Gesundheitskarte (eGK) einlösbar – Wissenswertes rund um die eGK – Teil 2
In Teil 2 geht es um den Datenschutz auf der eGK und darum, wie man künftig mit der eGK E-Rezepte abholen kann.
https://www.datenschutzticker.de/2022/09/e-rezepte-kuenftig-auch-mit-elektronischer-gesundheitskarte-egk-einloesbar-wissenswertes-rund-um-die-egk-teil-2/

Datenschutz nach dem Tod: DSGVO-Rechte für Verstorbene?
Was passiert eigentlich mit personenbezogenen Daten, wenn jemand stirbt? Welche Rechte gibt es hinsichtlich personenbezogener Daten nach dem Tod? Welche Möglichkeiten gibt es, Daten über den Tod hinaus zu schützen oder zu bewahren? Dieser Beitrag gibt eine Übersicht, wie es mit dem Recht und den Daten nach dem Tod weiter geht.
https://www.dr-datenschutz.de/datenschutz-nach-dem-tod-dsgvo-rechte-fuer-verstorbene/

Die Berichtigung von personenbezogenen Daten
Der Berichtigungsanspruch aus Art. 16 DSGVO, wonach die betroffene Person vom für die Datenverarbeitung Verantwortlichen unverzüglich die Berichtigung der sie betreffenden Daten verlangen kann, wird hier betrachtet…
https://www.datenschutz-notizen.de/die-berichtigung-von-personenbezogenen-daten-2237022/

Digitalministerium (BMDV) plant Alternative zu Cookie-Bannern
Das Bundesministerium für Digitales und Verkehr (BMDV) hat einen Entwurf einer „Einwilligungsverwaltungs-Verordnung“ erstellt. Das Dokument wurde offiziell noch gar nicht veröffentlicht. Erste Details des 21 Seiten umfassenden Entwurfes sind jedoch schon durchgesickert.
https://www.dr-datenschutz.de/digitalministerium-bmdv-plant-alternative-zu-cookie-bannern/

Multi-Faktor-Authentifizierung im Homeoffice
Die Multi-Faktor-Authentifizierung (MFA) ist eine Methode, bei der die Zugangsberechtigung durch mehrere unabhängige Merkmale (Faktoren) überprüft wird. Der Beitrag gibt hierzu einen kurzen Überblick.
https://www.datenschutz-notizen.de/multi-faktor-authentifizierung-im-homeoffice-3937526/

Die Aufgaben des Informationssicherheitsbeauftragten (ISB)
Die Aufgaben eines ISBs sind bedeutsam und vielfältig. Der Beitrag gibt einen Überblick!
https://www.dr-datenschutz.de/die-aufgaben-des-informationssicherheitsbeauftragten-isb/