Rainer Knyrim
Rechtsanwalt und Partner bei Knyrim Trieb Rechtsanwälte

Nun auch Facebook Pixel und Login unzulässig?

Kurz nach dem Erscheinen des letzten Heftes hat die DSB eine möglicherweise folgenschwere Entscheidung getroffen: Sie stellte fest, dass im August 2020 auf der Website eines österr Unternehmens „Facebook Pixel" und ein „Facebook Login" unzulässig implementiert waren. Durch diese Facebook-Business-Tools wurden personenbezogene Daten des Bf (vertreten durch NOYB), nämlich Nutzer-Identifikations-Nummer, IP-Adresse und verschiedene Browser-Parameter, an Facebook in die USA übermittelt, obwohl das Unternehmen für diese Datenübermittlung kein angemessenes Schutzniveau gem Art 44 DSGVO gewährleistet hatte. Die DSB folgte inhaltlich ihrer Argumentationslinie aus der im Jänner 2022 publizierten *Google Analytics*-Entscheidung (s Dako 2022/13, 2022/55). Sie stellte fest, dass Facebook sich im August 2020 noch auf das vom EuGH bereits aufgehobene „Privacy Shield"-Übereinkommen für den Datentransfer in die USA gestützt hatte. Standarddatenschutzklauseln wurden von Facebook erst nach dem Tatzeitpunkt implementiert und es waren keine Ausnahmetatbestände nach Art 49 erfüllt (zB Einwilligung).

Es ist noch nicht endgültig geklärt, ob die mittlerweile von Facebook als Vertragszusatz implementierten Standarddatenschutzklauseln den Anforderungen der DSB genügen oder ob es möglich ist, einen Datentransfer auf eine transparente und informierte Einwilligung zu stützen. Die DSB hat weder die Standarddatenschutzklauseln inhaltlich geprüft, noch ob ausreichende zusätzliche Maßnahmen iSd *Schrems II*-Entscheidung und der EDSA-Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten implementiert waren.

Gerade Letzteres sollte daher geprüft werden, wenn der Datentransfer beim Einsatz von „Facebook Pixel" und „Facebook Login" (dieses heißt mittlerweile „Facebook Connect") auf Standarddatenschutzklauseln gestützt wird.

Die Entscheidung könnte weitreichende Konsequenzen für die Einsatzmöglichkeiten der Login-Tools für Webseiten und Apps haben, da auch bspw Google oder Apple solche Login-Möglichkeiten anbieten. Bei diesen ist daher ebenfalls zu prüfen, ob und welche Daten diese transferieren und wie ein Transfer abgesichert wird. Klar ist: Nach dieser Entscheidung können Unternehmen künftig Pixel- oder Login-Tools nicht mehr einfach ohne rechtliche Prüfung einsetzen.

Digitale Signatur – Erfolgsmodell in Österreich

Wie *Markus Vesely*, Co-Geschäftsführer von A-Trust, im Interview in diesem Heft ausführt, hat va der „Grüne Pass" wesentlich dazu beigetragen, Hemmschwellen gegenüber Signatur- und Zertifikatslösungen abzubauen, sodass sich die Zahl der Handy-Signatur User:Innen während der Pandemie verdoppelt hat. Bereits 3,2 Millionen nutzen die Handy-Signatur von A-Trust, weitere 460.000 die ID Austria. Täglich werden bis zu 350.000 Signaturen über A-Trust ausgelöst. Dies ist nicht nur eine gute Nachricht für die Digitalisierung, sondern vermutlich auch für den Klimaschutz, denn jede digitale Signatur ersetzt potentiell die Unterschrift auf einem ressourcenaufwendig erzeugten Papierdokument. Wir widmen der digitalen Signatur daher den Schwerpunkt dieses Heftes, in dem *Jan Hospes, Lisa Seidl* und *Andreas Czák* über Österreichs Identität, die ID Austria und die von ihnen dazu durchgeführte Datenschutz-Folgenabschätzung berichten. *Viktoria Haidinger* hat mehrere Fragen aus der Praxis zur ID Austria und zur digitalen Signatur zusammengestellt.

HinweisgeberInnenschutzgesetz in Kraft

Mit mehr als einem Jahr Verspätung wurde nun endlich am 24. 2. 2023 das HSchG publiziert (BGBl I 2023/6). Die Whistleblowing-Stellen müssen nun binnen sechs Monaten umgesetzt werden; Unternehmen mit weniger als 250 Beschäftigten haben bis 17. 12. 2023 Zeit. *Hans-Jürgen Pollirer* hat die Checkliste Whistleblowing aktualisiert; Sie können damit die verfügbaren Anbieter für Whistleblowing-Software sowie Ihre eigenen Strukturen prüfen. Beachten Sie insb die Antwortfristen, Geheimhaltungsverpflichtungen und Speicherfristen für Daten und Protokolle!

Herzlichst Ihr, *Rainer Knyrim*

Dako 2023/15

Rainer Knyrim/Reinhard Ebner
Rechtsanwalt und Partner bei Knyrim Trieb Rechtsanwälte/freier Journalist

Elektronische Identität für Personen und Unternehmen

Interview mit Markus Vesely, Geschäftsführer A-Trust. Der „Grüne Pass" hat zur Zeit der Corona-Pandemie wesentlich dazu beigetragen, Hemmschwellen gegenüber elektronischen Signatur- und Zertifikatslösungen abzubauen, meint Markus Vesely. Im Interview erläutert er den Weg vom elektronischen Führerschein zu einer europäischen digitalen Identität.

Datenschutz konkret: Corona sorgte in vielen Bereichen für einen Digitalisierungsschub. Gilt dies auch für die Nutzung elektronischer Signaturen und der digitalen Identität?

Markus Vesely: Ganz allgemein lässt sich sagen, dass sich die Zahl der Handy-Signatur-User:innen während der Pandemie, also in knapp zwei Jahren, verdoppelt hat. Wir liegen zurzeit bei mehr als 3,2 Millionen Personen, die diese Lösungen verwenden. Das ist eine hohe Quote im Vergleich zur Gesamtbevölkerung Österreichs – auch wenn man bedenkt, dass die Nutzung der Handy-Signatur erst ab 14 Jahren möglich ist.

Die Pandemie hat sicherlich dazu beigetragen, Hemmschwellen zu senken. Die Menschen haben gesehen, welche Vorteile es bringt, wenn man nicht immer aufs Amt laufen muss, sondern Dinge von zu Hause aus erledigen kann. Die „Killerapplikation", wenn man so will, war allerdings der „Grüne Pass". Dadurch hat sich die Akzeptanz, aber auch die Marktverbreitung der Lösungen im Bereich der elektronischen Identität wesentlich erhöht.

Datenschutz konkret: Wo steht Österreich damit im europäischen Vergleich?

Vesely: Bei der Umsetzung digitaler Verwaltungsservices liegt Österreich laut eGovernment-Benchmark 2022 europaweit gesehen im guten Mittelfeld. Im Bereich der Handy-Signatur oder der elektronischen Identität gehören wir neben Ländern wie Malta und Estland sogar zu den Spitzenreitern und sind in dieser Hinsicht auch wesentlich fortgeschrittener als bspw unser deutscher Nachbar. In anderen Bereichen wiederum zeigen gerade Malta und Estland, das durchaus noch Luft nach oben ist.

Datenschutz konkret: Womit wir beim Thema der elektronischen Signatur wären. Welche Arten der Signatur gibt es und was charakterisiert diese?

Vesely: Vereinfacht lassen sich drei Arten elektronischer Signaturen unterscheiden. Da wäre zum einen die **einfache elektronische Signatur (EES)**. Diese ist entsprechend unsicher: Es gibt keine Möglichkeit zur Identifizierung der unterzeichnenden Person bzw ist die Signatur nicht zwingend eindeutig einer Person zuzuordnen. Zudem lässt sich das Dokument nachträglich verändern.

Bei der **fortgeschrittenen elektronischen Signatur (FES)** ist Letzteres nicht mehr der Fall. Darüber hinaus ist eine Identitätsprüfung nach erfolgter Unterschrift möglich.

Die höchste Sicherheitsstufe stellt die **qualifizierte elektronische Signatur (QES)** dar. Der Unterschied im Vergleich zur FES: Hier bedarf es zusätzlich noch einer abgesicherten Signaturerstellungseinheit – zB mittels Hardware-Sicherheitsmodul (HSM) – und eines Überwachungs-Audits. Eine qualifizierte elektronische Signatur darf nur von einem sog Vertrauensdiensteanbieter bzw Trust Service Provider ausgegeben werden.

Sicher ist dabei nicht nur die Signaturerstellungseinheit, auch das zugrundeliegende Zertifikat muss von einem Vertrauensdiensteanbieter ausgegeben werden. A-Trust bietet drei Zertifikate an: die Handy-Signatur, ID Austria und xIDENTITY. Das letztgenannte Zertifikat steht auch jenen zur Verfügung, die ihren Wohnsitz nicht in Österreich haben.

Datenschutz konkret: Nicht nur Personen, auch Unternehmen können mittlerweile elektronisch signieren. Wie läuft das ab?

Vesely: Da ein Unternehmen als juristische Person nicht selbst handlungsfähig ist, wird dieses immer von natürlichen Personen, die für das Unternehmen in ihrer Funktion signieren, vertreten. Neben Handy-Signatur oder ID Austria, welche Zertifikate für natürliche Personen darstellen, können aber auch elektronische Firmensiegel erworben werden.

Dazu ist aber zu sagen, dass mit einem elektronischen Firmensiegel die berufenen Organe einer Firma, die ja auch im Firmenbuch eingetragen sind, nicht übergangen werden können. Ein Firmensiegel kann sozusagen nicht die Verantwortlichkeiten und Zuständigkeiten des Geschäftsführers oder eines Prokuristen übernehmen und hat daher für sich alleine keine Rechtsgültigkeit.

Außerdem können dabei auch Zertifikate anderer Trust Service Provider, welche bspw in Italien oder Spanien sitzen, zum Einsatz kommen. Weiters gibt es die sog Amtssignatur, mit der behördliche Dokumente die gleiche Legitimation erlangen wie eine öffentliche Urkunde.

Phishing-Attacken sind durch eine 2-Faktor-Authentifizierung praktisch ausgeschlossen.

Datenschutz konkret: Welchen Mehrwert bringen elektronische Signaturen und Siegel den Unternehmen – gerade auch im Hinblick auf Datenschutz und Datensicherheit?

Vesely: Ein Vorteil ist sicherlich, dass die Bearbeitung ohne Medienbrüche vor sich geht. Dh, es müssen keine Dokumente ausgedruckt und Unterschriften eingescannt werden oder dergleichen. Das spart nicht nur Zeit, sondern auch Ressourcen.

Handy-Signatur und ID Austria verlangen eine Zwei-Faktor-Authentifizierung, sei es durch einen ergänzenden Code, einen Fingerabdruckscan oder biometrische Gesichtserkennung des Smartphones. Klassische Phishing-Attacken sind damit praktisch ausgeschlossen.

Datenschutz konkret: Wie garantiert Ihr Unternehmen die Sicherheit und Zuverlässigkeit der zur Verfügung gestellten digitalen Signaturen?

Vesely: Als Vertrauensdiensteanbieter unterliegen wir strengen Kontrollen der Regulierungsbehörde RTR. Missbräuche sind unverzüglich zu melden. Damit es erst gar nicht dazu kommt, sind wir verpflichtet, alle zwei Jahre eine aufwendige Konformitätsbewertung durchzuführen. Damit sind mehrere Mitarbeiter:innen jeweils monatelang beschäftigt. Wir stehen auch kurz vor dem Abschluss einer ISO-27001-Zertifizierung, für die hohe Standards im Informationssicherheitsmanagement zu erfüllen sind.

Markus Vesely im Gespräch mit Rainer Knyrim © Eva Puella

Cybersecurity ist bei uns in der obersten Management-Ebene des Unternehmens angesiedelt und ausnahmslos alle Mitarbeitenden müssen dazu Online-Schulungen absolvieren. Ein externes Unternehmen überprüft zudem mit zu Testzwecken erstellten Phishing-Mails und Social-Engineering-Anrufen die Wirksamkeit unserer Maßnahmen.

Datenschutz konkret: Welche technische Infrastruktur nutzen Sie?
Vesely: Im Hintergrund steht ein privates Hochsicherheitsrechenzentrum mit Standort in Österreich. Alle Daten sind redundant an mehreren Standorten gespeichert – es werden also keine Webservices von internationalen Anbietern verwendet.

Im Endeffekt wird es eine europäische digitale Identität geben.

Datenschutz konkret: Wie wird sich die digitale Signatur der ID Austria aus Ihrer Sicht weiterentwickeln?
Vesely: Die eIDAS-Verordnung 2.0 wird zurzeit im EU-Parlament verhandelt. Damit wird auch eine Weiterentwicklung der ID Austria einhergehen. Als Vertrauensdiensteanbieter sind wir dabei einer der Stakeholder im Hintergrund, da wir das qualifizierte Zertifikat für die ID Austria liefern.

Im Endeffekt wird das – durch eine Nostrifizierung der Staaten untereinander – eine europäische digitale Identität. Mit der gleichen digitalen EU-Identität soll zB die Ummeldung des Wohnsitzes oder auch die Beantragung einer Familienbeihilfe überall innerhalb der EU möglich sein. In die digitale Identität sollen darüber hinaus qualifizierte Attribute – bspw ein Universitätsabschluss – einfließen können. Das kann etwa für Bewerbungen nützlich sein.

Datenschutz konkret: Welche Schwerpunkte sehen Sie künftig bei der Nutzung der ID Austria?
Vesely: Mit dem elektronischen Führerschein ist die ID Austria erstmals für eine breite Bevölkerungsschicht relevant. Die nächsten Schritte sind wahrscheinlich der Altersnachweis und der digitale Zulassungsschein. Schon jetzt gibt es eine Ausweisplattform als ergänzende Smartphone-App zum Download. Diese wird nach und nach mit digitalen Ausweisen bestückt werden.

Datenschutz konkret: Mit welchen Unternehmen und Organisationen kooperieren Sie, um die Akzeptanz und Verwendung digitaler Signaturen zu fördern?
Vesely: Um die qualifizierte elektronische Signatur weiter zu etablieren, arbeiten wir schon jetzt mit Anbietern von Signaturplattformen wie Adobe Sign, DocuSign und MOXIS zusammen. Unsere Schnittstelle wird dabei direkt integriert, wodurch User:innen für die Nutzung die jeweilige Plattform nicht verlassen müssen. Ein Kauf- oder Dienstvertrag kann zB auch direkt in einem bestehenden Dokumentenmanagementsystem unterschrieben werden, denn auch dafür bieten wir Lösungen an. Das kann besonders für größere Unternehmen interessant sein, die unsere Zertifikate lückenlos in ihr gesamtes ERP-System einbinden wollen.

Unsere sog Signatur-Box bietet zudem die Möglichkeit, unsere Schnittstelle entsprechend zu integrieren, ohne dass die zu signierenden Dokumente das Unternehmen dafür verlassen müssen, was va bei hochsensiblen Daten notwendig ist.

Datenschutz konkret: Wie kommt man nun zu einer elektronischen Signatur oder zu einem Firmensiegel?
Vesely: Für die Handy-Signatur gibt es derzeit noch viele Registrierungsstellen – Magistrate, Bezirksämter, Sozialversicherungsanstalten und viele mehr. Die ID Austria darf gegenwärtig nur von Pass- und Finanzämtern ausgegeben werden.

Das ebenfalls qualifizierte Zertifikat xIDENTITY kann direkt über unser Unternehmen oder über einen von uns ausgebildeten „Registration Officer" erlangt werden. Alternativ kann die Authentifizierung bspw über Video-Ident-Verfahren, also ein Videotelefonat, oder auch über ein neues Robo-Ident-Verfahren erfolgen. Im eGovernment ist xIDENTITY zwar nicht gültig, aber damit lässt sich im gesamten europäischen Wirtschaftsraum qualifiziert und somit rechtssicher unterschreiben.

Dako 2023/16

Zum Thema

Über den Interviewpartner

Ing. Dr. Markus Vesely ist Co-Geschäftsführer von A-Trust. Seine Hauptagenden liegen im Bereich des Vertriebs und der Technik. Bis 2020 war der WU-Absolvent als Vertriebsleiter für Zentral- und Osteuropa bei Rohde & Schwarz tätig. Davor war er ua im Bereich Forschung und Entwicklung bei der Frequentis AG beschäftigt.
E-Mail: markus.vesely@a-trust.at

Factbox A-Trust

A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH wurde im Jahr 2000 gegründet und zählt mittlerweile 34 Mitarbeitende. Über drei Millionen Menschen nutzen die Handy-Signatur von A-Trust, weitere 460.000 Personen die ID Austria: So werden täglich zwischen 200.000 und 350.000 Signaturen über A-Trust ausgelöst. A-Trust wirkt in enger Zusammenarbeit mit den Ministerien an der Digitalisierung Österreichs mit.

Barbara Wagner
BAWAG Group AG

Beauskunftung der konkreten Empfänger – Praktische Umsetzung

Identifikation; Auftragsverarbeiter; offenkundig unbegründeter und exzessiver Antrag; Betriebs- und Geschäftsgeheimnis. Der EuGH stellte in der Entscheidung C-154/21, *Österreichische Post*, fest, dass das Recht auf Auskunft auch die Bekanntgabe der konkreten Empfänger umfasst. Der Beitrag zeigt Fälle, in denen die Identifikation der Empfänger nicht möglich ist, und gibt Tipps für die Umsetzung der Vorgaben des EuGH in die Praxis.

EuGH-Entscheidung

Art 15 DSGVO regelt das Auskunftsrecht des Betroffenen. Gem Art 15 Abs 1 lit c DSGVO hat diese folgende Informationen zu enthalten: *„Die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden"*. Strittig war, ob der Verantwortliche entscheiden kann, was er beauskunftet: die Kategorien der Empfänger oder die konkreten Empfänger. Der OGH legte diese Frage dem EuGH im Wege eines Vorabentscheidungsverfahrens zur Klärung vor.

Der EuGH stellte in der Entscheidung vom 12. 1. 2023, C-154/21, fest, dass das Recht auf Auskunft auch die **Bekanntgabe** der **konkreten Empfänger** umfasst, denen personenbezogene Daten offengelegt wurden oder noch werden.

Der EuGH hält fest, dass dieses Auskunftsrecht der betroffenen Person erforderlich ist, um ihr die Ausübung anderer Rechte zu ermöglichen. Damit soll sichergestellt werden, dass Personen ihr Recht auf Berichtigung, Löschung, Einschränkung der Verarbeitung und Widerspruch ausüben oder im Schadensfall gerichtliche Rechtsbehelfe einlegen können. Um diese Rechte geltend machen zu können, müssen die Angaben zu Empfängern möglichst genau sein. Daher besteht ein Anspruch auf Bekanntgabe der Identität der konkreten Empfänger. Die Empfänger **müssen nicht genannt werden**, wenn der Antrag offenkundig unbegründet oder exzessiv ist oder es nicht möglich ist, sie zu identifizieren, etwa weil sie noch gar nicht bekannt sind. Dann reicht es aus, die Empfängerkategorien anzugeben.

Fehlende Möglichkeit zur Identifikation

In der Entscheidung hält der EuGH fest, dass es unter bestimmten Umständen nicht möglich ist, Informationen über konkrete Empfänger zu erteilen, insb wenn diese noch nicht bekannt sind. Leider führt der EuGH zu dem Thema nichts Näheres aus. Ein Hauptanwendungsfall könnten frühere **Empfänger** sein, die der Verantwortliche **nicht mehr identifizieren** kann.[1]

Zur Vertragserfüllung ziehen Unternehmen eine Vielzahl an Auftragsverarbeitern (insb im Bereich der IT) heran. Dabei kommt es laufend zu Änderungen der Auftragsverarbeiter. Gerade in Unternehmen mit langjährigen Kundenbeziehungen (wie bei Banken, Versicherungen) kann es im Laufe der Zeit zu vielfachen **Wechseln bei Auftragsverarbeitern** kommen. Wichtig ist idZ, dass es nach Beendigung der Auftragsverarbeitung in der Regel zur **Löschung** der **Daten beim Auftragsverarbeiter** kommt.

Für den Verantwortlichen ist in so einem Fall nicht mehr nachvollzichbar, an welche früheren Auftragsverarbeiter die spezifischen Kundendaten weitergegeben wurden. Die Empfänger können daher nicht identifiziert und beauskunftet werden. Nachdem diese aber keine Daten mehr speichern, besteht auch keine Notwendigkeit zur Auskunftserteilung. Der Zweck der Auskunft über konkrete Empfänger ist die Möglichkeit zur Ausübung anderer Rechte, wie jene zu Löschung und Berichtigung, welche mangels gespeicherter Daten ins Leere gehen würden.

