

## Ausgabe 01/2022

Liebe Leserin, lieber Leser,

der aktuelle Newsletter hält wieder interessante Themen für Sie bereit. Die Entscheidung der österreichischen Datenschutzbehörde, dass die Übermittlung personenbezogener Daten in die USA aufgrund der Nutzung des Trackingtools „Google Analytics“ auf einer österreichischen Website nicht datenschutzkonform ist, sorgt für viele Fragen. Wir geben Ihnen einen kurzen Überblick, was dies bedeutet.

Unsere Themen und Quellen im Überblick:

- **Zugriff auf E-Mails und Dateien von ehemaligen Mitarbeitern**  
<https://www.datenschutz-guru.de/zugriff-auf-e-mails-und-dateien-von-ehemaligen-mitarbeitern/>
- **Die elektronische Krankmeldung – aus AU wird eAU**  
<https://www.althammer-kill.de/aktuelles/news/detail/die-elektronische-krankmeldung-aus-au-wird-eau>
- **Österreichische DSB hält Einsatz von Google Analytics für nicht DSGVO-konform**  
<https://www.datenschutz-notizen.de/oesterreichische-dsb-haelt-einsatz-von-google-analytics-fuer-nicht-dsgvo-konform-4833535/>
- **Dürfen Arbeitgeber den Impfausweis kopieren?**  
<https://www.datenschutz-notizen.de/duerfen-arbeitgeber-den-impfausweis-kopieren-1033501/>
- **Urteile**
- **weitere interessante Links**

Viel Spaß beim Lesen,

freundliche Grüße

Mario Barthel

---

## ➤ Zugriff auf E-Mails und Dateien von ehemaligen Mitarbeitern

Manchmal ist es notwendig nach dem Verlassen eines Mitarbeiters noch auf sein E-Mail-Postfach oder auf sein individuelles Laufwerk zuzugreifen. Doch was ist, wenn hier auch private E-Mails oder Dokumente gespeichert sind? Dies kann zu datenschutzrechtlichen Problemen führen, z. B. wenn die private E-Mail-Nutzung den Mitarbeitern erlaubt ist. Wir empfehlen immer, dies im Datenschutzhandbuch auszuschließen.

Abhängig ist dies von vielen Faktoren, auf die gar nicht näher eingegangen werden soll. Vielmehr soll eine einfach umzusetzende Lösung vorgestellt werden. Sicherlich gibt es Ausnahmesituationen, wie eine vorzeitige Freistellung eines Mitarbeiters, in denen dies nicht funktioniert – in der Regel sollte aber auf diese Weise möglichen Risiken vorgebeugt werden.

Der Lösungsansatz ist ganz pragmatisch:

1. Bevor eine Mitarbeiterin oder ein Mitarbeiter das Unternehmen verlässt, ist diese Person verpflichtet, ihren E-Mail-Account und die Dateien in den genutzten Ordnern bzw. IT-Systemen auf „private“ Dateien zu sichten.
2. Findet die Person private Inhalte, bei denen sie nicht möchte, dass das Unternehmen darauf zugreift, dann kann die Person die Löschung initiieren. Entweder selbst oder – falls dies nicht möglich ist – durch den IT-Support bzw. die jeweils zuständige Abteilung.
3. Ist eine Löschung der Dateien technisch (oder rechtlich) nicht möglich, könnte man über eine Sperrung der Daten nachdenken, soweit dies technisch umsetzbar ist.

Hierfür ist eine Art „Laufzettel“ erforderlich, den der Mitarbeiter erhält, bevor er aus dem Unternehmen ausscheidet. Als ein solches Beispiel stellen wir Ihnen im Anhang das word-Dokument „**Pflichtenliste für Mitarbeiter, die das Unternehmen verlassen**“ zur Verfügung.

## ➤ Die elektronische Krankmeldung – aus AU wird eAU

Ablauf der elektronischen Arbeitsunfähigkeitsbescheinigung (eAU):

**Seit dem 1. Januar 2022**

- Die Arztpraxis meldet die Arbeitsunfähigkeit elektronisch an die Krankenkasse. Diese Daten werden verschlüsselt über die Telematikinfrastruktur übermittelt. Eine Bescheinigung muss der Patient bei der Krankenkasse nicht mehr einreichen. Diese erhält er bis Ende Juni nur noch für den Arbeitgeber, die entsprechend weiterzuleiten ist.

**Ab dem 1. Juli 2022**

- Die Krankenkasse muss eine Meldung zum elektronischen Abruf der AU-Daten für Arbeitgeber erstellen. Der Arbeitnehmer informiert den Arbeitgeber lediglich darüber, dass er erkrankt ist. Der Arbeitgeber kann die eAU selbst bei der Krankenkasse abrufen.

