Ausgabe 03/2022

Liebe Leserin, lieber Leser,

hier unser neuer Newsletter mit interessanten Themen für Sie. Darüber hinaus warnt das Bundesamt für Sicherheit in der Informationstechnik (BSI) nach §7 BSI-Gesetz vor dem Einsatz von Virenschutzsoftware des russischen Herstellers Kaspersky. Das BSI empfiehlt, Anwendungen aus dem Portfolio von Virenschutzsoftware des Unternehmens Kaspersky durch alternative Produkte zu ersetzen (s. auch unter interessante Links). Unsere Mandanten haben wir mit Mail vom 17. März 2022 darauf hingewiesen und die Empfehlung ausgesprochen, sich hier mit dem Systemadministrator in Verbindung zu setzen.

Unsere Themen und Quellen im Überblick:

- **Wichtige Datenschutzgrundsätze für die Verarbeitung von Daten**
  https://www.dr-datenschutz.de/wichtige-datenschutzgrundsaetze-fuer-die-verarbeitung-von-daten/

- **3G- Nachweispflicht entfällt – Was passiert mit den Gesundheitsdaten?**
  https://www.datenschutzticker.de/2022/03/3g-nachweispflicht-entfaellt-was-passiert-mit-den-gesundheitsdaten/

- **Die (unterschätzte) Tragweite der Rechenschaftspflicht**
  https://www.datenschutz-notizen.de/die-unterschaetzte-tragweite-der-rechenschaftspflicht-1534173/

- **Datenschutzkonformer Einsatz des Betriebssystems Windows 11**
  https://www.datenschutz-notizen.de/datenschutzkonformer-einsatz-des-betriebssystems-windows-11-3334162/

- **Urteile**

- **weitere interessante Links**

Viel Spaß beim Lesen,

freundliche Grüße

Mario Barthel

➢ Wichtige Datenschutzgrundsätze für die Verarbeitung von Daten

Für eine datenschutzkonforme Verarbeitung von Daten ist die Einhaltung und Beachtung der Datenschutzgrundsätze von besonderer Bedeutung. Hier ein Überblick mit Erläuterungen:

- **Datenminimierung** (Art. 5 Abs. 1 lit. c DSGVO)
  Nach dem Grundsatz der Datenminimierung gilt, immer so wenig personenbezogene Daten wie möglich Daten zu verarbeiten, wie zur Erreichung des Zwecks notwendig sind.

- **Zweckbindung** (Art. 5 Abs. 1 lit. b) DSGVO)
  Die Zwecke der Datenverarbeitung müssen bereits bei der Erhebung personenbezogener Daten festgelegt, eindeutig und legitim sein. Eine Weiterverarbeitung zu anderen Zwecken ist möglich, sofern die Zwecke der Weiterverarbeitung nicht mit den ursprünglichen Erhebungszwecken unvereinbar sind und eine Rechtsgrundlage hierfür vorliegt.

- **Transparenz** (Art. 5 Abs. 1 lit. a) DSGVO)
  Der Grundsatz der Transparenz soll insbesondere gewährleisten, dass die betroffene Person im engeren Sinne ihre Betroffenenrechte und im weiteren Sinne generell ihr Recht auf informationelle Selbstbestimmung wahrnehmen kann. Er setzt voraus, dass eine für die Öffentlichkeit oder die betroffene Person bestimmte Information präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache abgefasst ist. Präzisiert wird der Grundsatz der Transparenz in Art. 12 ff. DSGVO (Informationspflicht und Auskunftsrecht), Art. 25 DSGVO und Erwägungsgrund 78 (Datenschutz durch Technik (Data protection by design) und datenschutzfreundliche Voreinstellungen (Data protection by default)) sowie Art. 42 f. DSGVO und Erwägungsgrund 100 (Zertifizierungsverfahren sowie Datenschutzsiegel und -prüfzeichen).

- **Richtigkeit** (Art. 5 Abs. 1 lit. d) DSGVO)
  Der Verantwortliche muss sicherstellen, dass
  - nur personenbezogene Daten verwendet werden, die sachlich richtig sind,
  - diese auf den neuesten Stand sind und
  - unrichtige personenbezogene Daten unmittelbar gelöscht oder korrigiert werden.

- **Speicherbegrenzung** (Art. 5 Abs. 1 lit. e) DSGVO)
  Es ist nicht erlaubt personenbezogene Daten länger zu verarbeiten, als es für die Zwecke, für die sie eingeholt wurden, notwendig ist. Daher sind die personenbezogenen Daten zu löschen, wenn der Zweck erreicht wurde. Ausnahmen sind öffentliches Archiv-Interesse, wissenschaftliche oder historische Forschungszwecke oder auch statistische Auswertungen.