Dasselbe Thema gibt es beim **Zugriff auf Daten** in den IT-Systemen des Verantwortlichen **durch Dritte**. Diesen Dritten wurden Daten offengelegt. Geloggte Zugriffe auf die Daten werden nicht unbegrenzt gespeichert. Nach Löschung der Logdateien kann nicht mehr festgestellt werden, dass der Dritte auf die Daten zugegriffen hat.

Beispiele aus dem Alltag einer Bank:

- **Überweisungsbelege** sind undeutlich ausgefüllt und können nicht automatisch gebucht werden. Eine menschliche Überprüfung ist notwendig. Ein Teil der Überprüfungen wird von Mitarbeitern der Bank, ein Teil durch einen Auftragsverarbeiter, der Zugriff auf das IT-System der Bank hat, durchgeführt.
- Die Bank betreibt ein Archivsystem für **Kontoauszüge**. Kunden fordern speziell aufbereitete Auszüge an. Ein Auftragsverarbeiter übernimmt die Aufbereitung und arbeitet dafür im Archivsystem der Bank.
- In einem **IT-System** gibt es Probleme. Ein Dritter greift zur Fehlerbehebung auf das IT-System des Verantwortlichen zu, wobei es zur Offenlegung von Kundendaten kommt.

Der Zugriff auf die Systeme des Verantwortlichen wird in allen Fällen geloggt. Die Logdateien werden nach einiger Zeit gelöscht. Eine Auskunft über die konkreten Empfänger der Offenlegung ist nicht möglich.

Auftragsverarbeiter

Auch Auftragsverarbeiter zählen zu den Empfängern und werden idR konkret beauskunftet. Der EuGH begründet das Recht der Nennung konkreter Empfänger damit, dass dort die Betroffenenrechte wie Recht auf Auskunft, Berichtigung und Löschung geltend gemacht werden können. Im Fall einer Auftragsverarbeitung werden die Betroffenenrechte an den Verantwortlichen gerichtet. Eine Bekanntgabe konkreter Empfänger kann daher der Transparenz dienen, führt aber nicht dazu, dass Auftragsverarbeiter Anfragen Betroffener beantworten. Werden Anfragen zu Betroffenenrechten an Auftragsverarbeiter gerichtet, senden diese sie an den Verantwortlichen zur Beantwortung weiter. Daher wäre eine Auskunft über die konkreten Auftragsverarbeiter für die Rechtsdurchsetzung nicht erforderlich.

Offenkundig unbegründeter und exzessiver Antrag

Lehnt der Verantwortliche eine Auskunft über konkrete Empfänger ab, muss er gem

[1] Zur fehlenden Protokollierungspflicht Böszörmenyi, Eine kritische Auseinandersetzung mit EuGH C-154/21, *Österreichische Post*, Dako 2023/19, in diesem Heft Seite 32.

Art 12 Abs 5 DSGVO nachweisen, warum der Antrag offenkundig unbegründet oder exzessiv ist. Das Exzessive muss sich nicht pauschal auf die gesamte Auskunftsanfrage beziehen. Der EuGH stellt fest, dass auch einzelne Aspekte einer Auskunftsanfrage wie ein Verlangen aller konkreten Empfänger exzessiv sein können. Bisher war das typische Beispiel für exzessive Anfragen ein Betroffener, der laufend Auskunftsersuchen an denselben Verantwortlichen stellt. Leider führt die Entscheidung nicht aus, was exzessiv iZm Empfängern bedeutet.

Nach Beantwortung der Frage durch den EuGH muss nun der OGH seine Entscheidung treffen. Es bleibt zu hoffen, dass der OGH eine Aussage zur **Auslegung von „exzessiv"** trifft.[2]

Der *EDSA* arbeitet derzeit an der Finalisierung der Richtlinien zur Auskunft. Es wäre zu begrüßen, wenn die Frage der Auslegung des Begriffes „exzessiv" im Rahmen der Richtlinien umfassender als in der Version 1.0[3] beantwortet würde.[4]

Behörden als Empfänger

In Art 4 Z 9 DSGVO wird definiert, wann Behörden als Empfänger anzusehen sind. Nicht zu den Empfängern zählen demnach: *„Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der MS möglicherweise personenbezogene Daten erhalten"*. Wenn der Verantwortliche Daten an solche Behörden weitergegeben hat, müssen diese nicht bei den Empfängern aufgelistet werden. Dabei ist zu beachten, dass es sich nur um Behörden handelt, **die im Einzelfall** (bei einem bestimmten Untersuchungsauftrag) Daten erhalten. Das können zB Steuer- und Zollbehörden, Finanzermittlungsstellen, unabhängige Verwaltungsbehörden oder Finanzmarktbehörden sein.

Die Ausnahme gilt jedoch nicht für **regelmäßige Übermittlungen von Daten an Behörden.** Ein Beispiel dafür sind etwa die laufenden Meldungen von Kontostammdaten in das beim BMF geführte Kontenregister durch Kreditinstitute. Hier ist das BMF im Rahmen einer Auskunft als konkreter Empfänger anzuführen.

Betriebs- und Geschäftsgeheimnis

Sollte die Auskunft über einzelne Empfänger das Geschäfts- oder Betriebsgeheimnis des Verantwortlichen oder eines Dritten gefährden, kann die Auskunftserteilung in der Regel gem § 4 Abs 6 DSG unterbleiben.

Auch ErwGr 63 DSGVO behandelt das Thema Geschäftsgeheimnis: *„Dieses Recht sollte die Rechte und Freiheiten anderer Personen, etwa Geschäftsgeheimnisse oder Rechte des geistigen Eigentums und insb das Urheberrecht an Software, nicht beeinträchtigen. Dies darf jedoch nicht dazu führen, dass der betroffenen Person jegliche Auskunft verweigert wird."*

Die obigen Regelungen können nicht verwendet werden, um generell die Auskunft zu verweigern. Es müssen tatsächliche Gründe vorliegen, die eine Auskunftserteilung über (einzelne) Empfänger verhindern.

Umsetzung der Vorgaben des EuGH in der Praxis

Erstellen Sie eine Liste konkreter Empfänger

PRAXISTIPP

Hier finden Sie mögliche Quellen, die Ihnen beim Erstellen der Liste helfen können:

- **Vertragsdatenbank, Einkaufsabteilung;**
- **IT-Bereich;**
- **Buchhaltung;**
- **Verzeichnis der Verarbeitungstätigkeiten;**
- **Informationsblatt gem Art 13 und 14 DSGVO;**
- **interne Stellen fürs Meldewesen;**
- **Mahnwesen, Rechtsfallbearbeitung;**
- **Leiter der operativen Prozesse im Unternehmen.**

Bitte vergessen Sie nicht auf folgende, mögliche Empfänger:

- Aufsichtsbehörden oder Meldestellen;
- ausgelagerte Rechenzentren, IT-Archive, E-Mail-Systeme, digitale Signaturen;
- Auskunfteien wie KSV und CRIF;
- Banken oder Zahlungsverkehrsdienstleister;
- Buchhaltung, Steuerberatung;
- Call Center;
- Cookies und Tracking;
- Dienstgeber/Sicherheitengeber bei Verpfändungen und Abtretungen;
- Druckdienstleister;
- Inkasso, Anwälte zur Rechtsfallbetreibung;
- Konzerngesellschaften (als Auftragsverarbeiter, bei Datenweitergabe aus regulatorischen Gründen oder zu Marketingzwecken);
- Kooperationspartner, Vermittler, Provisionsempfänger;
- Kundenbindungsprogramme;
- Marketing und Marktforschung;
- öffentliche Register;
- Post;
- Telefonaufzeichnung, Videoüberwachung;
- Telekom und Unternehmen, die SMS (mit Passwörtern) verschicken;
- Versicherungen.

HINWEIS

Bitte vergessen Sie nicht, dass neben Kunden auch alle anderen Betroffenen, wie Mitarbeiter und Geschäftspartner, Anspruch auf eine Aufstellung der konkreten Empfänger haben.

Konkreter Empfänger bekannt – Daten beim Empfänger gelöscht

In vielen Fällen werden Daten an Empfänger übermittelt, um einen Auftrag zu erfüllen. Die übermittelten Daten werden dann beim Empfänger gelöscht. Eine Rechtsdurchsetzung beim Empfänger geht ins Leere. Solche Empfänger sollten nicht angeführt werden müssen. Beispiele:

- Ein Unternehmen übermittelt Daten an ein Marktforschungsinstitut, damit dieses Interviews mit Kunden führt. Das Ergebnis der Kundenbefragung wird an das Unternehmen rückübermittelt. Das Marktforschungsinstitut löscht alle Daten.
- Eine Druckerei erhält Kundendaten. Nach dem Drucken der Dokumente werden die Daten vernichtet.

Konkreter Empfänger bekannt – konkrete Daten unbekannt

Ein Dritter hat Zugriff auf das IT-System des Verantwortlichen. Er arbeitet in dessen Infrastruktur. Die Protokolle der Zugriffe werden nach einiger Zeit gelöscht. Wegen Löschung der Protokolle ist nicht mehr bekannt, auf welche Daten der Dritte zugegriffen hat. Daher ist nicht feststellbar, ob Daten an den Dritten offengelegt wurden. Die Bekanntgabe der konkreten Dritten ist möglich.

Maßgeschneiderte Auskunft: Tatsächlich jeder Empfänger?

Im Rahmen der Bearbeitung konkreter Auskunftsanträge stellte sich bei einigen

[2] Anmerkung der Redaktion: Nach Redaktionsschluss wurde die Sache zur Vermeidung einer ÜberraschungsE an das Erstgericht zurückverwiesen – OGH 17. 2. 2023, 6 Ob 20/23v. [3] EDSA, Guidelines 01/2022 on data subject rights – Right of Access, Version 1.0. [4] Siehe Leitinger, Und täglich grüßt das Auskunftsrecht, Dako 2022/47 (85).

Konstellationen die Frage, inwieweit die Bekanntgabe bestimmter Empfänger überhaupt notwendig ist, damit der Kunde seine Rechte durchsetzen kann. Die DSGVO kennt eine Mitwirkungspflicht bei Verarbeitung großer Mengen von Informationen. ErwGr 63 DSGVO hält dazu Folgendes fest: *„Verarbeitet der Verantwortliche eine große Menge von Informationen über die betroffene Person, so sollte er verlangen können, dass die betroffene Person präzisiert, auf welche Information oder welche Verarbeitungsvorgänge sich ihr Auskunftsersuchen bezieht, bevor er ihr Auskunft erteilt."*

PRAXISTIPP

Umgang mit Kundenanfragen: Fragen Sie nach, welche Empfänger den Kunden tatsächlich interessieren. Die Erfahrung zeigt, dass oftmals nur Informationen zu bestimmten Empfängern benötigt werden („Wer hat negative Daten von mir erhalten?", „Welche öffentlichen Stellen erhalten eine Auflistung meiner Konten?", „An welche Konzerngesellschaften haben Sie meine Daten weitergegeben?", „Welche Meinungsforscher haben meine Daten?"). Eine Übermittlung der tatsächlich benötigten Empfänger trägt zur Kundenzufriedenheit bei. Eine Übermittlung aller Empfänger inkl IT-Dienstleister und Auftragsverarbeiter beantwortet idR nicht die Kundenfrage.

Fazit

Es bleibt zu hoffen, dass die Entscheidung im Rahmen der Guidelines zur Auskunft oder durch weitere EuGH-Entscheidungen konkretisiert wird. Es sollte diskutiert werden, ob tatsächlich alle Empfänger konkret anzuführen sind. Bestimmte Empfänger wie konkrete Auftragsverarbeiter sollten im Rahmen künftiger Rechtsprechung von der Auskunft ausgenommen werden. Die Auskunft über konkrete Auftragsverarbeiter ist für die Rechtsdurchsetzung nicht erforderlich, führt aber zu einem hohen Mehraufwand bei Unternehmen.

Dako 2023/17

Zum Thema

Über die Autorin

MMag. Barbara Wagner ist Konzern-Datenschutzbeauftragte in der BAWAG Group AG.
E-Mail: Barbara.Wagner@bawaggroup.com

Hinweis

Zur EuGH-E *Österreichische Post* siehe *Böszörmenyi*, Eine kritische Auseinandersetzung mit EuGH C-154/21, *Österreichische Post*, Dako 2023/19, in diesem Heft Seite 32.

Jan Hospes/Lisa Seidl/Andreas Czák
Research Institute – Digital Human Rights Center

Österreichs elektronische Identität

E-ID; ID Austria; elektronische Signatur; digitaler Führerschein. Die ID Austria ersetzt die Handy-Signatur. Eine Schlüsselfunktion der ID Austria wurde mit der Einführung der Ausweisplattform geschaffen. Das Research Institute – Digital Human Rights Center hat dazu eine Datenschutz-Folgeabschätzung im Auftrag des BMDW durchgeführt. Die wesentlichen Erkenntnisse dieser Arbeit werden in aller Kürze dargestellt.

Die ID Austria ist die österr Umsetzung eines elektronischen Identitätsnachweises (E-ID). Gem § 2 Z 10 E-GovG ist dieser eine logische Einheit, die eine qualifizierte elektronische Signatur mit einer Personenbindung und den zugehörigen Sicherheitsdaten und -funktionen verbindet. Sie kann als Weiterentwicklung von Handy-Signatur und Bürgerkarte bezeichnet werden und steht allen Bürger*innen in der App „Digitales Amt" zur Verfügung. Im behördlichen Umfeld wird daher die Handy-Signatur durch die ID Austria vollständig ersetzt. Eine Schlüsselfunktion der ID Austria wurde mit der Einführung der Ausweisplattform geschaffen. Diese bietet auf Basis der ID Austria eine Plattform zur Nutzung des digitalen Führerscheins und zukünftig auch anderer digitaler Ausweisdokumente in verschiedenen behördlichen wie privatwirtschaftlichen Zusammenhängen. Bereits in der Entwicklung der Anwendungen und Systeme wurden intensive datenschutzrechtliche Überlegungen angestellt, um eine möglichst datenschutzfreundliche Architektur herzustellen. Research Institute – Digital Human Rights Center hat zu den genannten Systemen durchgeführte Datenschutz-Folgenabschätzungen im Auftrag des Bundesministeriums für Digitalisierung und Wirtschaftsstandort (BMDW)[1] intensiv begleitet und ausführliche Berichte über die Ergebnisse erstellt.[2, 3] Die wesentlichen Erkenntnisse dieser Arbeit sollen hier in aller Kürze dargestellt werden.

Einordnung und Voraussetzungen der ID Austria

Wesentliche datenschutzrechtliche Weichenstellungen für die Ausgestaltung der ID Austria und der Ausweisplattform werden durch den nationalen Gesetzgeber determiniert. Elektronische Identitätsnachweise sind gem § 2 Z 10 **E-GovG**[4] als personenbezogenes Datum iSv Art 4 Z 1 DSGVO[5] zu qualifizieren und in §§ 4 ff E-GovG werden die Rechtsgrundlagen für die Datenverarbei-

[1] Während der Beauftragung kam es zu einem Übergang der relevanten Zuständigkeit vom BMDW hin zum Bundesministerium für Finanzen (BMF). Siehe Anl § 2 BMG; s www.bmf.gv.at/ministerium/aufgaben-und-organisation/Stammzahlenregisterbehoerde (Stand aller Links 3. 3. 2023). [2] Tschohl et al, ID Austria Datenschutz-Folgenabschätzung (2022); www.oesterreich.gv.at/dam/jcr:75b866bb-3735-4571-b859-39df84e2a281/DSFA_IDAUSTRIA_BMDW.pdf. [3] Tschohl et al, Digitaler Führerschein Datenschutz-Folgenabschätzung (2022); www.oesterreich.gv.at/dam/jcr:272fc1f7-1a2e-451e-8a19-98e6ba137843/DSFA-Bericht%20Digitaler%20F%C3%BChrerschein.pdf. [4] BG über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz – E-GovG), BGBl I 2004/10 idF BGBl I 2022/119. [5] VO (EU) 2016/679 des EP und des Rates vom 27. 4. 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der RL 95/46/EG (DSGVO), ABl L 2016/119, 1.

tung gestellt. Die Anbindung des digitalen Führerscheins ist im **FSG** geregelt.[6]

Voraussetzung für die Nutzung dieser Dienste ist die elektronische Signatur. Eine qualifizierte elektronische Signatur dient dem Zweck der **Zuordnung eines Dokuments zu einer spezifischen Person**, wie bei der eigenhändigen Unterschrift, und erfüllt das rechtliche Erfordernis der Schriftlichkeit iSd § 886 ABGB.[7] Der **Beweiswert** der elektronischen Signatur ist grundsätzlich jedoch faktisch höher als jener einer händischen Unterschrift, weil durch die Verifikationsmechanismen das Abstreiten der Authentizität der digitalen Signatur in der Praxis viel schwerer fallen wird. Im Gegensatz zur physischen Unterschrift ist neben der Vermutung der Authentizität auch die Vermutung der Integrität impliziert.

Betreiber*innen von Anwendungen, welche an die Infrastruktur der ID Austria andocken möchten, unterliegen im Akkreditierungsprozess gem § 18 Abs 2 E-GovG datenschutzrechtlichen Überprüfungen. Durch die vorgeschlagenen Anpassungen der eIDAS-VO[8] – welche die elektronische Identität auf europäischer Ebene regelt – steht die Einführung einer Self Sovereign Identity (SSI) im Raum. Kerngedanke dieses Konzepts der selbstbestimmten digitalen Identität ist, den E-ID ohne eine zentrale vermittelnde Instanz zu erzeugen.

Privacy by Design

Die Berücksichtigung von „Privacy by Design" (also Datenschutz durch Technikgestaltung iSd Art 25 DSGVO) und Datenminimierung wurde maßgeblich umgesetzt, indem ausschließlich eine selektive Übermittlung von Personenmerkmalen an berechtigte Anwendungen durchgeführt wird. Einen **besonderen Schutz** erfährt bei der ID Austria die **Stammzahl** von Bürger*innen, die als Basis für die Berechnung der zum Einsatz kommenden sektorspezifischen Identifikatoren fungiert. Es ist hervorzuheben, dass bereits in der grundlegenden Gestaltung des Systems Rücksicht darauf genommen wurde, dass es in späterer Folge möglich sein sollte, Ausweise vollständig offline vorzuweisen, was beim digitalen Führerschein auch faktisch umgesetzt werden konnte.

Die ID Austria setzt zum Schutz personenbezogener Daten stark auf **Pseudonymisierung**. Die zwei wesentlichen Identifikatoren, nämlich die Stammzahl (SZ) und das bereichsspezifische Personenkennzeichen (bPK), werden durch die Anwendung von Verschlüsselungsverfahren erzeugt, um so zum Schutz personenbezogener Daten innerhalb der betreffenden Verarbeitungstätigkeiten der ID Austria beizutragen.

Die Suche nach den Verantwortlichen

Sowohl die ID Austria als auch die Ausweisplattform bargen unerwartete Herausforderungen im Themenkomplex der datenschutzrechtlichen **Rollenverteilung**. Va im Hinblick auf die Rolle des bzw der Verantwortlichen kommt in Zusammenschau mit dem E-GovG zunächst der sog rechtlichen Verantwortlichkeit maßgebliche Bedeutung zu. Sich auf den gesetzlichen Festlegungen „auszuruhen", war allerdings unzureichend, vielmehr waren auch funktionelle Aspekte, welche die charakteristische Entscheidungsfunktion als faktisches Element des Verantwortlichen spiegeln, in die Beurteilung einzubeziehen. In enger Zusammenarbeit mit den Systementwickler*innen wurden diese Elemente sorgfältig untersucht und eingeordnet. Da die Systeme intensiven Datenaustausch befördern, könnten in weiterer Folge gemeinsame Verantwortlichkeiten erblickt werden. Dieser erste Anschein erwies sich bei näherer Betrachtung als unzutreffend, da gerade die gesetzlichen Maßgaben präzise Zuständigkeiten zuweisen. Die strenge und gezielte technische Umsetzung der gesetzlichen Vorgaben führt im Ergebnis zu **mehreren Einzelverantwortlichkeiten** und Auftragsverarbeitungen.

Methodik zur Risikobeurteilung

Die Risikobeurteilung gilt als Herzstück der Datenschutz-Folgenabschätzung.[9] Allerdings definiert die DSGVO weder ausdrücklich den Terminus „Risiko" noch gibt sie Aufschluss über die zu verwendende Methodik. Die verwendete Methodik basiert auf der **Risk Management ISO-Norm 31000:2018**, welche in einer umfassenden Umschau angereichert wurde.

Neu ist die Einführung einer Kommentierung der Risikoanalyseklassen.

Eine wichtige Neuerung ist die Einführung einer Kommentierung der Risikoanalyseklassen, die Aufschluss über die Gründe für die Einstufung der Risiken gibt. Einige der qualifizierten Risiken – etwa das Risiko einer rechtswidrigen Verarbeitung der Identitätsdaten oder Protokolldaten – können potenziell zu Diskriminierung und Ungleichbehandlung führen, weshalb die Datenschutz-Folgenabschätzung als „lebendiger Prozess" verstanden werden muss und gesamtgesellschaftliche Auswirkungen der Anwendungen weiterhin zu verfolgen sind.