Der Patient kann auf Wunsch weiterhin einen Ausdruck seiner Arbeitsunfähigkeitsbescheinigung erhalten. Die Datenübertragung zum Arbeitgeber erfolgt verschlüsselt in einer systemgeprüften Abrechnungssoftware. Diagnosedaten sind hier nicht enthalten. Um als Arbeitgeber auf die Umstellung gut vorbereitet zu sein, sollte bereits jetzt die Zeit genutzt werden. Ein Abruf der eAU ist bereits heute möglich, so dass die technische und administrative Umstellung auch vor dem 1. Juli 2022 passieren kann.

Folgendes ist organisatorisch und rechtlich zu beachten:

- Klären Sie ab, ob die von Ihnen eingesetzte Software „eAU-fit“ ist.
- Prüfen Sie die damit zusammenhängenden Prozesse und passen Sie diese ggf. an.
- Zuständige Beschäftigte müssen für das neue Verfahren geschult werden.
- Die betroffenen Mitarbeiter müssen bei Ihnen beschäftigt sein.
- Der Mitarbeiter muss Ihnen mitgeteilt haben, dass eine eAU abzurufen ist.

## ➤ **Österreichische DSB hält Einsatz von Google Analytics für nicht DSGVO-konform**

Die österreichische Datenschutzbehörde (DSB) hat entschieden, dass die Übermittlung personenbezogener Daten in die USA aufgrund der Nutzung des Trackingtools „Google Analytics“ auf einer österreichischen Website nicht als datenschutzkonform einzustufen ist und somit einen Datenschutzverstoß darstellt. Diese Entscheidung hat für viel Aufsehen gesorgt.

Die DSB begründet ihre Entscheidung vor allem damit, dass durch die Nutzung von Google Analytics personenbezogene Daten an den Auftragsverarbeiter Google LLC in die USA übermittelt wurden, ohne ein angemessenes Datenschutzniveau zu gewährleisten. Die in diesem Fall abgeschlossenen Standardvertragsklauseln und getroffene technische und organisatorische Maßnahmen reichten der DSB nicht aus. Die DSB argumentiert hier, dass die Standardvertragsklauseln lediglich einen Vertrag zwischen zwei Parteien darstellen. Dieser bietet keinen Schutz davor, dass Google als Kommunikationsdienstleister der Überwachung des US-Nachrichtendienstes unterliegt und somit verpflichtet ist, personenbezogene Daten zur Verfügung zu stellen. Hier bieten auch Maßnahmen wie z. B. eine Verschlüsselung keinen Schutz, da auch Verschlüsselungsschlüssel auf Anforderung für den Zugriff gewährt werden müssen.

Der Beschluss der DSB weist auf wesentliche Problematiken bei der Nutzung von Google Analytics hin. Möchte man hier kein Risiko eingehen, gibt es zahlreiche andere Produkte für die Reichweitenmessung, die ohne die Übermittlung personenbezogener Daten in ein Drittland auskommen. Ob die Entscheidung der DSB einer gerichtlichen Prüfung standhalten kann, ist aus folgenden Gründen fraglich.

- Der Verantwortliche schließt beim Einsatz von Google Analytics einen Auftragsverarbeitungsvertrag mit der Google Ireland Limited ab, wodurch nicht der Verantwortliche, sondern der Auftragsverarbeiter, also die Google Ireland Limited, zum Datenexporteur wird. Die Google Ireland Limited hat dabei gemäß Klausel 14 der Standardvertragsklauseln ein sogenanntes Transfer Impact Assessment durchzuführen und insgesamt ein angemessenes Datenschutzniveau zu gewährleisten, sodass der Verantwortliche (nur) mittelbar für die „unzulässige“ Datenübermittlung belangt werden könnte.
- Die DSB fasst den Begriff der personenbezogenen Daten sehr weit und lässt außer Acht, dass kein konkreter Zugriff eines US-Nachrichtendienstes nachgewiesen werden konnte und Google mitgeteilt hat, dass solche Zugriffe noch nie gewährt wurden.

Wer nicht auf Google Analytics verzichten, aber hierbei kein Risiko eingehen möchte, kann auf die Einwilligungslösung (Art. 49 Abs. 1 lit.a DSGVO) zurückgreifen. Hiernach ist eine datenschutzkonforme Übermittlung möglich, wenn:

*„(...) die betroffene Person[...] in die vorgeschlagene Datenübermittlung ausdrücklich eingewilligt [hat], nachdem sie über die für sie bestehenden möglichen Risiken derartiger Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien unterrichtet wurde, (...)“*

Diese Umsetzung kann mit einem Einwilligungsbanner auf der Website erfolgen. Vorausgesetzt der Einwilligungsbanner übermittelt nicht selbst schon Daten in die USA!!!