- **Rechenschaftspflicht** (Art. 5 Abs. 2 DSGVO)
  Der Verantwortliche muss nachweisen können, dass er die Datenschutzgrundsätze einhält. Der Verantwortliche muss auf Nachfragen der Aufsichtsbehörde in der Lage sein, die DSGVO-Konformität überzeugend belegen zu können.

- **Integrität & Vertraulichkeit** (Art. 5 Abs. 1 lit. f) DSGVO)
  Um eine angemessene Sicherheit zu gewährleisten, muss der Verantwortliche die personenbezogenen Daten vor unrechtmäßiger Verarbeitung von Unbefugten und vor unbeabsichtigter Schädigung und Verlust schützen. Hierfür sind geeignete technische und organisatorische Maßnahmen zu treffen.

- **Rechtmäßigkeit** (Art. 5 Abs. 1 lit. a) DSGVO)

Die Rechtmäßigkeit der Verarbeitung wird in Art. 6 DSGVO näher konkretisiert. Die Verarbeitung von personenbezogenen Daten ist demnach rechtmäßig, wenn eine der in Art. 6 Abs. 1 lit. a) bis lit. f) DSGVO genannten Voraussetzungen vorliegt.

- **Treu und Glauben** (Art. 5 Abs. 1 lit. a) DSGVO)
  Die personenbezogenen Daten dürfen nur so verarbeitet werden, wie es bei der Erhebung angegeben wurde und nicht anders. Die Verarbeitung darf nur in dem Umfang gemacht werden, auf welchen die Personen vertrauen. Hierbei geht es meist um die Frage, ob ein bestimmtes Verhalten als redlich bzw. anständig angesehen werden kann.

Datenschutzgrundsätze haben eine übergeordnete Stellung und sind letztlich mit allen Regelungen der DSGVO verwoben, da sie als Auslegungshilfe der anderen Vorschriften der DSGVO dienen. Die Nichteinhaltung der Datenschutzgrundsätze kann zu hohen Bußgeldern führen sowie Maßnahmen der Aufsichtsbehörde nach sich ziehen.

Die Datenschutzgrundsätze des Art. 5 DSGVO sind teilweise sehr weit gefasst. Folglich müssen sie durch zusätzliche Vorschriften aus der DSGVO erst näher konkretisiert werden, um dem gebotenen Datenschutzniveau der DSGVO gerecht zu werden.

➢ 3G- Nachweispflicht entfällt – Was passiert mit den Gesundheitsdaten?

Mit der Änderung des Infektionsschutzgesetzes entfällt ab dem 20. März 2022 die Pflicht für einen 3G-Nachweis am Arbeitsplatz. Die Datenschutzbeauftragte von NRW beschreibt in ihrer Stellungnahme vom 23. März 2022 die datenschutzrechtlichen Folgen. Hier eine kurze Übersicht:

- die Rechtsgrundlage zur Verarbeitung von Gesundheitsdaten, die besondere personenbezogene Daten i.S.d. Art. 9 Abs. 1 DSGVO darstellen, entfällt
- von Arbeitgebern erhobene Daten müssen spätestens sechs Monate nach Erhebung vernichtet oder gelöscht werden
- empfohlen wird, die Daten schon jetzt zu löschen
- Vermerke des Arbeitgebers über den Impfstatus der Angestellten sind umgehend (spätestens in 6 Monaten) zu löschen
- insbesondere kopierte oder gescannte Impfnachweise sind spätestens jetzt zu löschen
- die Löschung muss vollständig und unwiderruflich erfolgen

➢ Die (unterschätzte) Tragweite der Rechenschaftspflicht

Die sogenannte „Rechenschaftspflicht“ des Verantwortlichen ist in Art. 5 Abs. 2 DSGVO geregelt. Danach ist der Verantwortliche für die Einhaltung der Grundsätze des Datenschutzes, die wir im ersten Thema des Newsletters genauer beschrieben haben, verantwortlich und muss dessen Einhaltung nachweisen können.

Diese Dokumente sind hierbei von wesentlicher Bedeutung:

- Verzeichnis von Verarbeitungstätigkeiten,
- Verpflichtungserklärungen auf das Datengeheimnis,
- Meldung des bestellten Datenschutzbeauftragten an die zuständige Aufsichtsbehörde,
- Datenschutz-Schulungen und deren Inhalte,
- Datenschutz-Folgenabschätzungen,
- Gutachten zur Rechtmäßigkeit der Verarbeitung und Interessenabwägungen,
- Auftragsverarbeitungsverträge,
- Geeignete Garantien (Kapitel V DSGVO) für Übermittlungen an Drittländer,
- Richtlinien und Prozesse zur Meldung von Datenschutzverletzungen,
- Richtlinien und Prozesse zur Beantwortung von Betroffenenanfragen,
- Datenschutzverletzungen sowie Benachrichtigungen an betroffene Personen,
- Korrespondenz im Zusammenhang mit Betroffenenanfragen,
- Datenschutzhinweise,
- Einwilligungserklärungen