Protokollieren oder nicht protokollieren?

Sowohl bei der ID Austria als auch beim digitalen Führerschein erforderte die Erstellung eines Protokollierungskonzepts viel Fingerspitzengefühl und Tiefgang, wobei Interessen und Risiken untereinander abzuwägen waren. Eine verhältnismäßige Protokollierung wurde aus Gründen der Rechenschafts- und Nachweispflicht gem DSGVO[10] bzw aufgrund von Anforderungen an die Daten- und IT-Sicherheit implementiert. Jedoch gilt nach der DSGVO der Grundsatz der **Datenminimierung** (Art 5 Abs 1c DSGVO), wonach personenbezogene Daten *„auf das für die Verarbeitung notwendige Maß beschränkt sein"* müssen.

Die ID Austria protokolliert zum Zweck der Nachkontrolle von Verarbeitungsvorgängen (etwa bei Identitätsdiebstahl) und der Sicherstellung der Transparenz der Verarbeitung bestimmte Datenarten. Als Maßnahmen zur **Absicherung der Protokolldaten** wurden stringente Pseudonymisierungs- und Löschfristen etabliert und Umfang sowie Speicherdauer auf ein Minimum beschränkt. Im System Ausweisplattform konnte auf personenbezogene Protokollierung verzichtet werden. Die zur Erfüllung der Rechenschaftspflicht benötigten Nachweise können mit dem Systemzustand oder per Verweis auf Protokolle der ID Austria oder des Führerscheinregisters hergestellt werden. In beiden Fällen wurde die Protokollierung im Zuge der Risikoanalyse genau beleuchtet, um etwaige Risiken aufzuzeigen, ihr Eintreten abzuschätzen und ihnen zu begegnen.

[6] §§ 14, 15a, 16a, 39 BG über den Führerschein (Führerscheingesetz – FSG), BGBl I 1997/120. [7] § 4 BG über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen, BGBl 2016/50; *Haglmüller*, Elektronische Signatur, in RDB Keywords[1] (Stand 11. 10. 2021, rdb.at). [8] Vorschlag für eine VO des EP und des Rats zur Änderung der VO (EU) 910/2012 im Hinblick auf die Schaffung eines Rahmens für die europäische digitale Identität, COM (2021) 281 fin 2021/0136 (COD), zur angesprochenen Evaluierung s 1f. [9] *Sachs*, Die Datenschutz-Folgenabschätzung, BVD Verbandstage 2019. [10] Ausf *Kastelitz/Gamper*, Verarbeitung von Protokolldaten: datenschutzrechtliches „Must-have", „Nice-to-Have" oder „No-go"? jusIT 2022/60, 151.

State of the Art

Die Bedeutung der digitalen Signatur kann insb vor dem Hintergrund der Pandemie-Erfahrungen nicht zu geringgeschätzt werden und ihr Einsatz bildet einen wichtigen Grundpfeiler des Rechts auf Teilhabe am elektronischen Rechtsverkehr (§ 1a E-GovG). Bereits für die erste Auflage der ID Austria war es essenziell, datenschutzrechtliche Grundsätze, wie die Integrität und Vertraulichkeit der Daten, in besonderem Maße umzusetzen.[11] Allerdings müssen insb in Bezug auf die technische Weiterentwicklung, aber auch aufgrund von veränderten EU-Vorgaben regelmäßige **Evaluierungen** bzw Anpassungen sichergestellt werden. Besonders die mit der starken Beweiskraft der elektronischen Signatur einhergehende allgemeine **Risikoerhöhung** (man denke an Identitätsdiebstahl) ist zu bedenken.

Insgesamt ist festzustellen, dass sich die Datenschutz-Folgenabschätzung als Instrument zur Wahrung hoher datenschutzrechtlicher Standards bewährt hat. Das zeigt sich vordergründig an der intakten Wechselwirkung zwischen der Durchführung der gegenständlichen Folgenabschätzungen und der Ergreifung von – hier nur angeschnittenen – technischen und organisatorischen Maßnahmen in den beleuchteten Systemen.

Dako 2023/18

[11] Beleg für eine durchaus geglückte Umsetzung der elektronischen Identität ist die Honorierung der ID Austria beim eGovernment-Wettbewerb in Berlin; www.brz.gv.at/read_it/flip-book-ausgabe-03-2022.html S 13.

Zum Thema

Über die Autor*innen

Mag. iur. Jan Hospes ist Jurist mit Spezialisierung auf IT-Recht. Er ist als Researcher und Consultant am Research Institute – Digital Human Rights Center tätig.
Lisa Seidl, LL.M., ist Juristin mit Spezialisierung auf Grund- und Menschenrechte. Sie ist als Researcher und Consultant am Research Institute – Digital Human Rights Center tätig.
Dipl.-Ing. Andreas Czák, BSc, ist Wirtschaftsinformatiker mit Spezialisierung auf Datenschutz und Transparenz. Er ist in der Öffentlichkeitsarbeit für das Research Institute – Digital Human Rights Center tätig. E-Mail: kontakt@researchinstitute.at

Links

DSFA ID Austria: https://researchinstitute.at/veroeffentlichung-des-berichts-zur-id-austria-datenschutz-folgenabschaetzung/
DSFA-Ausweisplattform: https://researchinstitute.at/bericht-ueber-die-datenschutz-folgenabschaetzung-zum-digitalen-fuehrerschein-veroeffentlicht/

Janos Böszörmenyi
Rechtsanwalt bei der Schönherr Rechtsanwälte GmbH

Eine kritische Auseinandersetzung mit EuGH C-154/21, *Österreichische Post*

Empfängerkategorien; Wahlrecht; Verhältnismäßigkeit. Der EuGH entschied am 12. 1. 2023, C-154/21, *Österreichische Post*, dass Betroffene Auskunft über konkrete Empfänger ihrer personenbezogenen Daten verlangen dürfen. Ausnahmen hiervon sah der EuGH nur vor, wenn die Feststellung der Identität der Datenempfänger unmöglich ist und wenn das Auskunftsersuchen offenkundig unbegründet oder exzessiv ist.

Wahlrecht des Betroffenen

Betroffene haben ein Recht auf Auskunft über die Empfänger **oder** Empfängerkategorien ihrer Daten (Art 15 Abs 1 lit c DSGVO). Der EuGH hatte zum Beantworten einer Vorlagefrage des OGH[1] über die Reichweite dieses Rechts zu entscheiden.

Kern des Rechtsstreits war, wie das Bindewort „oder" auszulegen ist. Aus diesem „oder" ist nach einer Auffassung ein **Wahlrecht des Betroffenen**, nach anderer Auffassung ein **Wahlrecht des Verantwortlichen** abzuleiten. Nach dem EuGH lässt sich dieser Rechtsstreit anhand des Wortlauts nicht klären,[2] dennoch stehe das Wahlrecht dem Betroffenen zu. Das Urteil des EuGH ist zu akzeptieren, aber auch zu kritisieren:

- **ErwGr 63:**

Der EuGH meint, ErwGr 63 DSGVO sehe keine Einschränkung des Auskunftsrechts auf Empfängerkategorien vor, deswegen komme das Wahlrecht dem Betroffenen zu.[3] Was ein unverbindlicher ErwGr vorsieht, kann aber nicht entscheidend sein. Eine normative Anordnung darf nicht durch Verweis auf einen unverbindlichen ErwGr abgeändert werden.

- **Tatsächliches Auskunftsrecht:**

Das Wahlrecht soll dem Betroffenen weiters zukommen, weil in Art 15 DSGVO im Gegensatz zu den Art 13, 14 DSGVO ein *„tatsächliches Auskunftsrecht"* normiert sei.[4] Da dem Betroffenen das Auskunftsrecht eingeräumt wurde, müsse er auch zur Ausübung des Wahlrechts ermächtigt sein.[5] Diese Sicht verkennt, dass der Betroffene weder für die Ausübung des Auskunftsrechts noch für die Ausübung des Wahlrechts einer Rechtsgrundlage bedarf. Der Betroffene könnte auch dann ein Auskunftsersuchen an den Verantwortlichen stellen, wenn es Art 15 DSGVO (und auch § 1 Abs 3 DSG) nicht gäbe, nur würde der Betroffene womöglich keine Antwort erhalten. Das Auskunftsrecht gem Art 15 DSGVO ordnet kein Recht des Betroffenen, sondern eine Pflicht des Verantwortlichen an. Die gesetzliche Anordnung ist an den Verantwortlichen gerichtet. Er ist Adressat der Bestimmung und er hat die An-

[1] Vorabentscheidungsbeschluss 18. 2. 2021, 6 Ob 159/20f. [2] EuGH 12. 1. 2023, C-154/21, *Österreichische Post*, Rn 31f. [3] EuGH C-154/21, Rn 33. [4] EuGH C-154/21, Rn 36. [5] SA 9. 6. 2021, C-154/21, Rn 21.

ordnung zu befolgen. Dem Verantwortlichen wird ein Verhalten geboten und er kann bei gebotswidrigem Verhalten bestraft werden (Art 83 Abs 5 lit b DSGVO). Nach Art 15 DSGVO trifft den Verantwortlichen eine Auskunftserteilungspflicht. Daher hatte der Normsetzer Art 15 DSGVO so genau zu formulieren, dass der Verantwortliche als Adressat der Norm sein Verhalten an ihr ausrichten kann.[6] Der Verantwortliche hat der Norm zu entsprechen, deshalb muss er sich an ihrem Wortlaut – einschließlich des Bindeworts „oder" – ausrichten und das Wahlrecht ausüben dürfen.

Dem Transparenzgrundsatz wird entsprochen, wenn über Empfänger oder Empfängerkategorien informiert wird.

- **Transparenzgrundsatz:**

Nach dem EuGH spricht auch der Transparenzgrundsatz für das Wahlrecht des Betroffenen (Art 5 Abs 1 lit a DSGVO).[7] Doch auch dieses Argument überzeugt nicht. Welche Informationen nach dem Transparenzgrundsatz zu erteilen sind, ergibt sich aus den Art 13 bis 15 DSGVO. Diese Bestimmungen gestalten den – unbestimmten – Transparenzgrundsatz aus (nicht umgekehrt) und sie ordnen jeweils das Erteilen von Informationen über Empfänger oder Empfängerkategorien an. Dem Transparenzgrundsatz wird somit entsprochen, wenn über Empfänger oder Empfängerkategorien informiert wird.

- **Art 8 GRC:**

Hieran vermag Art 8 GRC – auf den der EuGH Bezug nimmt[8] – nichts zu ändern, denn diese Bestimmung kennt überhaupt kein Recht auf Auskunft über Empfänger. Auch im Übereinkommen zum Schutz personenbezogener Daten des Europarates wird man vergeblich nach einem Recht auf Auskunft über Empfänger suchen.[9] Selbst nach Inkrafttreten einer bereits beschlossenen Nov wird dieses Europarats-Übereinkommen – genau wie es in der ehemaligen DS-RL vorgeschen war und in der DSGVO normiert ist – zur Gewährleistung einer transparenten Datenverarbeitung eine Information über Empfänger oder Empfängerkategorien vorsehen.[10] Die europäischen Gesetzgeber haben kein Auskunftsrecht über konkrete Empfänger beschlossen.

- **Überprüfung der Rechtmäßigkeit der Verarbeitung:**

Entgegen der Auffassung des EuGH[11] ist eine Auskunft über konkrete Empfänger auch **nicht** erforderlich, um den Betroffenen in die Lage zu versetzen, die Rechtmäßigkeit der Verarbeitung seiner Daten zu überprüfen. Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten hängt davon ab, ob die Daten für einen bestimmten Zweck an eine bestimmte Empfängerkategorie offengelegt werden dürfen. Zur Beurteilung der Rechtmäßigkeit der Verarbeitung genügt zu wissen, ob die Daten etwa einem Steuerberater (= Empfängerkategorie) offengelegt wurden. Sofern die Daten für einen bestimmten Zweck (zB Lohnverrechnung) **einem** Steuerberater offengelegt werden dürfen, müssen sie innerhalb der EU iSd Dienstleistungsfreiheit **allen** Steuerberatern für denselben Zweck offengelegt werden dürfen.[12] Zur Überprüfung der Rechtmäßigkeit der Verarbeitung genügt daher die Auskunft, dass die Daten zur Lohnverrechnung einem Steuerberater innerhalb der EU (bzw EWR) offengelegt wurden. Einem Arbeitnehmer den Steuerberater seines Arbeitgebers offenzulegen, ist zum Schutz personenbezogener Daten nicht erforderlich.

Trotz der Rs *Rijkeboer* nahm der Normsetzer keine Protokollierungspflicht in die DSGVO auf.

- **Praktische Wirksamkeit:**

Das Wahlrecht soll dem Betroffenen weiters zukommen, damit die praktische Wirksamkeit der Betroffenenrechte auf Berichtigung, Löschung und Einschränkung der Verarbeitung gewährleistet wird.[13] Gemeint ist die Durchsetzbarkeit dieser Rechte auch bei den Datenempfängern. In diese Richtung äußerte sich der EuGH bereits in der Rs *Rijkeboer*. Damals trug er den MS – und nicht den Verantwortlichen – auf, eine Aufbewahrungsfrist, also eine Protokollierungspflicht, für Daten über *„Empfänger oder Empfängerkategorien"* festzulegen.[14] Eine Protokollierung ist zur zuverlässigen Feststellung der konkreten Empfänger erforderlich.[15] Trotz der Rs *Rijkeboer* nahm der Normsetzer jedoch keine Protokollierungspflicht in die DSGVO auf.

- **Art 19 DSGVO:**

Der Normsetzer verhalf den genannten Betroffenenrechten auf anderem Weg zur praktischen Wirksamkeit. Mit Art 19 DSGVO wurde Art 12 lit c DS-RL in die DSGVO übernommen. Wie schon in der Vorgängerbestimmung ist vorgesehen, sämtlichen Datenempfängern jede Berichtigung oder Löschung sowie jede Einschränkung der Verarbeitung personenbezogener Daten **mitzuteilen**, außer dies erweist sich als **unmöglich** oder ist mit einem **unverhältnismäßigen Aufwand** verbunden (Art 19 Satz 1 DSGVO). Die **Mitteilungsempfänger** haben eigenständig zu prüfen, ob sie den Betroffenenanträgen ebenfalls entsprechen müssen.[16] Über die Vorgängerbestimmung hinaus wurde den Verantwortlichen die Pflicht auferlegt, dem Betroffenen – auf Antrag – die Mitteilungsempfänger offenzulegen (Art 19 Satz 2 DSGVO). Dadurch wird dem Betroffenen ermöglicht, die Rechtmäßigkeit der Verarbeitung seiner Daten beim Mitteilungsempfänger zu überprüfen und seine Betroffenenrechte durchzusetzen. Entgegen der Auffassung des EuGH[17] stützt Art 19 Satz 2 DSGVO nicht das Wahlrecht des Betroffenen, sondern macht eine Auskunft über konkrete Empfänger überflüssig.

- **Auftragsverarbeiter:**

Die praktische Wirksamkeit kann bei der größten Empfängerkategorie, den Auftragsverarbeitern, durch Bekanntgabe konkreter Empfänger **nicht** gewährleistet werden, weil die Einhaltung der Betroffenenrechte durch Auftragsverarbeiter ausschließlich vom Verantwortlichen sicherzustellen ist (Art 28 Abs 3 lit e DSGVO). **Die Betroffenenrechte können gegen Auftragsverarbeiter nicht ausgeübt werden.** Richtet der Betroffene eine Anfrage an den Auftragsverarbeiter, hat der Auftragsverarbeiter diese Anfrage an den Verantwortlichen weiterzuleiten. Der Betroffene wird also sinnlos im Kreis geschickt. Bei Verdacht auf rechtswidriges Verhalten des Auftragsverarbeiters legt der Verantwortliche dessen Identität zur eigenen Entlastung offen, sonst hat er für die Rechtswidrigkeit einzustehen. Der Auftragsverarbeiter wird selbst zum Verant-

[6] EuGH 20. 5. 2003, C-465/00, *Österreichischer Rundfunk*, Rn 77 mwN; EGMR 17. 1. 2023, 19475/20, *Künsberg Sarre*, Rn 64 mwN. [7] EuGH C-154/21, Rn 35. [8] EuGH C-154/21, Rn 44. [9] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CET 108 (1981). [10] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CET 223 (2018); s Art 8 Abs 1 lit d und Art 9 Abs 1 lit b letzter Halbsatz in der konsolidierten Fassung. [11] EuGH C-154/21, Rn 37. [12] Die DSGVO hat das Ziel, den freien Verkehr personenbezogener Daten in der Union zu ermöglichen (Art 1 Abs 3 DSGVO). [13] EuGH C-154/21, Rn 38 f. [14] EuGH 7. 5. 2009, C-553/07, *Rijkeboer*, Rn 62 ff. [15] DSK 12. 11. 2004, K120.902/0017-DSK/2004; 7. 12. 2004, K120.937/0007-DSK/2004; VfSlg 18.230/2007; VwSlg 17.680 A/2009. [16] *Haidinger* in *Knyrim*, DatKomm Art 19 DSGVO Rn 15 (Stand 1. 12. 2021, rdb.at). [17] EuGH C-154/21, Rn 41.

wortlichen (Art 28 Abs 10 DSGVO) und der Betroffene kann die Rechtmäßigkeit der Verarbeitung seiner Daten bei diesem überprüfen sowie seine Betroffenenrechte durchsetzen.

- **Verarbeitungskette:**

Die praktische Wirksamkeit der Betroffenenrechte ist auch gegenüber weiteren Empfängern einer Verarbeitungskette gewährleistet. Denn Auftragsverarbeiter haben ihre **Subauftragsverarbeiter** zur rechtmäßigen Datenverarbeitung anzuhalten (Art 28 Abs 4 DSGVO) und sämtliche Datenempfänger, die selbst Verantwortliche sind, haben allfällige weitere Empfänger der Verarbeitungskette gem Art 19 DSGVO zu informieren und auf Antrag die jeweiligen Mitteilungsempfänger dem Betroffenen mitzuteilen. Ein zusätzliches Recht auf Auskunft über konkrete Empfänger ist nicht erforderlich.

- **Größenschluss:**

Kommt den Betroffenen das Wahlrecht zu, kann in Art 15 Abs 1 lit c DSGVO auf die Wortfolge *„oder Kategorien von Empfängern"* verzichtet werden. Denn die Empfängerkategorien können aus den Identitäten der Empfänger geschlossen werden. Wer ein Recht auf Auskunft über konkrete Empfänger hat, muss iSe Größenschlusses auch über Empfängerkategorien Auskunft verlangen dürfen. Die Wortfolge *„oder Kategorien von Empfängern"* wurde aus Art 15 Abs 1 lit c DSGVO somit weginterpretiert. Ein beschränkter Anwendungsbereich für diese Wortfolge verbleibt nur, wenn man den Verhältnismäßigkeitsgrundsatz beachtet und der Betroffene die Ausübung seines Wahlrechts zu begründen hat.

Verhältnismäßigkeitsgrundsatz

Der Verhältnismäßigkeitsgrundsatz zählt zu den allgemeinen Grundsätzen des Primärrechts[18] und ist daher bei der Auslegung des Sekundärrechts stets zu beachten. Insb wenn Informationen für die Auskunftserteilung **neu zu erstellen** sind, ist die dafür erforderliche **Arbeitsbelastung** zu berücksichtigen.[19] Vor diesem Hintergrund erscheint die Position des Europäischen Datenschutzausschusses (**EDSA**), wonach die Verhältnismäßigkeit der Arbeitsbelastung bei der Auskunftserteilung unerheblich ist,[20] primärrechtswidrig.

Die Einschränkung des Auskunftsumfangs auf Empfängerkategorien trägt dem Grundsatz der Verhältnismäßigkeit Rechnung und ist auch sachgerecht, weil mit der Pflicht zur Auskunftserteilung ein erheblicher **Ressourcenaufwand** verbunden ist. Aus demselben Grund sind etwa zur Wahrung der Verhältnismäßigkeit über die Herkunft von Daten nur verfügbare Informationen zu erteilen (Art 15 Abs 1 lit g DSGVO) und darf die Mitteilung gem Art 19 DSGVO bei unverhältnismäßigem Aufwand unterbleiben.

Nach dem EuGH darf die Auskunft auf Empfängerkategorien eingeschränkt werden, wenn es *„nicht möglich ist, Informationen über konkrete Empfänger"* zu erteilen[21] oder das Auskunftsersuchen gem Art 12 Abs 5 DSGVO offenkundig unbegründet oder exzessiv ist.[22] Dies folgt nach der Argumentation des EuGH aus dem Erfordernis, das Auskunftsrecht unter Wahrung des Grundsatzes der Verhältnismäßigkeit gegen die Grundrechte von Verantwortlichen abzuwägen.[23] Laut dem EuGH sind somit die Grundrechte der Verantwortlichen zu berücksichtigen. Dies ergibt sich auch aus **Art 15 Abs 4 DSGVO**, wonach die Rechte und Freiheiten *„anderer Personen"* zu beachten sind. Solche anderen Personen sind auch die Verantwortlichen.[24]

Einschränkung des Auskunftsumfangs ist sachgerecht, weil mit der Auskunftserteilung ein erheblicher Ressourcenaufwand verbunden ist.