## ➤ **Dürfen Arbeitgeber den Impfausweis kopieren?**

Für Mitarbeitende in Einrichtungen des Gesundheitswesens muss ab dem 15. März 2022 die Voraussetzung „geimpft“ oder „genesen“ vorliegen (2G-Regelung). Andernfalls hat der Arbeitgeber dies an das Gesundheitsamt zu melden, welches die Möglichkeit hat, ein Betretungs- oder Berufsausübungsverbot gegenüber der betroffenen Person auszusprechen.

Kommt der Arbeitgeber seiner Kontroll- und Dokumentationspflicht nicht nach, kann dies als Ordnungswidrigkeit zu Bußgeldern bis zu 25.000 EUR führen. Doch wie setzt er diese Pflicht datenschutzkonform um?

Hier wäre es einfach, den Impfausweis zu kopieren und abzulegen, was jedoch dem Prinzip der Datensparsamkeit widerspricht. Denn der Impfausweis enthält neben den benötigten Daten wie Vor- und Nachname oder die Anzahl und das Datum der Impfungen weitere Informationen, die nicht von Belang sind.

Zu empfehlen ist die Nutzung eines entsprechenden Formulars, dass nur die benötigten Daten berücksichtigt, die bei der Einsichtnahme in den Impfausweis erfasst werden. Dies kann digital oder analog erfolgen.

## ➤ **Urteile**

### Nutzung von Google Fonts auf Webseite datenschutzwidrig, berechtigtes Interesse nicht ausreichend

Die Einbindung von Google Fonts ist datenschutzwidrig und kann auch nicht durch das berechtigte Interesse nach Art. 6 Abs.1 f) DSGVO abgedeckt werden.

Der Beklagte hatte die Google Fonts nicht lokal auf seinem Server gespeichert, sondern per Link auf seiner Webseite eingebettet. Das LG München I sah darin einen Datenschutzverstoß.

*Urteil des LG München I vom 20. Januar 2022 - Az.: 3 O 17493/20*

### Wann liegt Rechtsmissbrauch beim DSGVO-Auskunftsanspruch vor

In diesem Fall war der Kläger bei der verklagten Versicherung krankenversichert. Er wehrte sich gegen Prämien erhöhungen der Versicherung, die er für unbegründet hielt und verlangte in diesem Zusammenhang von der Beklagten auch Auskunft nach Art. 15 DSGVO.

Das OLG Hamm stufte diese Anfrage als rechtsmissbräuchlich ein, sodass das angefragte Unternehmen das Begehren ablehnen kann.

Bei der Auslegung, was in diesem Sinne rechtsmissbräuchlich ist, ist auch der Schutzzweck der DSGVO zu berücksichtigen. Das Auskunftsrechts soll es der betroffenen Person problemlos und in angemessenen Abständen ermöglichen, sich der Verarbeitung der sie betreffenden personenbezogenen Daten bewusst zu werden und die Rechtmäßigkeit dieser Verarbeitung überprüfen zu können. Dies ist jedoch nicht das Anliegen des Klägers.

Sinn und Zweck der von ihm begehrten Auskunftserteilung ist vielmehr ausschließlich die Überprüfung etwaiger vom Beklagten vorgenommener Prämienanpassungen wegen möglicher formeller Mängel. Eine solche Vorgehensweise ist vom Schutzzweck der DSGVO aber nicht umfasst.

*Urteil des OLG Hamm vom 15. November 2021 – Az: 20 U 269/21*

## Datenschutzrechtliche Pflichten bei einem ärztlichen Behandlungsvertrag

Wird ein Patient in einem Krankenhaus behandelt, hat das betreffende Unternehmen entsprechende organisatorische Maßnahmen zu ergreifen, um sicherzustellen, dass nur solche Angestellte auf die Krankendaten Zugriff nehmen können, deren Mitarbeit notwendig ist.

Der Kläger war selbst Chefarzt der Inneren Abteilung des verklagten Krankenhauses und wurde aufgrund eines Herzinfarkts 2015 selbst in der kardiologischen Abteilung der Klinik behandelt.

Im Nachhinein stellte sich heraus, dass während seiner Behandlung mehrere Mitarbeiter auf seine Krankheitsdaten Zugriff nahmen, die hierzu nicht berechtigt waren. Dies stufte das Gericht als Datenschutzverstoß ein.