Wie lange die Nachweise gespeichert oder aufbewahrt werden müssen, ist nicht konkret geregelt, sondern richtet sich nach den möglichen negativen Folgen und Haftungsfragen. Bei eventuellen Abmahnungen, Prüfungen oder Bußgeldverfahren von Aufsichtsbehörden ist es sehr hilfreich, wenn der Verantwortliche Nachweise für eine datenschutzkonforme Verarbeitung vorweisen kann. Daher sollte man sich bei der Aufbewahrungsdauer der entsprechenden Nachweise an den bußgeldrechtlichen und zivilrechtlichen Regelverjährungsfristen (i. d. R. drei Jahre ab Kenntnis) orientieren. Um der Rechenschaftspflicht in angemessener Weise zu entsprechen, ist die Implementierung einer Datenschutzorganisation sehr zu empfehlen. Unseren Mandanten helfen wir gern bei der Erstellung der o.g. Dokumente.

➢ Datenschutzkonformer Einsatz des Betriebssystems Windows 11

Viele Unternehmen nutzen bereits Windows 11 oder überlegen darauf umzusteigen. Hierbei gibt es datenschutzrechtlich einiges zu beachten. Konkrete Empfehlungen für Windows 11 von Aufsichtsbehörden oder dem Bundesamt für Sicherheit in der Informationstechnik (BSI) liegen noch nicht vor. Daher sollten die derzeit für Windows 10 geltenden datenschutzrechtlichen technischen und organisatorischen Maßnahmen (davon inbegriffen die derzeit datenschutzrechtlich empfohlenen Konfigurationseinstellungen) umgesetzt werden, auf die der Artikel anschaulich eingeht.

Ein wichtiger Punkt bleibt weiterhin das datenschutzrechtliche Problem, dass beim Einsatz von Windows Betriebssystemen Daten an Microsoft in die USA übertragen werden. Hierbei ist es zwar möglich, diese Übertragung durch Konfigurationseinstellungen zu steuern, eine vollständige Unterbindung der Datenübertragung ist jedoch aktuell nicht gewährleistet.

Soll Windows genutzt werden, gibt es zwei Möglichkeiten:

1. Verantwortliche müssen für die Übermittlung personenbezogener Daten an Microsoft eine **Rechtsgrundlage** gemäß Artikel 6 Datenschutz-Grundverordnung (DSGVO) nachweisen können. Sofern die übermittelten Daten in den Anwendungsbereich der problematischen US-Aufklärungsprogramme fallen müssen sie darüber hinaus nachweisen, dass durch Übermittlungsinstrumente und zusätzliche Maßnahmen ein Schutzniveau sichergestellt werden kann, das im Wesentlichen dem im Europäischen Wirtschaftsraum garantierten Niveau entspricht (EuGH-Urteil vom 16.07.2020 – C-311/18 – Schrems II).

2. Die Telemetriedatenübermittlung ist vollständig zu unterbinden. Wird durch technische Maßnahmen verhindert, dass eine Übertragung von Daten an Microsoft stattfindet, dann benötigt der Verantwortliche auch keine Übermittlungsgrundlage.

Die Unterbindung der Datenübertragung wird allerdings nur bei der Entreprise Version überhaupt ermöglicht, jedoch nicht vollumfänglich ausgeschlossen. Es ist daher zu empfehlen, die rechtlichen und technischen Datenschutzvorgaben aus dem Prüfschema der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) so umfangreich wie möglich umzusetzen. Je nach getroffenen technischen und organisatorischen Maßnahmen, miteinbezogen auch die gewählten Konfigurationseinstellungen, stellt sich sodann auch die Frage der Risikobewertung im Rahmen einer Datenschutzfolgenabschätzung.

➢ Urteile

<u>BEM-Verfahren scheitert aufgrund fehlerhafter Datenschutzhinweise</u>

In diesem Fall ging es um die Wirksamkeit der ordentlichen krankheitsbedingten Kündigung eines Arbeitnehmers. Vor der Kündigung hatte der Arbeitgeber mehrmals zum betrieblichen Eingliederungsmanagement (BEM) eingeladen, worauf der Arbeitnehmer nicht reagierte.