Die Grundrechte des Verantwortlichen werden durch jedes Auskunftsersuchen berührt. Der Auskunftspflicht ist ein Eingriff ins **Grundrecht auf unternehmerische Freiheit** (Art 16 GRC) immanent, weil der Verantwortliche bei der freien Nutzung der ihm zur Verfügung stehenden Ressourcen eingeschränkt wird.[25] Ferner wird regelmäßig ein Eingriff ins **Grundrecht auf Achtung des Privatlebens** verwirklicht (Art 8 EMRK und Art 7 GRC), weil dieses Grundrecht auch berufliche und geschäftliche Tätigkeiten und damit die Geheimhaltung von vertraulichen Informationen schützt.[26] Bei der Information über Datenempfänger sind auch die Grundrechte dieser Empfänger in die Abwägung einzubeziehen.

Da jedes Auskunftsersuchen in die Grundrechte der Verantwortlichen eingreift,[27] ist stets eine **Verhältnismäßigkeitsprüfung** durchzuführen, unabhängig davon, ob das Auskunftsersuchen exzessiv ist. Daher sind die zulässigen Einschränkungen des Auskunftsrechts auf Empfängerkategorien folgend zu verstehen:

Jedes Auskunftsersuchen greift in Grundrechte ein, daher ist stets eine Verhältnismäßigkeitsprüfung durchzuführen.

- **Unmöglichkeit:**

Ist es *„nicht möglich"*, die Empfänger zu identifizieren, darf eine Auskunft auf Empfängerkategorien eingeschränkt werden. Würde der EuGH mit „nicht möglich" eine **faktische oder rechtliche Unmöglichkeit** meinen, wäre der Verweis des EuGH auf den Verhältnismäßigkeitsgrundsatz unnötig. Denn bei faktischer oder rechtlicher Unmöglichkeit kann eine Auskunft per se nicht erteilt werden und ist daher auch nicht geschuldet.[28] Auf die Verhältnismäßigkeit kommt es nicht an. Kennt der Verantwortliche die Identitäten der Empfänger nicht, treffen ihn Nachforschungs- und Rekonstruktionspflichten. Diese Pflichten haben ihre Grenze aber ebenso wie Art 19 DSGVO im Verhältnismäßigkeitsgrundsatz zu finden. Eine Auskunft über konkrete Empfänger ist somit **unmöglich**, wenn die Identität der konkreten Empfänger nur mit unverhältnismäßigem Arbeitsaufwand festgestellt und rekonstruiert werden könnte.

- **Exzessiv:**

Die Tatbestände des Art 12 Abs 5 DSGVO wurden nach bisheriger Auffassung als Fälle des Rechtsmissbrauchs verstanden.[29] Dieser Auffassung folgte der EuGH offensichtlich nicht, denn bei missbräuchlicher Rechtsausübung kann es nicht auf die Verhältnismäßigkeit ankommen. Somit ist ein Auskunftsersuchen nicht erst nach Überschreiten der

[18] EuGH 11. 2. 2021, C-77/20, *K. M.*, Rn 36. [19] EuGH 10. 11. 2022, C-163/21, *PACCAR*, Rn 67 ff. [20] EDPB, Guidelines 01/2022 on data subject rights – Right of access (2022) Rn 164, FN 89. [21] EuGH C-154/21, Rn 48. [22] EuGH C-154/21, Rn 49. [23] EuGH C-154/21, Rn 47. [24] EDPB, Guidelines 01/2022 on data subject rights – Right of access (2022) Rn 169. [25] EuGH 27. 3. 2014, C-314/12, *UPC Telekabel*, Rn 50; 30. 6. 2016, C-134/15, *Lidl*, Rn 29. [26] EuGH 14. 2. 2008, C-450/06, *Varec*, Rn 48 ff; VfSlg 20.345/2019, Rn 51. [27] Zu denken ist auch an die Grundrechte auf Erwerbsfreiheit (Art 6 StGG) und Eigentum (Art 5 StGG; Art 1 1 ZProtMRK; Art 17 GRC). Verantwortliche des öffentlichen Bereichs sind idR keine Grundrechtsträger, dennoch dürfen auch ihre Ressourcen nicht überstrapaziert werden. Der EuGH bezog sich auf Grundrechte, weil er über die Auskunftserteilungspflicht eines Verantwortlichen des privaten Bereichs urteilte. [28] OGH 5. 5. 1988, 6 Ob 9/88; DSB 27. 8. 2014, DSB-D121.876/0005-DSB/2014; 1. 10. 2014, DSB-D122.020/0012-DSB/2014; 12. 5. 2016, DSB-D122.468/0006-DSB/2016; 19. 11. 2020, 2020-0.743.659; BVwG 17. 11. 2015, W214 2014069-1; VwGH 10. 9. 2010, 2010/17/0084 (rechtliche Unmöglichkeit). [29] BVwG 28. 9. 2022, W274 2259250-1, S 3; *Lembke*, Der datenschutzrechtliche Auskunftsanspruch im Anstellungsverhältnis, NJW 2020, 1841 (1846).

Grenze zum Rechtsmissbrauch als exzessiv anzusehen. Vielmehr ist bei der Beurteilung der Aufwand des Verantwortlichen miteinzubeziehen. Verlangt etwa ein Betroffener die Herausgabe von Informationen, deren Beschaffung für den Verantwortlichen mit erheblichem Aufwand verbunden ist, ohne sein Interesse an der Information hinreichend darzulegen, ist das Auskunftsersuchen als **exzessiv** zu qualifizieren.

Bei offenkundig unbegründeten Ersuchen darf die Auskunft auf Empfängerkategorien eingeschränkt werden.

- **Offenkundig unbegründet:**

Auskunftsersuchen dürfen ohne Begründung gestellt werden.[30] Ist ein Auskunftsersuchen offenkundig unbegründet, darf die Auskunft nach dem EuGH jedoch auf Empfängerkategorien eingeschränkt werden. Ein Auskunftsersuchen, das keine Begründung enthält, ist offenkundig ohne Begründung und somit **offenkundig unbegründet**. Wird in einem Auskunftsersuchen das Interesse an der Auskunft nicht begründet, darf die Auskunft daher auf Empfängerkategorien eingeschränkt werden. Dieses Ergebnis wird durch das Bindewort „oder" bezweckt und ist auch sachgerecht, weil vom Verantwortlichen ein **unnötiger und unverhältnismäßiger Aufwand** abgewendet wird.

Conclusio

Der EuGH hat den Verantwortlichen eine weitere Last auferlegt. Sie haben unabhängig von den konkreten Umständen des Falls sämtliche Datenempfänger, einschließlich Auftragsverarbeiter, zu beauskunften. Hierzu haben sie entweder jede Datenoffenlegung zu protokollieren oder die Datenempfänger nachzuforschen und zu rekonstruieren.

Immerhin fordert der EuGH zum Ausgleich dieser Last eine Verhältnismäßigkeitsprüfung. Es ist jedoch anzunehmen, dass die Rechtsprechung, insb jene der Aufsichtsbehörden, der primärrechtswidrigen Position der EDSA folgen und die Verhältnismäßigkeit außer Acht lassen wird. Für die Wortfolge *„oder Kategorien von Empfängern"* verbleibt in Art 15 Abs 1 lit c DSGVO dann kein Raum.

PRAXISTIPP

Verantwortliche sind gut beraten, sich auf die Beantwortung von Auskunftsersuchen intensiv vorzubereiten. In Verfahren vor Behörden und Gerichten sollte zum Erzwingen der gebotenen Verhältnismäßigkeitsprüfung der Eingriff in die Grundrechte des Verantwortlichen ausdrücklich eingewendet werden.

Dako 2023/19

[30] VwSlg 17.706 A/2009; DSB 26. 7. 2019, DSB-D123.921/0005-DSB/2019; BVwG 5. 7. 2022, W252 2246597-1; EDPB, Guidelines 01/2022 Rn 13, 165.

Zum Thema

Über den Autor

Janos Böszörmenyi ist Rechtsanwalt bei der Schönherr Rechtsanwälte GmbH in Wien. Zur EuGH-E *Österreichische Post* siehe *Wagner*, Beauskunftung der konkreten Empfänger – Praktische Umsetzung, Dako 2023/17 in diesem Heft Seite 28.
E-Mail: j.boeszoermenyi@schoenherr.eu

Natalie Ségur-Cabanac
Head of Regulatory & Compliance und Data Protection Officer bei Hutchison Drei Austria GmbH („Drei").

Das Zusammenspiel von DSGVO und dem sektorspezifischen Datenschutzrecht im TKG

Adressatenkreis; Beschränkungen bei der Bearbeitung; Datenkategorien des TKG 2021; Spamparagrafen; Data Breach. Das Zusammenspiel zwischen DSGVO und ePrivacy RL ist in der Praxis schwierig. Der Adressatenkreis und Begriffsdefinitionen finden sich im Kodex für die elektronische Kommunikation. Die Umsetzung in Österreich erfolgte durch das TKG 2021. Der Beitrag zeigt Freiräume und Beschränkungen bei der Bearbeitung von personenbezogenen Daten auf.

Zwei Grundrechte im Fokus: Datenschutz und Kommunikationsgeheimnis

Mit der Datenschutzgrundverordnung (EU 2016/679) wurde die frühere Datenschutzrichtlinie (95/46/EG) abgelöst. Seit deren Inkrafttreten 2018 hat die Bedeutung des Datenschutzes in Europa, insb in Unternehmen und Behörden, stark zugenommen, nicht zuletzt auch wegen der zunehmenden Digitalisierung im Alltag und der Rolle und der Bedeutung von personenbezogenen Daten dabei. Die DSGVO bildet ein solides und umfangreiches Rahmenwerk für die Verarbeitung von personenbezogenen Daten in Europa. Der Schutz personenbezogener Daten und die Achtung der Privatsphäre sind europäische Grundrechte (Art 7 und 8 GRC). In Art 7 GRC ist außerdem das Grundrecht auf Achtung des Kommunikationsgeheimnisses verbrieft.

Adressatenkreis der sektorspezifischen Datenschutzregelungen

Anbieter von (öffentlich zugänglichen) Kommunikationsdiensten unterliegen zusätzlich zur DSGVO auch der RL 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), im Folgenden kurz **ePrivacy RL** genannt. Mit den neuen Möglichkeiten, die das Internet bietet, entstehen für die Nutzer in Bezug auf ihre personenbezogenen Daten neue Risiken. Die ePrivacy RL adressiert den Schutz der Privatsphäre in der elektronischen Kommunikation. Dabei sollte die ePrivacy RL als **sektorspe-**

zifisches Datenschutzrecht neben der damals noch in Geltung stehenden Datenschutzrichtlinie (95/46/EG) für den angesprochenen Adressatenkreis fungieren.

Die ePrivacy RL ist bald fünf Jahre nach Inkrafttreten der DSGVO noch immer in Kraft, eine Nachfolgeregelung einer ePrivacy VO wird seit Jahren ohne Ergebnis verhandelt.

Als RL muss – im Gegensatz zur DSGVO – die ePrivacy RL in nationale Gesetze umgesetzt werden. Wir haben also heute eine Situation, wo es eine weitgehend harmonisierte allgemeine DSGVO in Europa gibt, aber nach wie vor nationale Umsetzungsgesetze auf Basis einer ePrivacy RL, die noch in Bezug auf eine alte Datenschutzrichtlinie verabschiedet wurden. Das macht es dem Anwender:innenkreis nicht gerade leichter, zumal das **Zusammenspiel** zwischen den beiden Normen in der Praxis **schwierig** ist.

Der Europäische Datenschutzausschuss hat in einer sehr frühen **Stellungnahme** (5/2019 vom 12. 3. 2019) nach Inkrafttreten der DSGVO zum Zusammenspiel zwischen ePrivacy RL und der DSGVO klargestellt, dass die ePrivacy RL nach wie vor als lex specialis zur DSGVO gilt und darüber hinaus auch Ergänzungen enthält, wie zB den Schutz von Endnutzern eines öffentlich zugänglichen elektronischen Kommunikationsdienstes auch dann, wenn diese juristische Personen sind.

Wer jedoch konkret zum Adressatenkreis gehört bzw was als **„Kommunikationsdienst"** zu sehen ist, definiert nicht die ePrivacy RL selbst, sondern wurde hierzu ursprünglich auf die Begriffsbestimmungen der RL 2002/21/EG über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste („Rahmenrichtlinie") verwiesen. Demnach handelt es sich dabei va um klassische Telefonie- und Internetzugangsdienste. Inzwischen wurde dieser Rechtsrahmen durch die RL (2018/1972) über den europäischen **Kodex für die elektronische Kommunikation** (EEKK) neu erlassen. Verweise auf die Rahmenrichtlinie gelten seither als Verweise auf den EEKK.

Der EEKK **erweitert den Begriff** der Anbieter von Kommunikationsdiensten auch auf Dienste, die „klassischen" Kommunikationsdiensten in der Funktionsweise gleichwertig sind (gemeint sind hier zB Messengerdienste, die über das Internet erbracht werden). Dies hat zur Folge, dass die ePrivacyRL nun auch auf diese Dienste anwendbar ist.

In Österreich ist der EEKK im Telekommunikationsgesetz 2021 (TKG 2021) umgesetzt worden. Die ePrivacy RL wurde ebenfalls bereits im TKG 2003 umgesetzt. Im Zuge der **Neukodifizierung** des **TKG 2021** wurden die bisherigen Bestimmungen des TKG 2003 mit wenigen Adaptierungen übernommen, wobei die datenschutzrechtlichen Bestimmungen im neuen TKG streng genommen auf den nun erweiterten Adressatenkreis des EEKK anwendbar sind.

Ein sehr weiter Adressatenkreis, nämlich jedermann, der über elektronische Kommunikationsdienste Werbung übermittelt, unterliegt dem sog **Spamverbot** in § 174 TKG (unerbetene Nachrichten).

TKG erfasst mehr als personenbezogene Daten

Die DSGVO regelt die Verarbeitung von personenbezogenen Daten. Besteht kein Personenbezug, so ist die DSGVO nicht anwendbar. Die ePrivacy RL bzw das TKG gelten in manchen Bestimmungen auch für nicht personenbezogene Informationen wie zB die Cookieregelung in § 165 Abs 3 TKG.

Freiräume und Beschränkungen bei der Bearbeitung von personenbezogenen Daten

Das TKG 2021 enthält für den 14. Abschnitt (Kommunikationsgeheimnis, Datenschutz) eigene Begriffsbestimmungen. So wird der Anbieter als Betreiber von öffentlichen Kommunikationsdiensten (§ 160 Abs 3 Z 1) und der „Benutzer" als Person definiert, die die einen öffentlichen Kommunikationsdienst für private oder geschäftliche Zwecke nutzt, ohne diesen Dienst zwangsläufig abonniert zu haben (§ 160 Abs 3 Z 2). Benutzer kann auch eine juristische Person sein.

Die **Hauptleistung** eines **Verantwortlichen** nach TKG besteht in der Ermöglichung von Kommunikation über eine Telekommunikationsinfrastruktur (Leitungen, Richtfunk, Antennen, Schnittstellen etc). Dabei werden personenbezogene Daten verarbeitet.

Eine **Verarbeitung von personenbezogenen Daten** benötigt allgemein

- einen legitimen Zweck (den der Verantwortliche weitgehend frei wählen kann),
- eine rechtliche Grundlage gem Art 6 DSGVO sowie
- die Einhaltung der Prinzipien der DSGVO (Art 5 DSGVO) durch alle an der Verarbeitung Beteiligten.

Der risikobasierte Ansatz, den die DSGVO erlaubt, existiert im TKG nicht.

Das TKG 2021 bzw die ePrivacy RL regeln idZ sehr spezifisch und abschließend, welche Daten dabei verarbeitet werden dürfen, legen fest, für welche Zwecke, und sehen konkrete Löschfristen und Zugangs- und Zugriffsregelungen vor. Insofern sind Anbieter nach dem TKG bei der Datenverarbeitung sehr eng daran gebunden. Der risikobasierte Ansatz, den die DSGVO in mancher Hinsicht erlaubt, existiert im TKG nicht.

Datenkategorien des TKG 2021

Das TKG 2021 kennt **drei Kategorien** von Daten:

- Stammdaten,
- Verkehrsdaten und
- Inhaltsdaten.

Werden diese Daten verarbeitet, kommen die sektorspezifischen Datenschutzregelungen der ePrivacy RL bzw des TKG 2021 zur Anwendung.

Stammdaten sind persönliche Informationen eines Vertragsinhabers eines Telekommunikationsvertrags (zB Name, akademischer Grad, Adresse, Rufnummer, Vertragsinformationen, Geburtsdatum, Bonität) und dürfen nur verarbeitet werden, um einen Telekommunikationsvertrag abschließen, ihn zu erfüllen und ihn zu beenden. Stammdaten sind nach Beendigung und Verrechnung des Vertrags zu löschen, sofern keine anderen gesetzlichen Aufbewahrungspflichten bestehen.

Verkehrsdaten sind jene Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden. Es sind Daten wie Zeitpunkt, Standort, Rufnummer, IP-Adresse, Mobilfunkzelleninformationen eines konkreten Kommunikationsvorgangs. Verkehrsdaten sind unmittelbar nach dem Kommunikationsvorgang zu löschen, sofern sie nicht zu betrieblichen Zwecken (zB Störungsbehebungen, Notrufe) oder zur Verrechnung gebraucht werden. Einzige Ausnahme ist die Verarbeitung von Verkehrsdaten für sog Dienste mit Zusatznutzen auf Basis einer Einwilligung.

Inhaltsdaten sind die Inhalte einer Kommunikation. Für diese gilt ganz besonders das Kommunikationsgeheimnis. Inhalte dürfen tatsächlich nicht gespeichert

werden. Sie dürfen nur insofern verarbeitet werden, als es zur Weiterleitung einer Nachricht erforderlich ist.

Betroffenensicht

Anbieter agieren bei der Erbringung von Leistungen nach dem TKG in der Regel als Verantwortliche iSv Art 4 Z 7 DSGVO. Eine Kommunikation hat in der Regel zumindest zwei Teilnehmer. Beide Teilnehmer eines elektronischen Kommunikationsdienstes sind auch Betroffene iSv Art 4 Z 1 DSGVO, wenn ihre Daten dabei von den beteiligten Anbietern verarbeitet werden. Das TKG bezeichnet diese als „bloße" Benutzer, im Gegensatz zum Vertragsnehmer, der den Vertrag über die Telekommunikationsleistung mit dem jeweiligen Anbieter hält. Anbieter haben demnach potenziell Personen als Betroffene zu betrachten, deren Identität sie gar nicht kennen.

Beispiel

Ein Vater schließt einen Handyvertrag ab, überlässt das Gerät dann aber seiner Tochter zur Nutzung. Der Anbieter kennt die Identität des Vaters, aber nicht die der Tochter, verarbeitet aber Daten der Tochter, wenn diese das Handy zum Telefonieren oder Surfen nutzt.

Das ist insb dann relevant, wenn es um die **Betroffenenrechte** gem **Art 12 ff DSGVO** geht, zumal ein Anbieter genau darauf achten muss, wessen Daten in welchem Kontext verarbeitet werden und wem gegenüber Informationspflichten und Auskunftsverpflichtungen etc gelten. Es kann also sein, dass jemand einen Auskunftsanspruch gem Art 15 DSGVO an einen Anbieter richtet, dessen Identität nicht bekannt ist. Gleichzeitig darf ein Anbieter keine Auskunft über Daten der Tochter an den Vater geben und ebenso umgekehrt, weil es sich hierbei – wie beim Datenschutzrecht an sich – um ein höchstpersönliches Recht handelt.

Betroffenenrechte gelten auch für Daten, die aufgrund des TKG 2021 verarbeitet werden.

Bleiben wir bei den Betroffenenrechten gem DSGVO: Diese gelten natürlich grundsätzlich auch für **Daten**, die aufgrund des **TKG 2021** verarbeitet werden, wobei sich gerade an den Verkehrsdaten zeigt, dass selbst hier ein Interessenausgleich notwendig ist: Alle Teilnehmer einer Kommunikation haben Anspruch auf Geheimhaltung der Kommunikation (inklusive der dabei erzeugten Daten), ein Anbieter könnte diesen verletzen, wenn er seinen Kunden Auskunft über Verkehrsdaten geben würde. Außerdem ist nicht sicher, wer tatsächlich einen Anschluss genutzt hat. Die Daten von „bloßen" Benutzern sind zu schützen, auch gegenüber dem auskunftsberechtigten Kunden des Anbieters. Insofern besteht kein Auskunftsanspruch auf Verkehrsdaten iSv § 167 TKG 2021. Das wurde in Entscheidungen der ehemaligen DSK und der DSB[1] und schließlich auch von der Datenschutzbehörde durch Genehmigung des ISPA-Code of Conduct[2] 2018 (überarbeitet und neu genehmigt im August 2022) bestätigt.