Dabei sei es unerheblich, ob die Ursache in dem Unterlassen entsprechender organisatorischen Maßnahmen liege oder in dem Fehlverhalten eines Mitarbeiters zu suchen sei.

Der Kläger verlor dennoch aufgrund von Verjährung.

*Urteil des LG Flensburg vom 19. November 2021 – Az. 3 O 227/19*

## ➤ **Weitere interessante Links**

### Experten-Gutachten zu U.S.-Überwachungsgesetzen

Die Datenschutzkonferenz hat das „Gutachten zum aktuellen Stand des US-Überwachungsrechts und der Überwachungsbefugnisse“ von Stephen I. Vladeck vom 15.11.2021 veröffentlicht und in dem Dokument „Wesentliche Befunde des Gutachtens von Stephen I. Vladeck vom 15.11.2021 zur Rechtslage in den USA“ zusammengefasst.

[https://www.datenschutzkonferenz-online.de/weitere\\_dokumente.html](https://www.datenschutzkonferenz-online.de/weitere_dokumente.html)

### Häufige Fragestellungen nebst Antworten zur Verarbeitung von Beschäftigtendaten im Zusammenhang mit der Corona-Pandemie

Anwendungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 20. Dezember 2021.

<https://datenschutz-hamburg.de/assets/pdf/DSK-Anwendungshilfe.pdf>

## Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021

DSK hat am 20. Dezember 2021 hierzu eine neue Orientierungshilfe veröffentlicht.

[https://www.datenschutzkonferenz-online.de/media/oh/20211220\\_oh\\_telemedien.pdf](https://www.datenschutzkonferenz-online.de/media/oh/20211220_oh_telemedien.pdf)

## Cookie-Einwilligung: Ist die Information, dass Dritte keinen (!) Zugriff auf Cookies haben, zwingend erforderlich?

Nach § 25 Abs. 1 TTDSG sind die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, nur zulässig, wenn der Endnutzer auf der Grundlage **von klaren und umfassenden Informationen** eingewilligt hat. Diese Information des Endnutzers und die Einwilligung haben gemäß Satz 2 nach der DSGVO zu erfolgen. Aber was genau ist mit „umfassenden Informationen“ gemeint?

<https://www.delegedata.de/2022/01/cookie-einwilligung-ist-die-information-dass-dritte-keinen-zugriff-auf-cookies-haben-zwingend-erforderlich/>

## Leitfaden zum Umgang mit Datenpannen – Teil 1 und 2

Teil 1 des Leitfadens beschäftigt sich mit den Fragen, wann eine Datenpanne vorliegt und welche Vorkehrungen zur Vermeidung einer Datenpanne getroffen werden können. In Teil 2 geht es um das Vorgehen bei Kenntnisnahme von einer Datenpanne: Wie wird eine Datenpanne gemeldet und wie sollten die betroffenen Personen informiert werden?

<https://www.datenschutz-notizen.de/leitfaden-zum-umgang-mit-datenpannen-teil-1-1833273/>

<https://www.datenschutz-notizen.de/leitfaden-zum-umgang-mit-datenpannen-teil-2-1133293/>

## Datenschutzkonferenz empfiehlt die Corona- Warn- App als datenschutzfreundlichere Alternative zur Kontakterfassung

Unter dem Vorsitz des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Herrn Prof. Ulrich Kelber, wurden die grundrechtlichen Bedenken bei der Kontaktdatenerfassung in der Corona- Pandemie durch die Gesundheitsämter neu thematisiert.

<https://www.datenschutzticker.de/2022/02/datenschutzkonferenz-empfehl-die-corona-warn-app-als-datenschutzfreundlichere-alternative-zur-kontakterfassung/>

## Bericht des unabhängigen, interdisziplinären Beirats zum Beschäftigtendatenschutz

Am 17. Januar 2022 übergab der Beirat für den Beschäftigtendatenschutz zum Abschluss seiner Tätigkeit die nachfolgenden Thesen und Empfehlungen zur Fortentwicklung des Beschäftigtendatenschutzes an den Bundesminister für Arbeit und Soziales, Hubertus Heil.

[https://www.bmas.de/SharedDocs/Downloads/DE/Arbeitsrecht/ergebnisse-beirat-beschaefigtendatenschutz.pdf?\\_\\_blob=publicationFile&v=2](https://www.bmas.de/SharedDocs/Downloads/DE/Arbeitsrecht/ergebnisse-beirat-beschaefigtendatenschutz.pdf?__blob=publicationFile&v=2)