Das Landesarbeitsgericht teilte im Ergebnis die Ansicht des Arbeitsgerichts, dass die Kündigung nicht sozial gerechtfertigt sei. Es stütze seine Entscheidung maßgeblich auf die unsachgemäße Einleitung des BEM Verfahrens aufgrund von Datenschutzverletzungen des Arbeitgebers. Moniert wurde, dass der Arbeitgeber in der vorgelegten Datenschutzerklärung eine zu weitgehende Preisgabe von Gesundheitsdaten verlangt hatte. Des Weiteren fehlte der Hinweis, dass Angaben gegenüber dem Arbeitgeber zu Diagnosen oder ähnlich sensiblen Daten freiwillig angegeben werden können.

Urteil des LAG Baden-Württemberg vom 20. Oktober - Az.: 4 Sa 70/20

<u>Wann wird eine E-Mail-Signatur zur Werbung?</u>

In diesem Fall ging es um die Frage, ob in einer E-Mail-Signatur bereits Werbung enthalten war, ohne dass eine wirksame Einwilligung hierfür vorgelegen hat. Ein Unternehmen hatte seinem Kunden zwei E-Mails gesendet, die zwar inhaltlich auf die Vertragsabwicklung Bezug genommen hatten, aber jeweils den folgenden Zusatz enthielten:

„XXXXX. Organisiert, denkt mit, erledigt. Nutzen Sie www.XXXXX.de"

Der Kunde klagte, dass es sich dabei bereits um Werbung gehandelt habe. Unstreitig war, dass der Kunde zu keinem Zeitpunkt eine Einwilligung für Telefon- oder E-Mail-Werbung erteilt hatte. Nach einer erfolglosen Abmahnung nahm der Kunde das Unternehmen unter Berufung auf sein Allgemeines Persönlichkeitsrecht in Anspruch.

Das Gericht kam in der Berufung zu dem Ergebnis, dass es auf den Gesamtanteil der Werbung an der Mail nicht ankomme. Vielmehr müsse eine solche Mail unabhängig davon beim Enthalten eines werblichen Zusatzes generell als Werbung qualifiziert werden.

Urteil des KG Berlin vom 15. September 2021 – Az: 5 U 35/20

➢ Weitere interessante Links

BSI warnt vor dem Einsatz von Kaspersky-Virenschutzprodukten
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt nach §7 BSI-Gesetz vor dem Einsatz von Virenschutzsoftware des russischen Herstellers Kaspersky. Das BSI empfiehlt, Anwendungen aus dem Portfolio von Virenschutzsoftware des Unternehmens Kaspersky durch alternative Produkte zu ersetzen.
https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220315_Kaspersky-Warnung.html

BvD nimmt Stellung zur „Orientierungshilfe Telemedien 2021" der DSK
Die Datenschutzkonferenz (DSK) hat am 20. Dezember 2021 eine Neufassung ihrer 2019 erstellten Orientierungshilfe für Anbieter von Telemedien verabschiedet. Die Neufassung der Orientierungshilfe war aufgrund wesentlicher Rechtsänderungen erforderlich, die mit der Geltung des Telekommunikation-Telemedien-Datenschutzgesetzes (TTDSG) ab dem 1. Dezember 2021 eingetreten sind.
https://www.bvdnet.de/bvd-nimmt-stellung-zur-orientierungshilfe-telemedien-2021-der-dsk/

Arbeitgeber und das Fernmeldegeheimnis nach dem TTDSG
Ist der Arbeitgeber zur Einhaltung des Fernmeldegeheimnisses verpflichtet? Wie verhält sich die Anwendung des TTDSG zur DSGVO? Welche Fallstricke sind da zu beachten? Diesen Fragen widmet sich der Beitrag, der in der Zeitschrift „Datenschutz und Datensicherheit" 2/2022 veröffentlicht wurde und als pdf heruntergeladen werden kann.
https://www.datenschutz-notizen.de/wp-content/uploads/2022/03/DuD_2_2022_ArbeitgeberUnd-DasFernmeldegehe.pdf

Angemessenheitsbeschlüsse nach Art. 45 DSGVO
Die Europäische Kommission kann sogenannte Angemessenheitsbeschlüsse fassen. Der Artikel informiert über diese Beschlüsse und führt auf, für welche 14 Staaten diese zurzeit existieren.
https://www.datenschutzticker.de/2022/03/angemessenheitsbeschluesse-nach-art-45-dsgvo/

Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO)
Die Berliner Beauftragte für Datenschutz und Informationsfreiheit hat Orientierungshilfe zum Thema Direktwerbung veröffentlicht.
https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2022-OH-Werbung.pdf

Doctolib und Datenschutz aus Sicht der Arztpraxis
Der Artikel beleuchtet, ob Doctolib datenschutzkonform genutzt werden kann. Hinweis für unsere Praxen, dieser Beitrag sollte gelesen werden.
https://www.datenschutz-recht-medizin.de/doctolib-datenschutz-arztpraxis/