Neben natürlichen Personen sind nach dem TKG **auch** die Daten von **juristischen Personen geschützt**, sofern es um die im TKG geregelten Datenarten (Stammdaten, Verkehrsdaten, Inhaltsdaten) geht. Der Schutz leitet sich direkt aus der ePrivacy RL (Art 1 Abs 2) ab, während Art 1 DSG (der das allgemeine Datenschutzrecht auf juristische Personen ausweitet) keine Grundlage in der DSGVO hat. Das TKG sieht in § 164 Abs 1 insofern eine Einschränkung des Schutzes vor, als eine Datensicherheitsverletzung nur bezüglich von *„nicht öffentlich zugänglichen Daten einer juristischen Person"* gegeben ist. Das bedeutet, dass öffentlich zugängliche Daten einer juristischen Person nicht dem sektorspezifischen Datenschutzrecht des TKG unterliegen. Dieselbe Einschränkung findet sich nach der Nov 2021 in § 174 TKG „Unerbetenen Nachrichten", dem sog **„Spamparagrafen"**, der nicht nur für Anbieter gilt, sondern für alle Anrufe und Nachrichten, die zu Werbezwecken über elektronische Medien übermittelt werden. Fraglich ist, ob die neu formulierte Einschränkung zur Folge hat, dass öffentlich zugängliche Daten von juristischen Personen nicht dem Spamverbot unterliegen.

Meldung von Datensicherheitsverletzungen

Datensicherheitsverletzungen sind gem Art 33 DSGVO binnen 72 Stunden an die Datenschutzbehörde zu melden. Auch Art 4 Abs 3 der ePrivacy RL (§ 160 TKG 2021) verpflichtet zur Meldung. Zusätzlich gilt für Anbieter seit 2013 eine eigene VO (EU 611/2013) zu Meldepflichten von Datensicherheitsvorfällen, wonach die Frist für eine Erstmeldung 24 Stunden beträgt und binnen drei Tagen eine Zweitmeldung zu übermitteln ist. In der Praxis kann diese kurze Frist sehr herausfordernd sein. Eine zusätzliche Meldepflicht nach Art 33 DSGVO besteht dann nicht.[3]

Für Anbieter gilt seit 2013 eine eigene Meldepflicht mit einer Frist von 24 Stunden.

Der ISPA-Code of Conduct enthält eine Vorlage für eine solche Datensicherheitsmeldung. Passiert eine Datensicherheitsverletzung in Datenverarbeitungen, die nicht vom TKG erfasst sind, so gilt die allgemeine 72-Stundenfrist von Art 33 DSGVO auch für Anbieter von Telekommunikationsdienstleistungen. Darüber hinaus haben Anbieter laut § 164 Abs 6 TKG ein eigenes Verzeichnis der Verletzungen des Schutzes personenbezogener Daten zu führen. Es ist davon auszugehen, dass dabei mit der Führung eines Verzeichnisses auch die Dokumentationspflichten gem Art 33 Abs 5 DSGVO erfüllt werden.

Ausblick

Anbieter von Telekommunikationsdiensten tragen im Hinblick auf den Schutz der Privatsphäre ihrer Nutzer eine hohe Verantwortung. Das enge Korsett des Rechtsrahmens gewährleistet das. Als einzige Rechtsgrundlage für die Datenverarbeitung nach TKG kommt das **Gesetz** bzw die **Erfüllung eines Vertrags** in Betracht. Selbst mit Einwilligung ist eine darüber hinausgehende Verarbeitung der TKG-Daten nur in einem sehr engen Rahmen möglich (für die Erbringung von Diensten mit Zusatznutzen). Die Rechtsgrundlage des überwiegenden berechtigten Interesses (Art 6 Abs 1 lit f DSGVO) ist im TKG nicht explizit vorgesehen. Hier scheint die ePrivacy RL in Österreich zu eng umgesetzt worden zu sein. Selbst der EuGH[4] sieht hier mehr Spielraum. Nach Ansicht des EuGH ist nämlich eine Verarbeitung mit Einwilligung des Betroffenen oder auch im legitimen Interesse zulässig, solange dies zu einem der in der ePrivacy RL genannten Zwecken oder auf Basis einer gem Art 15 Abs 1 ePrivacy RL

[1] DSB 15. 4. 2016, DSB-D122.418/0002-DSB/2016 mwN.
[2] www.ispa.at/coc/. [3] Rz 44 Stellungnahme EDSA 5/2019 zum Zusammenspiel e-Datenschutz-Richtlinie und DSGVO. [4] C-597/19.

erlassenen Ausnahmebestimmung erfolgt bzw im Einklang damit steht.

Die Branche sieht gespannt auf die Verhandlungen zu einer neuen ePrivacy VO, in denen die Frage gelöst werden soll, inwieweit Anbieter auf Basis eines überwiegenden berechtigten Interesses eigene Verarbeitungszwecke rechtfertigen können. Ein Punkt, der mit ein Grund für die langjährige Verzögerung der VO ist.

Dako 2023/20

Zum Thema

Über die Autorin

Natalie Ségur-Cabanac ist Head of Regulatory & Compliance und Data Protection Officer bei Hutchison Drei Austria GmbH („Drei").
E-Mail: Natalie.Segur-Cabanac@drei.com

Hans-Jürgen Pollirer
Senior Management Consultant bei der Secur-Data Betriebsberatungs-GmbH

Checkliste Whistleblowing gemäß HSchG

Anwendungsbereich; Umsetzungsfristen; Dokumentationspflichten; Informationssicherheit; Sanktionen. Die Checkliste enthält Prüffragen, die bei der Umsetzung des HinweisgeberInnenschutzgesetzes (HSchG) zu beachten sind. Auch bei bereits implementierten Whistleblowingsystemen ist zu prüfen, ob sie den Bestimmungen des HSchG entsprechen.

Einleitung

Bereits in der Dako 2020/23 wurde das Thema Whistleblowing im Rahmen einer Checkliste behandelt. Diese basierte allerdings auf der RL (EU) 2019/1937 des EP und des Rates vom 23. 10. 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden.[1] Eine Umsetzung dieser RL, die durch die MS spätestens bis zum 17. 12. 2021 erfolgen hätte sollen, lag in Österreich zum Zeitpunkt der Veröffentlichung dieser Checkliste allerdings noch nicht vor. Mit mehr als einjähriger Verspätung haben nun der NR am 1. 2. 2023 und der BR am 16. 2. 2023 das neue HinweisgeberInnenschutzgesetz (HSchG) mit anschließenden Gesetzesänderungen beschlossen; mit 24. 2. wurde es im BGBl I 2023/6[2] veröffentlicht. Dies allerdings gegen die Stimmen der Opposition, welche die Bestimmungen für unzureichend halten. So seien außerhalb der RL nur einzelne innerstaatliche Straftaten umfasst, nicht aber etwa Betrug oder Veruntreuung sowie Mobbing, Diskriminierung, Menschenhandel oder Untreue.

Ziel des HSchG

Ziel des HSchG ist es, Personen, die Informationen über rechtlich fragwürdige Praktiken in ihrem beruflichen Umfeld weitergeben, vor Repressalien am Arbeitsplatz und anderen negativen Konsequenzen sowie existenzbedrohenden Gerichtsprozessen zu schützen. So enthält § 20 den Schutz vor Vergeltungsmaßnahmen gegen Hinweisgeberinnen und Hinweisgeber und der Personen in ihrem Umkreis. Ua sind Suspendierung, Kündigung, Gehaltskürzungen, Disziplinarmaßnahmen, Versagung einer Beförderung explizit verboten.

Anwendungsbereich

Das HSchG ist auf Hinweise zu Rechtsverletzungen in Unternehmen und juristischen Personen des öffentlichen Sektors mit jeweils 50 oder mehr Arbeitnehmern/Bediensteten anzuwenden. Gem § 3 Abs 3 HSchG gilt das für Hinweise zu **Verstößen in den Bereichen**

1. Öffentliches Auftragswesen;
2. Finanzdienstleistungen, Finanzprodukte und Finanzmärkte sowie Verhinderung von Geldwäsche und Terrorismusfinanzierung;
3. Produktsicherheit und -konformität;
4. Verkehrssicherheit;
5. Umweltschutz;
6. Strahlenschutz und nukleare Sicherheit;
7. Lebensmittel- und Futtermittelsicherheit, Tiergesundheit und Tierschutz;
8. öffentliche Gesundheit;
9. Verbraucherschutz;
10. Schutz der Privatsphäre und personenbezogener Daten sowie Sicherheit von Netz- und Informationssystemen;
11. Verhinderung und Ahndung von Straftaten nach den §§ 302 bis 309 StGB.

Punkt 11 behandelt zusätzlich zu den in der RL (EU) 2019/1937 enthaltenen Rechtsbereichen im Bereich der Beamten und Amtsträger sowie Schiedsrichter (Mitglieder von Schiedsgerichten) den Missbrauch der Amtsgewalt (§ 302), die fahrlässige Verletzung der Freiheit der Person oder des Hausrechts (§ 303), Bestechlichkeit (§ 304), Vorteilsannahme (§ 305), Vorteilsannahme durch Beeinflussung (§ 306), Bestechung (§ 307), Vorteilszuwendung (§ 307a), Vorteilszuwendung durch Beeinflussung (§ 307b), verbotene Intervention (§ 308) sowie Geschenkannahme und Bestechung von Bediensteten oder Beauftragten (§ 309).

Weiters sind Rechtsverletzungen zum Nachteil der finanziellen Interessen der EU sowie die Verletzung von Binnenmarktvorschriften und der Körperschaftsteuervorschriften umfasst.

[1] https://kurzelinks.de/6evq [2] www.ris.bka.gv.at/eli/bgbl/i/2023/6

Umsetzung des HSchG

Normadressaten des neuen HSchG sind sowohl Einrichtungen des öffentlichen Sektors als auch private Unternehmen und gemeinnützige Einrichtungen und Vereine, sofern sie mindestens 50 Mitarbeiterinnen und Mitarbeiter beschäftigen. Unabhängig von der Anzahl der Mitarbeiterinnen und Mitarbeiter sind gem § 3 Abs 2 HSchG auch bestimmte Branchen verpflichtet, einen **internen Meldekanal** zu implementieren. Diese Verpflichtung bezieht sich auf Art 8 Abs 4 der RL (EU) 2019/1937 und betrifft insb Unternehmen des Finanzdienstleistungssektors wie zB die Bilanzbuchhaltungsberufe, Versicherungsmakler, Vermögensberater, Wertpapiervermittler, Immobilienmakler uÄ.

Alle Adressaten sind verpflichtet, eine **interne Meldestelle** einzurichten, wobei konkrete Vorgaben über die Ausgestaltung im HSchG nicht enthalten sind. Gem § 13 HSchG müssen jedoch gewisse Voraussetzungen erfüllt sein, zB die Bereitstellung der notwendigen finanziellen oder personellen Mittel sowie die Möglichkeit zur unparteiischen Prüfung von Hinweisen auf ihre Stichhaltigkeit. Hinweise müssen der internen Stelle schriftlich, mündlich oder in beiden Formen mitgeteilt werden können, insb müssen auch anonyme Hinweise möglich sein.

Gem § 11 Abs 1 HSchG müssen Hinweisgeberinnen und Hinweisgeber dazu angeregt werden, die Abgabe von Hinweisen an die interne Stelle gegenüber externen Stellen zu bevorzugen. Als **externe Stelle** ist zur Entgegennahme und Behandlung von Hinweisen für Rechtsträger des privaten Sektors oder des öffentlichen Sektors gem § 15 Abs 1 HSchG das Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung zuständig.

Arbeitsrechtliche Aspekte

Da idR die Mehrheit der Hinweisgeberinnen und Hinweisgeber Arbeitnehmerinnen und Arbeitnehmer sein werden, stellt sich auch die Frage, inwieweit der **Betriebsrat** (BR) in die Umsetzung des Whistleblowingsystems (kurz: WBS) **einzubeziehen** ist. Zu dieser Thematik gibt es im HSchG keinerlei Hinweise. Entspricht das implementierte WBS den Bestimmungen des HSchG, so ist nach mM idR der Abschluss einer Betriebsvereinbarung (BV) entbehrlich, da eine gesetzliche Verpflichtung zur Einrichtung eines WBS aufgrund des HSchG besteht. Nur wenn die Hinweismöglichkeiten des WBS über die vom HSchG umfassten und dort abschließend angeführten Bereiche hinausgehen und die Menschenwürde berühren, wird der Abschluss einer BV notwendig sein. Jedenfalls wird anhand des geplanten WBS fallweise evaluiert werden müssen, ob ein Mitbestimmungsrecht des BR vorliegt.

Umsetzungsfristen

Wie nachfolgend gezeigt, sind die Umsetzungsfristen für die Implementierung des WBS sehr knapp bemessen. Entsprechende Umsetzungsmaßnahmen müssen daher sowohl im öffentlichen Sektor wie auch von privaten Unternehmen, gemeinnützigen Einrichtungen und Vereinen relativ rasch eingeleitet werden:

Unternehmen und juristische Personen des öffentlichen Sektors

- ab 250 Arbeitnehmern: bis (spätestens) 25. 8. 2023
- von 50 bis 249 Arbeitnehmern: bis (spätestens) 17. 12. 2023

Dokumentationspflichten

Gem § 9 HSchG sind von internen und externen Stellen alle eingehenden Hinweise zu dokumentieren. Ihr Eingang ist den Hinweisgeberinnen und Hinweisgebern unverzüglich, spätestens aber innerhalb von sieben Tagen zu bestätigen. Erfolgt der Hinweis mündlich, so sind die Stellen nach Zustimmung der Hinweisgeberinnen und Hinweisgeber berechtigt, Tonaufzeichnungen oder Transkriptionen des Gesprächs anzufertigen.

Datenschutzrechtliche Aspekte

Als **Verantwortliche** iSd Art 4 Z 7 DSGVO gelten die jeweiligen Behörden bzw Unternehmen. Hinweisgeberinnen und Hinweisgeber gelten nur dann als Verantwortliche, wenn sie personenbezogene Daten verarbeiten, die über das erforderliche Ausmaß für die Verfolgung des Hinweises hinausgehen. Insb wird der Grundsatz der Datenminimierung des Art 5 Abs 1 lit c DSGVO zu beachten sein.

Bei gemeinsamem Betrieb eines WBS innerhalb einer **Konzerngesellschaft** sind diese gemeinsame Verantwortliche iSd Art 26 DSGVO.

Entspricht das implementierte WBS den Bestimmungen des HSchG, dann dient dieses iVm Art 6 Abs 1 lit c DSGVO als **Rechtsgrundlage**. Geht das WBS über die Rechtsbereiche des HSchG hinaus, kann die Datenverarbeitung gegebenenfalls auf das berechtigte Interesse des Verantwortlichen iSd Art 6 Abs 1 lit f DSGVO – allerdings erst nach einer Abwägung mit den Interessen des Betroffenen, die zugunsten des Verantwortlichen ausfällt – gestützt werden.

Grundsätzlich benötigt ein WBS, das den Bestimmungen des HSchG entspricht, **keine DSFA** gem Art 35 DSGVO, da der Gesetzgeber eine solche gem Art 35 Abs 10 und ErwGr 92 bereits auf abstrakter Ebene durchgeführt hat. Nur wenn das WBS über den Rechtsbereich des HSchG hinausgeht, wird eine DSFA durchzuführen sein.

Nach den Bestimmungen des § 8 Abs 9 HSchG **entfallen** folgende in der DSGVO normierte **Betroffenenrechte**, allerdings nur so lange und insoweit dies zum Schutz der Identität einer Hinweisgeberin oder eines Hinweisgebers oder zum Erreichen der Zwecke des WBS erforderlich ist:

- Recht auf Information (§ 43 DSG; Art 13, 14 DSGVO);
- Recht auf Auskunft (§ 1 Abs 3 Z 1, § 44 DSG; Art 15 DSGVO);
- Recht auf Berichtigung (§ 1 Abs 3 Z 2, § 45 DSG; Art 16 DSGVO);
- Recht auf Löschung (§ 1 Abs 3 Z 2, § 45 DSG; Art 17 DSGVO);
- Recht auf Einschränkung der Verarbeitung (§ 45 DSG; Art 18 DSGVO);
- Widerspruchsrecht (Art 21 DSGVO) sowie
- Recht auf Benachrichtigung von einer Verletzung des Schutzes personenbezogener Daten (§ 56 DSG; Art 34 DSGVO).

Die Unternehmen und juristischen Personen des öffentlichen Sektors haben aber sicherzustellen, dass Hinweisgeberinnen und Hinweisgeber sowie zusätzliche Personen, die von § 2 HSchG umfasst sind, Zugang zu Informationen über das implementierte WBS erhalten. Am besten wird das durch eine Information auf der Website sichergestellt werden können.

§ 8 Abs 11 HSchG sieht nun eine fünfjährige **Aufbewahrungsfrist** für personenbezogene Daten ab ihrer letzten Verarbeitung oder Übermittlung vor, während der ME noch eine dreißigjährige Aufbewahrungsfrist normierte. Nach § 8 Abs 12 HSchG sind durchgeführte Verarbeitungsvorgänge wie insb Änderungen, Abfragen und Übermittlungen zu protokollieren und drei Jahre nach Entfall der Aufbewahrungsfrist gem Abs 11 zu löschen.

Informationssicherheitstechnische Aspekte

Informationssicherheitstechnische Aspekte werden im HSchG nur rudimentär angesprochen. So enthält § 7 Abs 1 HSchG die Forderung, dass die Identität von Hinweisgeberinnen und Hinweisgebern durch die Meldestelle zu schützen ist. Weites enthält § 11 Abs 1 HSchG die Forderung, dass das WBS technisch und organisatorisch den Bestimmungen des Art 25 DSGVO entsprechen muss. Gem § 16 Abs 3 HSchG, der die Eignung der Meldekanäle externer Stellen regelt, müssen WBS den Schutz der Identität von Hinweisgebern und Hinweisgeberinnen sowie der von einem Hinweis betroffenen Personen, die Vertraulichkeit, den Datenschutz und die Verwendung standardisierter, dem Stand der Technik entsprechender Soft- und Hardware für das WBS gewährleisten.

Sanktionen

Die (versuchte) Behinderung von Hinweisgeberinnen und Hinweisgebern iZm einer Hinweisgebung, die Setzung der in § 20 HSchG genannten Maßnahmen zur Vergeltung der Hinweisgebung, die Verletzung der Vertraulichkeit oder die wissentliche Abgabe eines falschen Hinweises wird mit einer **Verwaltungsstrafe** bis zu € 20.000,– bzw im Wiederholungsfall mit bis zu € 40.000,– sanktioniert.

Für die Nichteinrichtung von internen Meldekanälen sieht das HSchG **allerdings keine Sanktion vor.**

Die Checkliste enthält Prüffragen, die Sie bei der Umsetzung des HSchG unterstützen sollen. Auch für Unternehmen, die bereits ein WBS eingeführt haben, ist die eine oder andere Prüffrage sicher von Interesse. Va wird bei bereits implementierten WBS zu prüfen sein, ob sie den Bestimmungen des HSchG entsprechen und welche zusätzlichen Maßnahmen zu treffen sind, wenn dies nicht der Fall ist.

Prüffragen

Prüffrage	ja	nein
Frage 1: Sind in Ihrem Unternehmen die notwendigen Voraussetzungen für die Einführung eines WBS gegeben? **Anmerkung:** *Voraussetzung für die erfolgreiche Einführung eines WBS ist es, Vorbehalte der Mitarbeiterinnen und Mitarbeiter auszuräumen und ihnen zu erklären, dass Sinn und Zweck dieser Maßnahme nicht die ungefilterte Verdächtigung anderer Personen ist („Vernadern"), sondern das Aufdecken schwerwiegender Missstände im Unternehmen. Es ist idZ unbedingt notwendig, frühzeitig zentrale Stakeholder wie das Management, die Personalabteilung, das Marketing, die IT-Abteilung, den BR und auch den DSBA (Datenschutzbeauftragten) in den Entscheidungsprozess vor Einführung eines WBS einzubinden.*		
Frage 2: Wurde vor Einführung des WBS geprüft, ob eine entsprechende Rechtsgrundlage vorliegt? **Anmerkung:** *Entspricht das WBS den Bestimmungen des HSchG, dann dient dieses iVm Art 6 Abs 1 lit c DSGVO als Rechtsgrundlage. Wenn das WBS zusätzlich Rechtsbereiche abdeckt, die vom HSchG nicht umfasst sind, kann die Datenverarbeitung auf das berechtigte Interesse des Verantwortlichen gem Art 6 Abs 1 lit f DSGVO gestützt werden; dies allerdings erst nach einer Abwägung mit den Interessen des Betroffenen, die zugunsten des Verantwortlichen ausfällt, und unter Beachtung der arbeitsrechtlichen Bestimmungen.*		
Frage 3: Wurde vor Einführung des WBS eine BV abgeschlossen bzw bei Nichtvorhandensein eines BR die Einwilligung aller Mitarbeiterinnen und Mitarbeiter eingeholt? **Anmerkung:** *Entspricht das WBS den Bestimmungen des HSchG, so ist nach mM idR der Abschluss einer BV nicht notwendig, da eine gesetzliche Verpflichtung zur Einrichtung eines solchen Systems besteht. Geht das Meldesystem jedoch über das HSchG hinaus und wird die Menschenwürde berührt, so ist das Mitwirkungsrecht des BR (insb §§ 96ff ArbVG) zu beachten und eine BV abzuschließen.* *Grundsätzlich kommen folgende Formen einer BV in Frage:* ■ **§ 96 Abs 1 Z 3 ArbVG:** *Wird das WBS als Kontrollmaßnahme eingesetzt, welche die Menschenwürde berührt – das wird bei den meisten WBS der Fall sein –, so hat der BR de facto ein Vetorecht gegen die Implementierung des Systems und seine Zustimmung im Rahmen einer BV ist für die Rechtswirksamkeit dieser Maßnahme erforderlich.* ■ **§ 96a Abs 1 Z 1 ArbVG:** *Ist das WBS mit automationsunterstützter Datenerfassung, -verarbeitung bzw -weitergabe verknüpft, so bedarf es ebenfalls der Zustimmung des BR. Diese kann jedoch durch die Entscheidung der Schlichtungsstelle ersetzt werden.* ■ **§ 97 Abs 1 Z 1 ArbVG:** *Diese Norm bietet die Rechtsgrundlage für allgemeine Ordnungsvorschriften, die das Verhalten im Betrieb regeln, und erfordert den Abschluss einer erzwingbaren BV.* *Bei Unternehmen, die über keinen BR verfügen und in denen somit der Abschluss einer BV gem § 96 Abs 1 Z 3 ArbVG nicht möglich ist, ist das Recht jedes einzelnen Mitarbeiters und jeder einzelnen Mitarbeiterin zu beachten und gem § 10 Abs 1 AVRAG die Einwilligung jedes einzelnen Mitarbeiters und jeder einzelnen Mitarbeiterin einzuholen.*		
Frage 4: Wurde der DSBA frühzeitig über die Einführung des WBS informiert? **Anmerkung:** *Dem DSBA kommt die Aufgabe zu, vor Inbetriebnahme des WBS die Einhaltung der datenschutzrechtlichen Grundsätze zu prüfen. Insb wird er zu prüfen haben, ob die Durchführung einer DSFA erforderlich ist.*		
Frage 5: Wird für den Betrieb des WBS ein externer Dienstleister eingesetzt? **Anmerkung:** *Wird ein externer Dienstleister teilweise oder zur Gänze mit dem Betrieb des WBS betraut, dann ist nach den Bestimmungen des Art 28 DSGVO eine Auftragsverarbeitungsvereinbarung abzuschließen.*		
Frage 6: Wird das WBS von mehreren Unternehmen gemeinsam betrieben? **Anmerkung:** *Soweit Verantwortliche iSd Art 4 Z 7 DSGVO ein WBS gemeinsam betreiben, so sind sie nach den Bestimmungen des § 8 Abs 4 Z 4 HSchG gemeinsam Verantwortliche iSd Art 26 DSGVO.*		
Frage 7: Wird ein WBS eingesetzt, das bereits vor der Geltung der DSGVO einer Vorabkontrolle der DSB unterzogen wurde? **Anmerkung:** *In diesem Fall ist die Durchführung einer DSFA entbehrlich.*		
Frage 8: Wurde vor dem Einsatz des WBS eine DSFA durchgeführt? **Anmerkung:** *Die Durchführung einer DSFA ist nur dann notwendig, wenn das WBS über die Rechtsbereiche des HSchG hinausgeht.*		
Frage 9: Wird der Personenkreis, der für die Nutzung des WBS in Frage kommt, über das Verfahren angemessen informiert? **Anmerkung:** *Der für die Nutzung des WBS in Frage kommende Personenkreis wird in § 2 HSchG definiert und hat gem § 10 HSchG einfachen Zugang zu klaren Informationen über das WBS zu erhalten. Am besten wird das durch eine Information auf der Website sichergestellt werden können. Der Mindestinhalt einer solchen Information kann § 10 Abs 2 HSchG entnommen werden.*		
Frage 10: Enthält die Information über das WBS eine klare Definition der meldefähigen Verstöße und wurden diese entsprechend kommuniziert? **Anmerkung:** *Neben dem in § 3 HSchG definierten „sachlichen Geltungsbereich" könnten uU auch noch andere für das Unternehmen relevante Inhalte definiert werden. Dabei sind mögliche Auswirkungen auf das Erfordernis einer DSFA sowie auf die arbeitsrechtlichen Bestimmungen zu beachten.*		

Prüffrage	ja	nein
Frage 11: Enthält die Information über das WBS eine klare Festlegung der zulässigen Hinweisgeberinnen und Hinweisgeber? ***Anmerkung:*** *§ 2 HSchG enthält eine detaillierte Aufzählung jener Personen, die vom Geltungsbereich umfasst sind. Das sind generell Personen, die aufgrund beruflicher Verbindung zu einem Rechtsträger des privaten oder des öffentlichen Sektors Informationen über Rechtsverletzungen erlangt haben.*		
Frage 12: Werden die Hinweisgeberinnen und Hinweisgeber angeregt, für ihre Hinweise die interne Meldestelle und nicht externe Meldestellen zu wählen? ***Anmerkung:*** *§ 11 HSchG fordert, dass WBS in einer Weise einzurichten sind, die Hinweisgeberinnen und Hinweisgeber zur Bevorzugung der internen Meldestelle anregt.*		
Frage 13: Wird die Identität der Hinweisgeberinnen und Hinweisgeber durch die internen und externen Stellen entsprechend geschützt? ***Anmerkung:*** *§ 7 Abs 1 HSchG fordert den Schutz der Identität von Hinweisgeberinnen und Hinweisgeber durch die internen und externen sowie die mit den Aufgaben der internen Stelle beauftragten Stellen während des Untersuchungsprozesses. Dieser Schutz kann durch entsprechende IT-Sicherheitsmaßnahmen wie ein flexibles Rechte- und Rollenprinzip, datenschutzkonforme Pseudonymisierung und Anonymisierung sowie durch entsprechende Arbeitsanweisungen an die Mitarbeiterinnen und Mitarbeiter der internen und externen Stellen erreicht werden.*		
Frage 14: Wurde geregelt, unter welchen Umständen die Identität der Hinweisgeberin oder des Hinweisgebers offengelegt werden darf? ***Anmerkung:*** *Nach den Bestimmungen des § 7 Abs 3 HSchG darf die Identität der Hinweisgeberinnen und Hinweisgeber nur dann offengelegt werden, wenn eine Verwaltungsbehörde, ein Gericht oder die Staatsanwaltschaft diese im Rahmen eines verwaltungsbehördlichen oder gerichtlichen Verfahrens oder eines Ermittlungsverfahrens nach der StPO für unerlässlich hält, wobei die Verhältnismäßigkeit dieser Maßnahme zu prüfen ist. Sollen Daten der Hinweisgeberin oder des Hinweisgebers offengelegt werden, so sind diese gem § 7 Abs 4 HSchG von der Behörde vor der Offenlegung zu unterrichten.*		
Frage 15: Ist sichergestellt, dass Hinweise, die offenkundig falsch gegeben werden, im Rahmen des WBS zurückgewiesen werden? ***Anmerkung:*** *§ 6 Abs 4 HSchG fordert die Zurückweisung von offenkundig falschen Hinweisen sowie eine nachrichtliche Meldung an die Hinweisgeberin oder den Hinweisgeber mit einem Hinweis auf mögliche Schadenersatzansprüche, die in § 24 HSchG normiert sind. Nach den Bestimmungen des § 9 Abs 1 HSchG ist jedoch jeder Hinweis auf seine Stichhaltigkeit zu prüfen.*		
Frage 16: Ermöglicht der Meldekanal die Abgabe der Hinweise in schriftlicher und/oder mündlicher Form? ***Anmerkung:*** *Die Art des Meldekanals wird den Unternehmen nicht exakt vorgeschrieben. Gem § 13 Abs 5 HSchG müssen die Hinweise der internen Stelle aber schriftlich oder mündlich oder in beiden Formen gegeben werden können, auch anonyme Hinweise müssen möglich sein. Grundsätzlich gibt es* ***fünf verschiedene Meldekanäle,*** *und zwar:* ■ **Briefkasten:** Aufstellung eines Briefkastens im Unternehmen, in den Hinweisgeber Meldungen einwerfen können. ■ **E-Mail:** Einrichtung eines zentralen E-Mailkontos, an das Hinweise gesendet werden können. ■ **Ombudsmann:** Bestellung einer externen Person (in der Regel ein Anwalt), der als Anlaufstelle für Hinweisgeber und Hinweisgeberinnen dient. ■ **Telefon:** Einrichtung einer zentralen Telefonnummer, unter der Hinweise abgegeben werden können. ■ **Digitales WBS:** Einrichtung einer Onlineplattform für Hinweisgeber und Hinweisgeberinnen. *Der Leitfaden für die Einführung von Hinweisgebersystemen der EQS-Group[3] bietet eine sehr gute Gegenüberstellung der Vor- und Nachteile der einzelnen Meldekanäle.*		
Frage 17: Ist die interne Stelle mit den zur Erfüllung ihrer Aufgaben notwendigen finanziellen und personellen Mitteln ausgestattet? ***Anmerkung:*** *Diese Forderung entspricht § 13 Abs 1 HSchG. Als interne Stelle wird gem § 5 Z 6 HSchG jene Person oder Abteilung oder sonstige Organisationseinheit innerhalb eines Unternehmens oder einer juristischen Person des öffentlichen Sektors bezeichnet, die Hinweise entgegennimmt, überprüft sowie im Hinblick auf Folgemaßnahmen oder sonst weiter behandelt.*		
Frage 18: Ist durch die interne Meldestelle die Entgegennahme und Behandlung von Hinweisen unparteilich und unvoreingenommen sichergestellt und erfolgt die Bestätigung des Eingangs der Meldung unverzüglich, spätestens jedoch nach 7 Kalendertagen? ***Anmerkung:*** *Nach den Bestimmungen des § 13 Abs 2 HSchG sind jedenfalls Vorkehrungen zu treffen, um internen Stellen die weisungsfreie Erledigung der Hinweise zu ermöglichen. § 9 Abs 1 HSchG fordert eine schriftliche Bestätigung des Eingangs des Hinweises an die Hinweisgeberin oder den Hinweisgeber unverzüglich, jedoch spätestens nach 7 Kalendertagen.*		
Frage 19: Ist sichergestellt, dass auf Ersuchen einer Hinweisgeberin oder eines Hinweisgebers eine Zusammenkunft zur Besprechung des Hinweises stattfinden kann? ***Anmerkung:*** *§ 13 Abs 5 HSchG fordert, dass derartigen Ersuchen einer Hinweisgeberin oder eines Hinweisgebers innerhalb von 14 Kalendertagen zu entsprechen ist.*		
Frage 20: Ist sichergestellt, dass Hinweisgeberinnen und Hinweisgeber ihre Hinweise ergänzen oder berichtigen können? ***Anmerkung:*** *Diese Forderung ergibt sich aus den Bestimmungen des § 13 Abs 8 HSchG. Auf Verlangen ist die Entgegennahme von Ergänzungen oder Berichtigungen spätestens nach 7 Kalendertagen schriftlich zu bestätigen.*		
Frage 21: Ist eine Rückmeldung an die Hinweisgeberin und den Hinweisgeber, welche Maßnahmen ergriffen worden sind, innerhalb angemessener Zeit möglich? ***Anmerkung:*** *§ 13 Abs 9 HSchG fordert, dass spätestens 3 Monate nach Entgegennahme eines Hinweises die Hinweisgeberin oder der Hinweisgeber darüber zu informieren ist, welche Folgemaßnahmen ergriffen wurden bzw aus welchen Gründen der Hinweis nicht weiterverfolgt wird.*		
Frage 22: Ist sichergestellt, dass personenbezogene Daten, die für die Bearbeitung eines Hinweises nicht benötigt werden, unverzüglich gelöscht werden? ***Anmerkung:*** *Nach den Bestimmungen des § 8 Abs 10 HSchG dürfen Daten, die zur Bearbeitung eines Hinweises nicht benötigt werden, nicht erhoben werden bzw sind unverzüglich zu löschen, falls sie unbeabsichtigt erhoben wurden.*		
Frage 23: Ist die fünfjährige Aufbewahrungsfrist für personenbezogene Daten sichergestellt? ***Anmerkung:*** *Nach den Bestimmungen des § 8 Abs 11 HSchG sind die personenbezogenen Daten ab ihrer letztmaligen Verarbeitung oder Übermittlung fünf Jahre und darüber hinaus so lange aufzubewahren, wie sie zur Durchführung bereits eingeleiteter verwaltungsbehördlicher oder gerichtlicher Verfahren oder eines Ermittlungsverfahrens nach der StPO erforderlich sind. Nach Ablauf der Aufbewahrungsfrist sind diese Daten unverzüglich zu löschen.*		

[3] https://www.integrityline.com/de/knowhow/white-paper/hinweisgeberschutz-fuer-unternehmen/

Prüffrage	ja	nein
Frage 24: Werden Verarbeitungsvorgänge protokolliert? **Anmerkung:** § 8 Abs 12 HSchG fordert die Protokollierung durchgeführter Verarbeitungsvorgänge wie insb Änderungen, Abfragen und Übermittlungen sowie die Aufbewahrung dieser Protokolle bis 3 Jahre nach Entfall der fünfjährigen Aufbewahrungspflicht (s Frage 23).		
Frage 25: Ist die Dokumentation von mündlichen Hinweisen gewährleistet? **Anmerkung:** § 9 Abs 2 HSchG erlaubt – bei Zustimmung der Hinweisgeberin oder des Hinweisgebers – die Tonaufzeichnung eines mündlich abgegebenen Hinweises oder eine Transkription des Gesprächs. Nach Möglichkeit ist der Hinweisgeberin und dem Hinweisgeber Gelegenheit zu geben, das Transkript zu prüfen und zu berichtigen.		
Frage 26: Kann der Hinweisgeber oder die Hinweisgeberin über ein personalisiertes Log-in auf das WBS zugreifen? **Anmerkung:** Die Anmeldemethode zum WBS und die zugehörigen Sicherheitsmaßnahmen müssen dem Schutzbedarf der übermittelten Inhalte angepasst werden. Weiters muss sichergestellt sein, dass durch Abfragen zur Authentifizierung nicht die Anonymität des Hinweisgebers und der Hinweisgeberin aufgehoben wird.		
Frage 27: Ermöglicht der gewählte Meldekanal dem Hinweisgeber, Bilder, Videos oder Textdateien zu übermitteln? **Anmerkung:** Je nach Art des Hinweises kann es notwendig sein, dass der Hinweisgeber und die Hinweisgeberin über die Meldung des entdeckten Missstandes hinaus ergänzende Materialien wie Dateien und Dokumente übermitteln muss.		
Frage 28: Ist im Rahmen des WBS die rechtskonforme Information der beschuldigten Personen sichergestellt? **Anmerkung:** Wenn personenbezogene Daten ohne Wissen der betroffenen Person (idF Beschuldigte) erhoben werden, so haben diese gem Art 14 DSGVO das Recht auf Information. Diese Informationspflicht kann allerdings nach den Bestimmungen des § 8 Abs 9 HSchG unterbleiben, wenn sie die Klärung und Verfolgung des aufgezeigten Missstandes gefährden würde. Diese Feststellung gilt auch in Bezug auf andere Betroffenenrechte wie Auskunft, Berichtigung, Löschung, Einschränkung und Widerspruch sowie die Benachrichtigung bei einem Data Breach.		
Frage 29: Enthält das WBS auch ein integriertes Fallmanagement-System (Case Management System)? **Anmerkung:** Das Fallmanagement-System sollte einfach zu bedienen sein und Funktionen bieten, die vom Empfang der Meldung über die Bearbeitung bis zur Verwaltung von Bearbeitungsvorgängen reichen. Es sollte weiters den Dialog zwischen dem Hinweisgeber oder der Hinweisgeberin und dem Fallmanager (Bearbeiter der Meldung) unterstützen.		
Frage 30: Verfügt das eingesetzte WBS über eine Sicherheitszertifizierung? **Anmerkung:** Ein WBS, das zB über eine ISO-27001-Zertifizierung verfügt, gewährleistet idR auch ausreichende Datensicherheit.		

Dako 2023/21

Zum Thema

Über den Autor

Prof. KommR Hans-Jürgen Pollirer ist Senior Management Consultant bei der Secur-Data Betriebsberatungs-GmbH und fachkundiger Laienrichter für Datenschutz am BVwG sowie juristischer und technischer EuroPriSe-Gutachter. E-Mail: hj.pollirer@secur-data.at

Literatur

- *Aigner*, Magisterarbeit „Whistleblowing in Österreich" (2011), http://othes.univie.ac.at/17347/1/2011-12-07_0948255.pdf;
- *Aschauer*, Whistleblowing im Arbeitsrecht (2012);
- *Grünanger/Goricnik* (Hrsg), Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle² (2018)
- *Hauser/Bretti-Rainalter/Blumer*, Whistleblowing Report 2021 (2021), www.integrityline.com/de/knowhow/white-paper/whistleblowing-report/;
- EDPS, Leitlinien zur Verarbeitung personenbezogener Daten im Rahmen eines Verfahrens zur Meldung von Missständen (2019); https://edps.europa.eu/system/files/2021-07/19-12-17_whisteblowing_guidelines_en_195_de.pdf;
- *Gruber/M. Raschauer* (Hrsg), Whistleblowing (2015).

Viktoria Haidinger
Wirtschaftskammer Österreich

Fragen aus der Praxis

Ein Betroffener hat einen Auskunftsantrag gestellt und diesen mit einer digitalen Signatur unterschrieben. Reicht das als Identitätsnachweis?

Seit Wirksamwerden der DSGVO darf der Verantwortliche nur bei begründeten Zweifeln an der Identität des Antragstellers weitere Informationen anfordern, die zur Bestätigung der Identität der Person erforderlich sind (Art 12 Abs 3 DSGVO). Wenn Sie solche Zweifel gar nicht haben, zB bei Mitarbeitern, dürfen Sie keine zusätzlichen Informationen anfordern.

Eine digitale Signatur ist als Identitätsnachweis geeignet (BVwG 27. 5. 2020, W214 2228346-1; 23. 4. 2021, W211 2228343-1), aber auch eine Ausweiskopie bleibt ein geeigneter Nachweis der Identität von Antragstellern (DSB 31. 7. 2019, DSB-D123.901/0002-DSB/2019).

Dako 2023/22

Ich möchte die ID Austria im Unternehmen einsetzen, allerdings ohne Verarbeitung biometrischer Merkmale. Geht das?

Das ist grundsätzlich möglich: Voraussetzung ist, dass jeder Mitarbeiter eine ID Austria mit Vollfunktion und einen sog FIDO-Token hat. Diese gibt es in unterschiedlichen Ausführungen, wie zB den „GoTrust Idem Key FIDO2" in USB-A oder USB-C Ausführung, beide sind auch NFC-fähig. Der Mitarbeiter muss diesen FIDO-Token personalisieren, ua durch Hinterlegung in seinem A-Trust Konto. Die Handhabung funktioniert ähnlich wie bei den Signaturkarten: Das Gerät steckt im Computer bzw ist per NFC verbunden. Soll die ID Austria eingesetzt werden, zB für einen Login über einen Browser oder die Signatur eines Dokuments im Programm pdf over, sind Benutzername und Signatur Passwort sowie anschließend der Signatur Code einzugeben. Mit einem Tippen auf den FIDO-Token wird der Prozess abgeschlossen.

Hinweis: Erfahrungsgemäß können Browser-Erweiterungen die Funktionalität der ID Austria stören, so etwa das Plugin der Sprachsoftware Dragon (getestet mit Chrome).

Dako 2023/23

Kann ich auch am Handy den FIDO-Token einsetzen?

Obschon sich der FIDO-Token mit dem Handy mittels USB-C oder NFC verbinden lässt, kann er laut schriftlicher Auskunft des Bürgerservice-Teams des BRZ nur für Webanmeldungen am PC genutzt werden. Die Verwendung der ID Austria auf einem Smartphone (mit Android) oder einem iPhone ist daher (derzeit?) nicht möglich.

Dako 2023/24

Mein Mitarbeiter hat noch keine ID Austria mit Vollfunktion. Wie kommt er ohne Biometrie am Handy zu einer solchen?

Nutzer einer behördlich ausgestellten Handy Signatur (zB über Finanz Online), die über einen gültigen Pass oder Personalausweis verfügen, können ihre Handy Signatur über die App Digitales Amt umstellen. Sollte Ihr Mitarbeiter eine Handy Signatur von einer nicht-behördlichen Registrierungsstelle ausgestellt bekommen haben oder eben die App Digitales Amt nicht nutzen wollen oder können, bleibt ihm ein Behördengang zu Polizei, Bezirksverwaltungsbehörde oder Finanzamt (Terminvereinbarung ist meist notwendig!) nicht erspart. Wohl nur mit „legistischer Vereinfachung" lässt sich begründen, dass in diesem Fall jeder mit Passfotos bei der Behörde vorstellig werden muss, also auch Personen, die einen gültigen Pass oder Personalausweis haben. Ein SMS-fähiges Handy ist zum Empfang einer SMS-TAN ebenfalls notwendig. Als Abschluss des Behördentermins erhält Ihr Mitarbeiter einen Zettel, auf dem die vorläufigen Login-Daten vermerkt sind. Für den Erstlogin hat man genau eine Chance, dh, vertippt man sich bei den Login-Daten, heißt es zurück zur Behörde.

www.oesterreich.gv.at/id-austria/registrierungsuebersicht/registrierung-per-sms-und-fido.html

Dako 2023/25

Eva Souhrada-Kirchmayer
Richterin am BVwG[1]

Rechtsprechung

„Medienprivileg": Aufhebung des § 9 Abs 1 DSG. Der VfGH hob das Medienprivileg wegen Verstoßes gegen das Grundrecht auf Datenschutz gem § 1 Abs 1 DSG auf. Der undifferenzierte Ausschluss der Anwendung aller (einfachgesetzlichen) Regelungen des DSG sowie einer Reihe von Kapitel der DSGVO widerspricht einer sachgerechten Abwägungspflicht.

Anlassfälle

Den Anträgen des BVwG auf Aufhebung des Medienprivilegs lagen zwei beim beantragenden Senat anhängige Beschwerdeverfahren zugrunde.

In einem Fall[2] brachte der Beschwerdeführer vor, dass ein Medienunternehmen auf seiner Homepage ua Bildaufnahmen veröffentlicht habe, wobei auf einer Bildaufnahme die Visitenkarte des Beschwerdeführers ungeschwärzt abgebildet worden sei.

Im anderen Fall[3] brachten zwei beschwerdeführende Parteien zusammengefasst vor, eine Verlagsgesellschaft und ein Rundfunkunternehmen hätten über ein „Datenleck" bei einem der zweitbeschwerdeführenden Partei zuzurechnenden E-Mail-Postfach, das in der Verfügungsmacht der erstbeschwerdeführenden Partei stehe, berichtet und nähere Umstände rechtswidrig offengelegt.

In beiden Fällen wurde zunächst bei der DSB eine **Verletzung des Grundrechts auf Geheimhaltung** (§ 1 Abs 1 DSG) geltend gemacht.

Die DSB wies in beiden Fällen die Beschwerden mit der Begründung **zurück**, dass es sich bei den Beschwerdegegnern um Medienunternehmen handle, die die Daten im Rahmen journalistischer Berichterstattung veröffentlicht hätten. Aufgrund der Anwendung des Medienprivilegs gem § 9 Abs 1 DSG sei die DSB unzuständig.

Gegen diese Bescheide erhoben die beschwerdeführenden Parteien jeweils **Beschwerde an das BVwG.**

[1] Prof. Dr. *Eva Souhrada-Kirchmayer* ist Richterin am BVwG und dort auch Vorsitzende eines Datenschutzsenats. Der Beitrag gibt ausschließlich ihre persönliche Meinung wieder und bindet das BVwG in keinem allfälligen Verfahren. [2] G 287/2022. [3] G 288/2022.

Aus Anlass dieser Beschwerden entstanden beim BVwG **Bedenken ob der Verfassungskonformität** des § 9 Abs 1 DSG. Das BVwG beantragte daher beim VfGH die **Aufhebung des § 9 Abs 1 DSG.**

Inhalt des Medienprivilegs

§ 9 Abs 1 DSG lautet:

(1) Auf die Verarbeitung von personenbezogenen Daten durch Medieninhaber, Herausgeber, Medienmitarbeiter und Arbeitnehmer eines Medienunternehmens oder Mediendienstes im Sinne des Mediengesetzes […] zu journalistischen Zwecken des Medienunternehmens oder Mediendienstes finden die Bestimmungen dieses BG sowie von der DSGVO die Kapitel II (Grundsätze), III (Rechte der betroffenen Person), IV (Verantwortlicher und Auftragsverarbeiter), V (Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen), VI (Unabhängige Aufsichtsbehörden), VII (Zusammenarbeit und Kohärenz) und IX (Vorschriften für besondere Verarbeitungssituationen) keine Anwendung. Die DSB hat bei Ausübung ihrer Befugnisse gegenüber den im ersten Satz genannten Personen den Schutz des Redaktionsgeheimnisses (§ 31 MedienG) zu beachten.

Aufhebungsanträge

In seinen Aufhebungsanträgen führte das BVwG aus, es hege primär Bedenken, dass eine **Geltendmachung des Grundrechts auf Datenschutz** im Anwendungsbereich des § 9 Abs 1 DSG **faktisch ausgehebelt werde**, da aufgrund des in dieser Bestimmung normierten Ausschlusses der Bestimmungen des DSG – und damit auch der **Unanwendbarkeit des § 24 Abs 1 DSG** – (sowie des gesamten Kapitel VI der DSGVO) einer betroffenen Person keine nationale Aufsichtsbehörde zur Verfügung stehe, um eine Verletzung des Grundrechts geltend zu machen.

Nach der **Rsp des VwGH** räume ausschließlich § 24 DSG der in ihrem persönlichen Grundrecht verletzten Person die Möglichkeit ein, die ihr gegenüber geschehene Rechtsverletzung feststellen zu lassen.[4]

Selbst bei Annahme einer unmittelbaren Anwendbarkeit des Art 77 DSGVO ergebe sich das Problem, dass dieser von seinem Wortlaut her (lediglich) auf gegenwärtig noch andauernde Rechtsverletzungen abzustellen scheine. Dementsprechend **sehe Art 58 DSGVO keine Feststellungsbefugnisse**, sondern Untersuchungs-, Abhilfe- und Genehmigungsbefugnisse **vor.**

Zwar könne wegen der unmittelbaren Anwendbarkeit von Art 79 DSGVO unter ergänzender Heranziehung von § 1 JN **bei einer Verletzung der DSGVO eine Zuständigkeit der Zivilgerichte** angenommen werden. Allerdings lasse sich im gegenständlichen Fall, in dem die Feststellung einer Verletzung des Grundrechts auf Geheimhaltung geltend gemacht worden sei, unter Heranziehung des Art 79 DSGVO gar **keine gerichtliche Zuständigkeit** begründen, da Art 79 lediglich auf Verletzungen der DSGVO Bezug nehme, **nicht aber auf nationale Gesetze wie das DSG.**

Selbst wenn man von einer Gerichtszuständigkeit ausginge, wäre die Regelung des § 9 Abs 1 DSG schon deshalb **unsachlich**, weil das Beschwerderecht bei der DSB niederschwelliger wahrgenommen werden könne (zB unentgeltliche Einbringung einer Beschwerde bei der DSB, keine Anwaltspflicht) als eine Klage beim zuständigen Landesgericht für Zivilrechtssachen.

Art 85 Abs 2 DSGVO erteile den MS den Auftrag, *„Abweichungen und Ausnahmen"* von bestimmten Kapiteln der DSGVO vorzusehen, **wenn dies als Ergebnis einer Interessenabwägung erforderlich sei** *(„um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen")*, wobei diese Interessenabwägung in § 9 Abs 1 DSG nicht abgebildet sei.

Neben der Verletzung des Grundrechts auf Datenschutz machte das BVwG auch eine Verletzung im **Gleichheitsgrundsatz**, eine Verletzung des **Verfahrens vor dem gesetzlichen Richter** und des **Art 8 GRC** (und Art 8 EMRK) geltend.

Vorbringen der Parteien

Die BReg teilte mit, dass sie von einer meritorischen Äußerung absehe. Die DSB gab eine Stellungnahme ab, in der sie die Verfassungskonformität des § 9 Abs 1 DSG behauptete. Zusammengefasst brachte die DSB vor, dass das Grundrecht auf Datenschutz nach § 1 DSG unmittelbar vor den Zivilgerichten geltend gemacht werden könne, sodass jedenfalls ein Rechtsschutzweg eröffnet sei.

Die DSB übersehe nicht, dass eine Klage wohl nicht auf Art 79 DSGVO gestützt werden könne, weil § 9 Abs 1 DSG ausdrücklich bestimmte Kapitel der DSGVO, insb die Kapitel II und III, ausnehme und somit dem angerufenen Gericht der Beurteilungsmaßstab für eine behauptete Verletzung der DSGVO entzogen wäre. Dies ändere allerdings nichts daran, dass eine Rechtsschutzmöglichkeit nach dem Mediengesetz iVm § 1 DSG oder lediglich gestützt auf § 1 DSG bestehe und eine betroffene Person somit nicht völlig schutzlos dastehe.

Außerdem habe die DSB eine eingeschränkte Zuständigkeit zur Behandlung von Beschwerden – nämlich, soweit eine Datenschutzverletzung in Ausübung journalistischer Tätigkeit gegenüber anderen Akteuren als den in § 9 Abs 1 DSG genannten geltend gemacht werde – anerkannt.

Auch das im Verfahren G 287/2022 beteiligte Medienunternehmen sowie die beschwerdeführenden Parteien im Verfahren G 288/2022 gaben Stellungnahmen ab, in welchen sie ihre Standpunkte darlegten.

Erkenntnis des VfGH

Mit Erkenntnis vom 14. 12. 2022[5] wurde **§ 9 Abs 1 DSG als verfassungswidrig aufgehoben.** Die Aufhebung tritt mit **Ablauf des 30. 6. 2024** in Kraft.

In seinen Erwägungen fasste der VfGH zunächst im Wesentlichen die Argumente des BVwG und der DSB sowie der sonstigen Parteien zusammen.

In weiterer Folge stellte der VfGH die maßgebliche Rechtsentwicklung und die geltende Rechtslage dar. Bereits § 48 DSG 2000, welcher Art 9 DS-RL umsetzen hätte sollen, habe eine datenschutzrechtliche Sonderregelung für Datenverarbeitungen zu journalistischen Zwecken vorgesehen. Eine neue Regelung sei zunächst in § 9 Datenschutz-AnpassungsG 2018[6] getroffen worden. An dessen Stelle sei der nun (tw) angefochtene § 9 DSG getreten, welcher mit dem DS-DRG 2018[7] erlassen worden sei. Dieser gehe auf einen Abänderungsantrag im Nationalrat zurück.

§ 9 Abs 1 S 1 DSG statuiere nunmehr eine **gänzliche Ausnahme** in dem Sinne, dass Datenverarbeitungen durch bestimmte, in der Bestimmung genannte Akteure (Medieninhaber, Herausgeber, Medienmitarbeiter und Arbeitnehmer eines Medienunternehmens oder Mediendienste iSd Mediengesetzes) zu journalistischen Zwecken des Medienunternehmens oder Mediendienstes zur Gänze von den Bestimmungen

[4] VwGH 14. 12. 2021, Ro 2020/04/0032. [5] G 287/2022–16, G 288/2022–14. [6] BGBl I 2017/120. [7] BGBl I 2018/24.

des DSG sowie von den in § 9 Abs 1 DSG bezeichneten Kapiteln der DSGVO ausgenommen seien.

Die geltende und nun angefochtene Fassung des § 9 Abs 1 DSG weiche von (dem beschlossenen, aber nicht in Kraft getretenen) § 9 Datenschutz-AnpassungsG insoweit ab, als dieser keinen kategorischen ausnahmslosen Vorrang für die Freiheit der Meinungsäußerung und der Informationsfreiheit vorgesehen habe, sondern diesen Vorrang nur festgelegt habe, *„soweit dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen"*. Dieser sog Erforderlichkeitsvorbehalt finde sich nun nur mehr in § 9 Abs 2 DSG.

Die DSGVO regle das Verhältnis von Datenschutz und Medienfreiheit nicht selbst, sondern delegiere diese Rechtssetzungsaufgaben an die MS. Gem Art 85 Abs 1 DSGVO hätten die MS durch Rechtsvorschriften das Recht auf den Schutz personenbezogener Daten gem dieser VO mit dem Recht der freien Meinungsäußerung und Informationsfreiheit, einschließlich der Verarbeitung zu journalistischen Zwecken, in Einklang zu bringen.

Der Gesetzgeber unterliege einer doppelten Bindung, nämlich einer Bindung an das Unionsrecht und einer Bindung an den verfassungsgesetzlich gezogenen Rahmen.

Der Regelungsgehalt des § 9 Abs 1 DSG sei unionsrechtlich nicht zwingend vorgegeben, daher unterliege die Bestimmung der Kontrolle durch den VfGH im Hinblick auf ihre Übereinstimmung mit dem innerstaatlichen Verfassungsrecht.

Ob § 9 Abs 1 DSG den Vorgaben des Unionsrechtes (vollständig) entspreche, habe der VfGH nicht zu beurteilen und sei für die Entscheidung nicht von Belang.

§ 9 Abs 1 DSG verstoße nach Auffassung des VfGH gegen das Grundrecht auf Datenschutz gem § 1 Abs 1 DSG.

§ 9 Abs 1 DSG ordne zunächst undifferenziert an, dass *„die Bestimmungen dieses Bundesgesetzes"* nicht anwendbar seien. Es verbiete sich allerdings die Auslegung, dass damit auch die Verfassungsbestimmung des § 1 DSG nicht anwendbar sei, weil der einfache Gesetzgeber die Verfassungsbestimmung als Maßstab für die Verfassungskonformität des angefochtenen § 9 Abs 1 DSG nicht auszuschließen vermöge.

Das Grundrecht auf Datenschutz gem § 1 Abs 1 DSG gewährleiste jedermann Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit er daran ein schutzwürdiges Interesse, insb im Hinblick auf die Achtung des Privatlebens, habe.

§ 1 Abs 2 DSG enthalte hierzu einen materiellen Gesetzesvorbehalt. Abgesehen von der Verwendung personenbezogener Daten im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung seien Beschränkungen des Anspruches auf Geheimhaltung demnach nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig.

Der Gesetzgeber sei sohin aufgrund des Grundrechtes auf Datenschutz stets gehalten, eine **Abwägung zwischen dem Interesse des Betroffenen am Schutz seiner personenbezogenen Daten und den gegenläufigen (berechtigten) Interessen eines anderen** vorzusehen. Nur wenn die Wahrung der gegenläufigen, berechtigten Interessen eines anderen das Recht auf Datenschutz des Betroffenen überwiege, sei ein gesetzlicher Eingriff in das Grundrecht auf Datenschutz erlaubt.

Der in § 9 Abs 1 DSG normierte, absolute und gänzliche – und damit undifferenzierte – Ausschluss der Anwendung aller (einfachgesetzlichen) Regelungen des DSG sowie der dort genannten Kapitel der DSGVO auf näher definierte Datenverarbeitungen zu journalistischen Zwecken eines Medienunternehmens oder Mediendienstes widerspreche dem in § 1 Abs 2 DSG normierten Erfordernis, dass der Gesetzgeber das Interesse am Schutz personenbezogener Daten mit dem Interesse der Medieninhaber, Herausgeber, Medienmitarbeiter und Arbeitnehmer eines Medienunternehmens oder Mediendienstes (iSd MedG) im Rahmen ihrer journalistischen Tätigkeit sachgerecht abzuwägen habe.

Der Gesetzgeber sei gehalten, einen angemessenen, **differenzierten Ausgleich** zwischen den Interessen einzelner Personen auf Datenschutz auch gegenüber Medien und den durch Art 10 EMRK geschützten Anforderungen journalistischer Tätigkeit vorzusehen.

Zu denken sei idZ etwa an Einschränkungen in personeller (wie derzeit in § 9 Abs 1 DSG vorgesehen), zeitlicher (uU bis zur Veröffentlichung eines Berichts) oder sachlicher (zB hinsichtlich bestimmter Datenverarbeitungen oder Betroffenenrechte) Hinsicht. Ebenso könnte der Gesetzgeber – als Ausgleich für den Ausschluss (bestimmter) datenschutzrechtlicher Bestimmungen – erhöhte Anforderungen an die interne Organisation, Dokumentation und technische Sicherung der verarbeiteten Daten vorsehen.

Für die Verfassungskonformität des § 9 Abs 1 DSG könne auch nicht ins Treffen geführt werden, dass eine Geltendmachung von Datenschutzverletzungen durch Verarbeitungen zu journalistischen Zwecken zwar nicht vor der DSB, aber vor den ordentlichen Gerichten möglich sei.

§ 9 Abs 1 DSG erweise sich daher als verfassungswidrig. Bei diesem Ergebnis erübrige es sich, auf die sonstigen Bedenken des antragstellenden BVwG unter dem Aspekt weiterer Grundrechte einzugehen.

Ausblick

Der VfGH hat dem Gesetzgeber eine „Reparaturfrist" von über eineinhalb Jahren eingeräumt. Bis dahin steht die Bestimmung grundsätzlich noch weiter in Geltung. Ausgenommen sind die genannten Anlassverfahren, in welchen die Bestimmung nicht mehr anwendbar ist („Ergreiferprämie"). Dementsprechend wurden die Bescheide der DSB in diesen Fällen vom BVwG ersatzlos behoben und die Behörde muss nunmehr inhaltlich entscheiden.

Zu hoffen ist, dass in die zukünftige Regelung – so wie dies in der Vorgängerregelung des geltenden § 9 Abs 1 DSG der Fall war – auch der „Bürgerjournalismus" wieder miteinbezogen wird, da sich sonst weiterhin Fragen der Verfassungsmäßigkeit bzw Unionsrechtskonformität stellen könnten.

§ 1 DSG
VfGH 14. 12. 2022, G 287/2022 und G 288/2022

Dako 2023/26

DATKOMM, 64.–66. LFG

Knyrim (Hrsg), Der DatKomm 64.–66. Lfg. Verlag Manz, Wien 2022. Faszikel in 2 Mappen, ca 2.380 Seiten, € 248,–

RA Dr. Rainer Knyrim versprach schon 2018 die künftige laufende Ergänzung des Werks. Der Herausgeber hat sein Versprechen sowohl in Print als auch in online eingehalten. So erschienen zuletzt im Dezember 2022 die 64.–66. Lfg mit 202 Seiten, die nun kurz zu besprechen sind.

Autorin und Redaktionsmitglied Mag. *Viktoria Haidinger,* LL.M., behandelt das Recht auf Datenübertragbarkeit **(Art 20 DSGVO)**, also die Möglichkeit, dass die betroffene Person ihre Daten erhält, um sie weiterzuverwenden. Viele Zusätze in ihrem ursprünglichen Text, einem zusätzlichen Teil zur Datenübertragbarkeit in anderen Rechtsvorschriften (zB TKG 2021) und 96 zum Teil neue Fußnoten.

Art 21 DSGVO (das Recht, eine grundsätzlich zulässige Datenverarbeitung zu untersagen) wird mit einem komplettierten Literaturverzeichnis, einer neuen Gliederung der Übersicht sowie vielen Einfügungen im alten Text versehen; zB bei Verstoß der Datenverarbeitung gegen die DSGVO (also im Gegensatz zu „zulässig") oder zum Thema Direktwerbung bis zum Widerspruchsrecht im Rahmen des TKG 2021.

Art 22 DSGVO (Automatisierte Entscheidungen im Einzelfall einschließlich Profiling): Die betroffene Person soll durch diesen Artikel vor Entscheidungen im Einzelfall geschützt werden, die ausschließlich auf automatisierte Verarbeitung einschließlich Profiling beruhen.

Ein ergänztes Literaturverzeichnis, eine abgeänderte Übersicht über die einzelnen Abschnitte und praktisch ein neuer Text sowie 152 Fußnoten. Dabei prozessual interessant die FN 15: Bei einer Klage wegen eines Verstoßes gegen Art 22 bei Gericht (duales Verfahren, Beschwerde wäre auch bei der DSB möglich) ist der Weg bis zum OGH mangels einer Beschränkung durch einen geringen Streitwert offen, weil eine Bewertung des Streitwerts durch das Berufungsgericht zu unterbleiben hat, da es sich bei Betroffenenrechten um höchstpersönliche Rechte handelt. Die Zulässigkeit der Revision hängt nur vom Vorliegen einer erheblichen Rechtsfrage iSd § 502 Abs 1 ZPO ab (OGH 6 Ob 131/18k).

Art 23 DSGVO (Beschränkungen): Neu sind Literaturverzeichnis und die Übersicht zum Kommentar sowie die Kommentierung dieses Artikels selbst. Zum Beispiel: Laut EDSA sind die Beschränkungen restriktiv zu interpretieren und es darf der Datenschutz nicht völlig ausgehebelt werden; oder zum Anwendungsbereich, dh, welche Rechte durch Rechtsvorschriften eingeschränkt werden können, zu den zulässigen Zielen, dabei Schutz der Unabhängigkeit der Justiz und den Schutz von Gerichtsverfahren. Zum Ende 118 zum Großteil neue Fußnoten. Interessant die FN 70 mit Entscheidungen des OGH zur Akteneinsicht gem § 219 Abs 2 ZPO.

Mag. *René Bogendorfer* hat zu den Art 28 bis 31 ein umfangreiches Werk mit 89 Seiten verfasst, welches eine ganze Druckseite für eine entsprechende Würdigung verlangen würde.

Art 28 DSGVO (Auftragsverarbeiter): Aus dem Inhalt der 54 zum Großteil neu überarbeiteten Seiten und den 233 Fußnoten ist va auf die Haftung des Auftragsverarbeiters für Verwaltungsstrafen, Geldbußen in nicht unbeträchtlicher Höhe und auf zivilrechtliche Schadenersatzansprüche nach Art 82 DSGVO und § 29 DSG hinzuweisen.

Art 29 DSGVO (Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters): Normadressaten dieser Bestimmung sind Auftragsverarbeiter und diesem oder dem Verantwortlichen unterstellte Personen, die Zugang zu personenbezogenen Daten haben. Durch die Weisungsgebundenheit soll der Verantwortliche stets „Herr der Datenverarbeitung" bleiben und deren Steuerung in Händen behalten, weil er nach Art 5 Abs 2 und Art 24 für zulässige und sichere Datenverarbeitungen verantwortlich ist.

Art 30 DSGVO (Verzeichnis von Verarbeitungstätigkeiten): In diesem Beitrag finden sich Ausführungen zum Zweck der Bestimmung, zu Sanktionen und va zu den Pflichten des Verantwortlichen und des Auftragsverarbeiters. Ferner zu Formvorschriften, zur Zurverfügungsstellung gegenüber der Aufsichtsbehörde, an den Datenschutzbeauftragten sowie an Dritte und schließlich zu den Ausnahmen gem Abs 6.

Art 31 DSGVO (Zusammenarbeit mit der Aufsichtsbehörde): Der Verantwortliche und der Auftragsverarbeiter sowie gegebenenfalls deren Vertreter haben nur auf Anfrage der Aufsichtsbehörde mit ihr zusammenzuarbeiten. Sie müssen daher nicht von sich aus tätig werden, es sei denn, die VO sieht dies vor. Dies ist zB der Fall nach Art 33 (Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde) oder Art 36 (vorherige Konsultation im Zuge einer Datenschutz-Folgenabschätzung).

Mag. *Andreas Rohner* hat die Bearbeitung des Beitrags zu Art 85–87 von RA Dr. *Johannes Öhlböck,* LL.M., aus 2018 übernommen und auf den Stand 1. 12. 2022 gebracht.

Art 85 DSGVO (Verarbeitung und Freiheit der Meinungsäußerung und Informationsfreiheit): Der Autor meint, der verkürzte Ausdruck Medienprivileg sollte richtig Medien-, Wissenschafts-, Kunst- und Literaturprivileg heißen. Neben aktueller Lit bringt *Rohner* ein neues Inhaltsverzeichnis, darin enthalten der Normzweck, Regelungsauftrag nach Abs 1, Abweichungen und Ausnahmen gem Abs 2 sowie Notifizierung laut Abs 3 sowie die österr Umsetzung (§ 9 DSG) bis hin zum Rechtsschutz. Erwartet wird dazu die E des VfGH über den Antrag des BVwG, § 9 Abs 1 DSG als verfassungswidrig aufzuheben (Stattgebung nach Redaktionsschluss). Mit 128 teils neuen Fußnoten schließt der ausgezeichnete Beitrag.

Art 86 DSGVO (Verarbeitung und Zugang der Öffentlichkeit zu amtlichen Dokumenten): Neu sind insb die Themen InformationsfreiheitsG sowie das Verhältnis zur PSI-RL und die Vorgaben für die Offenlegung.

Art 87 DSGVO (Verarbeitung der nationalen Kennziffer): Der Autor geht auf Themen wie Big Data, Definition der Begriffe nationale Kennziffer oder andere Kennzeichen von allgemeiner Bedeutung ein und meint, die Risken, welche bei der Verarbeitung dieser Kennziffern oder Kennzeichen typischerweise bestehen, liegen in potenziellen Missbrauchsszenarien, die mit der erhöhten Identifizierbarkeit der betroffenen Personen sowie den mit dem Kennzeichen zusammenhängenden Zusatzinformationen einhergehen. Eine besondere Gefahr ergibt sich daher in der Erstellung umfassender Persönlichkeitsprofile iSv Profiling.

Dem Herausgeber mit seinem Redaktionsteam und den Autorinnen und Autoren sowie den Mitarbeitern des Verlags MANZ darf Dank für die Mühe und den Aufwand gesagt werden.

Ernst M. Weiss

ZUM HINGEHEN

SEMINARE

- **20. 4. 2023: Datenschutzgrundverordnung im Marketing – ein Praxisseminar**

Business Circle. Vortrag: RA Dr. Rainer Knyrim (Knyrim Trieb Rechtsanwälte)
https://businesscircle.at/recht-steuern/seminar/datenschutzgrundverordnung-im-marketing-ein-praxisseminar/

- **24. 4. 2023: Intensivtagung HinweisgeberInnenschutzGesetz**

Rechtsakademie. Tagungsleitung: RA Dr. Stefan Zischka (Jank Weiler Operenyi Rechtsanwälte | Deloitte Legal), RA Mag. Sascha Jung, LL.M., LL.M. (Jank Weiler Operenyi Rechtsanwälte | Deloitte Legal)
www.manz.at/rechtsakademie

- **26. 4. 2023: Intensivtagung Neues Europäisches Daten(schutz)recht**

Rechtsakademie. Vortrag: RA Dr. Gerald Trieb, LL.M. (Knyrim Trieb Rechtsanwälte)
www.manz.at/rechtsakademie

- **27. 4. 2023: EU Datenschutzreform & neues Datenschutzgesetz**

Business Circle. Fachliche Leitung: RA Dr. Rainer Knyrim (Knyrim Trieb Rechtsanwälte). Vortrag: RA Dr. Gerald Trieb, LL.M. (Knyrim Trieb Rechtsanwälte)
https://businesscircle.at/recht-steuern/seminar/eu-datenschutz-reform-neues-datenschutz-gesetz/

- **11. 5. 2023: HR-Daten, Erlaubtes & Verbotenes**

Business Circle. Fachliche Leitung und Vortrag: RA Dr. Rainer Knyrim (Knyrim Trieb Rechtsanwälte). Vortrag: RA Dr. Barbara Bartlmä, LL.M. (Bartlmä Madl Rechtsanwälte)
https://businesscircle.at/datenschutz/seminar/hr-daten-erlaubtes-verbotenes/

- **11. 5. 2023: MANZ Compliance Day**

Rechtsakademie. Tagungsleitung: RA Dr. Felix Ruhmannseder (wkk law Rechtsanwälte)
www.manz.at/rechtsakademie

- **16. 5. 2023: Mit Bildern und Videos datenschutzkonform kommunizieren – Eine praxisorientierte Einführung**

Research Institute & Fairpicture Präsentation Whitepaper.
https://researchinstitute.at/fairpicture

- **25. 5. 2023: 5 Jahre DSGVO in Europa – Datenschutz-Vorbild oder Digitalisierungsbremse?**

Die Bundes- und Landessparte Information & Consulting sowie die Fachgruppe UBIT NÖ laden in Kooperation mit den Privacy Officers ins WiewerK Donaugasse 1, 3380 Pöchlarn (hybrid, wird aufgezeichnet). Keynote Prof. Dr. Martin Selmayr (Leiter der Vertretung der EK in Österreich) und anschließende Paneldiskussion mit Mag. Mathias Past (FG Ubit NÖ, Moderation), Dr. Andreas Zavadil (DSB), Dr. Thomas Schweiger LL.M., CIPP/E, (SMP Schweiger Mohr & Partner Rechtsanwälte OG), Dr. Heidi Scheichenbauer (Research Institute – Digital Human Rights Center) und Mag. Ursula Illibauer (BSIC WKÖ)
wko.at/ic

- **24.–25. 5. 2023: HEROES OF DATA PRIVACY 2023**

Referenten siehe Webseite.
www.heroesofdataprivacy.com/

- **25. 5. 2023: Datenschutz für Fortgeschrittene**

Business Circle. Vortrag: RA Dr. Rainer Knyrim (Knyrim Trieb Rechtsanwälte)
https://businesscircle.at/datenschutz/datenschutz-fuer-fortgeschrittene-und-re-zertifizierung-als-datenschutzbeauftragter/

- **31. 5. 2023: EU-US Data Privacy Framework – aktueller Stand und Ausblick, sowie Vorstellung des network.fair.data**

network.fair.data. Open House für Interessent*innen und Quartalstreffen für Mitglieder. Vortragende: Ing. Dr. Christof Tschohl, Dr. Heidi Scheichenbauer (beide Research Institute)
https://researchinstitute.at/network-fair-data/

- **14. 6. 2023: Jahrestagung Datenschutz (Wien)**

Rechtsakademie. Vortrag: RA Dr. Gerald Trieb, LL.M. (Knyrim Trieb Rechtsanwälte)
www.manz.at/rechtsakademie

- **21. 6. 2023: Datenschutzrecht in der Gemeindearbeit**

UNI for LIFE/Universität Graz. Vortrag: Dr. Gerald Trieb, LL.M. (Knyrim Trieb Rechtsanwälte)
www.uniforlife.at/de/weiterbildung/recht/seminare/datenschutzrecht-in-der-gemeindearbeit/

- **22. 6. 2023: Intensivtagung Arbeitnehmerdatenschutz und Mitarbeiterkontrolle**

Rechtsakademie. Tagungsleitung: Dr. Thomas Dullinger (Universität Wien) und RA Dr. Jens Winter (CMS Reich-Rohrwig Hainz Rechtsanwälte)
www.manz.at/rechtsakademie

LEHRGANG

- **19.–21. 6. 2023: Lehrgang zum zertifizierten Datenschutzbeauftragten**

Business Circle. Fachliche Leitung und Vortrag: RA Dr. Rainer Knyrim (Knyrim Trieb Rechtsanwälte)
https://businesscircle.at/recht-steuern/lehrgang/lehrgang-zum-zertifizierten-datenschutz-beauftragten/

KONFERENZEN

- **4.–5. 5. 2023: Jahrestagung der Datenschutzbeauftragten**

Österreichischer Städtebund. Vortrag: RA Dr. Gerald Trieb, LL.M. (Knyrim Trieb Rechtsanwälte)
www.staedtebund.gv.at/ausschuesse/datenschutzbeauftragte/tagungen/

Impressum gem. § 24 MedienG

Offenlegung gem. § 25 MedienG und Angaben zu § 5 ECG abrufbar unter https://www.manz.at/impressum

Medieninhaber und Herausgeber: MANZ'sche Verlags- und Universitätsbuchhandlung GmbH. **Anschrift:** Kohlmarkt 16, 1010 Wien. **Verlagsadresse:** Johannesgasse 23, 1010 Wien (verlag@manz.at). **Redaktion:** Dr. Rainer Knyrim (Chefredakteur); Mag. Viktoria Haidinger, LL.M.; DI. Michael Löffler; Prof. KommR Hans-Jürgen Pollirer, Ing. Dr. Christof Tschohl. **E-Mail:** dako@manz.at **Verlagsredaktion:** Dr. Elisabeth Maier, Johannesgasse 23, 1010 Wien, E-Mail: elisabeth.maier@manz.at **Hersteller:** Printera Grupa d.o.o., 10431 Sveta Nedelja. **Herstellungsort:** Sveta Nedelja, Kroatien. **Verlagsort:** Wien, Österreich. **Zitiervorschlag:** Dako 2023/Nummer. **Anzeigenkontakt:** Stefan Dallinger, Tel: (01) 531 61-114, Fax: (01) 531 61-596, E-Mail: stefan.dallinger@manz.at **Bezugsbedingungen:** Die Dako erscheint 5 × jährlich. Der Bezugspreis 2023(10. Jahrgang) beträgt € 179,– (inkl Versand in Österreich). Einzelheft € 43,00. Auslandspreise auf Anfrage. Nicht rechtzeitig vor ihrem Ablauf abbestellte Abonnements gelten für ein weiteres Jahr als erneuert. Abbestellungen müssen schriftlich bis spätestens 18. November des laufenden Abojahres beim Verlag einlangen. **Formatvorlagen:** Zum Download unter www.manz.at/formatvorlagen **Hinweis:** Auf eine geschlechtergerechte Sprache wird geachtet. Wird jedoch von einzelnen Autoren zugunsten der leichteren Lesbarkeit bloß die männliche oder die weibliche Form verwendet, sind immer beide Geschlechter gleichermaßen gemeint. **AZR:** Alle Abkürzungen entsprechen den „Abkürzungs- und Zitierregeln" (AZR), 8. Aufl (Verlag Manz, 2019).

Grafisches Konzept: Michael Fürnsinn für buero8, 1070 Wien (buero8.com).

MIX Paper from responsible sources FSC® C130095 www.fsc.org

GESETZGEBUNG

STATUS QUO ANGEMESSENHEITSBESCHLUSS EU-US DATA PRIVACY FRAMEWORK

In der Dako 1/2023 haben wir berichtet, dass die EK den Entwurf eines Angemessenheitsbeschlusses für das EU-US Data Privacy Framework vorgelegt hat.

Gem Art 45 Abs 3 iVm Art 93 Abs 2 DSGVO gelangt Art 5 VO 182/2011 zur Anwendung, dh, Angemessenheitsbeschlüsse der EK sind im „Prüfverfahren" des Komitologieverfahrens durchzuführen. Der hierfür zuständige Ausschuss ist jener für den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Code C49000), vgl Art 93 Abs 1 DSGVO. Wie dem öffentlich einsehbaren Register zum Ausschussverfahren (https://ec.europa.eu/transparency/comitology-register/screen/home) zu entnehmen ist, fand auf der Sitzung am 3. 2. 2023 ein erster Gedankenaustausch zum Entwurf der EK statt.

Der LIBE-Ausschuss des EP hat am 14. 2. 2023 einen Entwurf für eine ablehnende Entschließung gem Art 132 Abs 2 GO EP vorgelegt (www.europarl.europa.eu/doceo/document/LIBE-RD-740749_EN.pdf, Verfahrensnummer 2023/2501[RSP]). Der EDSA hat am 28. 2. 2023 eine grundsätzlich positive Stellungnahme zum Angemessenheitsbeschluss abgegeben (https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_en). Am nächsten Tag fand in einer LIBE-Sitzung eine Aussprache statt, in der sich Dr. *Andrea Jelinek* (Vorsitzende des EDSA) und *Bruno Gencarelli* (Leiter des Referats für Internationale Angelegenheiten und Datenströme der GD JUST) den kritischen Fragen und Äußerungen mancher MEPs stellen mussten (https://multimedia.europarl.europa.eu/en/webstreaming/libe-committee-meeting_20230301-1045-COMMITTEE-LIBE). In der Sitzung wurden Änderungsanträge zum Entwurf der Entschließung angekündigt (Frist: 9. 3. 2023). Die Abstimmung im Plenum wurde für 17. 4. 2023 angesetzt. Rein rechtlich ist das Kontrollrecht des EP gem Art 11 VO 182/2011 auf die Prüfung der Einhaltung der Durchführungsbefugnisse der EK beschränkt. Eine entsprechende Resolution des EP würde allerdings auch nur eine Überprüfungspflicht der vorgetragenen Bedenken durch die EK auslösen. Eine in Bezug auf den Inhalt ablehnende Entschließung des EP hätte daher rechtlich keine Konsequenzen, allerdings natürlich ein bedeutendes politisches Gewicht. Außerdem ist das EP zur Erhebung einer Nichtigkeitsklage befugt (Art 263 iVm Art 256 AEUV).

VERWALTUNG

EDSA: ARBEITSPROGRAMM 2023/24

Am 14. 2. 2023 hat der EDSA sein Arbeitsprogramm für das Biennium 2023/24 beschlossen; 4 Säulen werden definiert:

- Säule I – Harmonisierung vorantreiben und Compliance erleichtern, ua mit Leitlinien zu folgenden Themen:
  - Finalisierung/Aktualisierung nach öffentlicher Konsultation: Auskunftsrecht; Bestimmung der federführenden Aufsichtsbehörde eines für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters; Meldung von Datenschutzverletzungen.
  - Neu: Verwendung von Technologien zur Erkennung und Meldung von sexuellem Online-Missbrauch von Kindern; berechtigtes Interesse; Daten von Kindern; Verarbeitung von Daten für medizinische und wissenschaftliche Forschungszwecke; Nutzung von Social Media durch öffentliche Stellen.
- Säule II – Unterstützung der wirksamen Durchsetzung und effizienten Zusammenarbeit der nationalen Aufsichtsbehörden, ua mit Leitlinien zu folgenden Themen:
  - Finalisierung/Aktualisierung nach öffentlicher Konsultation: Bußgeld.
  - Neu: Art 61 DSGVO – Gegenseitige Unterstützung; Art 66 DSGVO – Dringlichkeitsverfahren; Formular für Beschwerden betroffener Personen; Anspruch auf rechtliches Gehör und Akteneinsicht bei Verfahren der Zusammenarbeit nach Art 60 DSGVO.
- Säule III – ein Grundrechtsansatz für neue Technologien, ua mit Leitlinien zu folgenden Themen:
  - Finalisierung/Aktualisierung nach öffentlicher Konsultation: Einsatz von Gesichtserkennung durch Strafverfolgungsbehörden.
  - Neu: Anonymisierung; Pseudonymisierung; Blockchain; Telemetrie- und Diagnosedaten; Zusammenspiel von KI-Gesetz und DSGVO.
- Säule IV – Die globale Dimension, mit Leitlinien zu folgenden Themen:
  - Finalisierung/Aktualisierung nach öffentlicher Konsultation: Genehmigung von Binding Corporate Rules für Verantwortliche.
  - Neu: Stellungnahmen zu und Überprüfung von Angemessenheitsbeschlüssen (USA, Japan etc); Genehmigung Binding Corporate Rules für Auftragsverarbeiter; Art 48 DSGVO – Verbindlichkeit ausländischer behördlicher Entscheidungen; Art 37 DSRL-PJ – Datenübermittlung vorbehaltlich geeigneter Garantien.

RECHTSPRECHUNG

KEINE EINSICHT EINES RECHTSPRAKTIKANTEN IN SEINEN PERSONALAKT

Gilt es in privatrechtlichen Arbeitsverhältnissen für selbstverständlich, dass ein AN Einsicht in seinen Personalakt erhält, so ist dies bei öffentlich-rechtlichen Ausbildungsverhältnissen nicht der Fall. So ist in der BVwG-E 16. 9. 2022, W195 2256300-1 nachzulesen, dass § 17 AVG das Recht zur Akteneinsicht nur den Parteien einräumt, die an einem bestimmten Verwaltungsverfahren beteiligt sind; ohne ein solches Verfahren kann daher niemandem ein solches Recht zustehen (mwN). Das (verfahrensrechtliche) Recht auf Akteneinsicht gem § 17 Abs 1 AVG setzt den Bezug zu einem bestimmten, wenn auch allenfalls schon abgeschlossenen Verfahren voraus (mwN). Vor diesem Hintergrund ist die von der beschwerdeführenden ex-Rechtspraktikantin sowohl im verfahrenseinleitenden Antrag auf Gewährung von Akteneinsicht als auch in der Beschwerde vertretene Rechtsansicht unzutreffend, ihr stünde gem § 17 AVG losgelöst vom Vorhandensein eines konkreten Verfahrens eine generelle Einsicht in den anlässlich ihrer Gerichtspraxis gebildeten Personalakt zu. Mangels Vorliegen eines öffentlich-rechtlichen Dienstverhältnisses scheidet die Anwendbarkeit des DienstrechtsverfahrensG im gegenständlichen Fall aus, ebenso wie des PersonalvertretungsG, da – so das BVwG – Richter:innen und Richteramtsanwärter:innen ausgenommen sind.

Auf die Idee, einen datenschutzrechtlichen Auskunftsantrag zu stellen, kam die Bf zu spät, nämlich erst im Rahmen der Beschwerde an das BVwG, womit sie die Sache des Verfahrens überschritt, und die entsprechenden Anträge zurückzuweisen waren.

Viktoria Haidinger, Wirtschaftskammer Österreich