# 27. Bericht der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen

## Bettina Gayk

## zum Datenschutz

**für die Zeit vom 1. Januar 2021**

**bis zum 31. Dezember 2021**

Herausgeberin:

Bettina Gayk

Landesbeauftragte für Datenschutz und Informationsfreiheit

Nordrhein-Westfalen

Kavalleriestraße 2–4

40213 Düsseldorf

Tel.: 0211 / 384 24 - 0

Fax: 0211 / 384 24 - 999

E-Mail: poststelle@ldi.nrw.de

Diese Broschüre kann unter www.ldi.nrw.de abgerufen werden.

Zitiervorschlag: 27. Bericht LDI NRW

ISSN: 0179–2431

Düsseldorf 2022

Titelbild © Bildagentur PantherMedia / kentoh (YAYMicro)

Gedruckt auf chlorfreiem Recyclingpapier

# Inhaltsverzeichnis

# Vorwort

Nun lege ich den ersten Bericht vor, der zumindest teilweise in meine Amtszeit fällt. Am 19. Mai 2021 hat mich der Landtag zur neuen Landesbeauftragten gewählt. Für die breite Unterstützung, die ich dabei erhalten habe, bin ich sehr dankbar. Das mir entgegengebrachte Vertrauen stärkt meine unabhängige Aufgabenwahrnehmung und ist mir zugleich eine Verpflichtung, mein Amt mit Sorgfalt zu führen.

Auch das Jahr 2021 war noch sehr von der Pandemie geprägt. Das zeigen einige Beiträge dieses Berichts. Datenverluste in Testzentren, Rückzahlung von Corona-Hilfen oder Dokumentationspflichten im Zusammenhang mit Impfnachweisen sind Themen, die uns beschäftigt haben. Da die Gesetzgebung zum Infektionsschutz oft und kurzfristig an die jeweilige Lage angepasst wurde, gab es ebenso kurzfristig häufig neue Datenschutzfragen, die wir klären mussten. Wir haben nicht auf Beschwerden gewartet, sondern die Bürger*innen und auch Unternehmen laufend und zeitnah über unsere Homepage informiert, wie Sachverhalte datenschutzkonform gelöst werden können.

Die Homepage ist ein wichtiges Stichwort: Bei meinem Amtsantritt hatte ich angekündigt, dass ich im Bereich der Öffentlichkeitsarbeit Verbesserungen erzielen möchte. Das ist arbeitsintensiv und für eine kleine Behörde eine besondere Mühe. Deshalb freue ich mich besonders, dass wir nun eine neue und modernere Homepage www.ldi.nrw.de starten konnten. Meinen Mitarbeiter*innen, die daran gearbeitet haben, die Seite zu gestalten und mit Inhalten zu füllen, danke ich sehr für ihr Engagement beim Relaunch.

Die Übermittlung personenbezogener Daten in Drittstaaten und vor allem in die USA möchte ich an dieser Stelle als ein weiterhin virulentes Datenschutzproblem ansprechen. Der Bericht geht nur an einigen wenigen Stellen darauf ein und repräsentiert insofern nicht die Bedeutung, die dieses Thema in der Beschwerdebearbeitung einnimmt. Datentransfers in die USA finden etwa bei der Nutzung vieler Softwareprodukte amerikanischer Unternehmen laufend statt. Die Unternehmen wollen Daten über die Anwender*innen der Programme für die Programmweiterentwicklung nutzen. Diese und andere Datenübermittlungen sind aber vielfach nur zulässig, sofern sie durch besondere Garantien abgesichert sind, die einen unverhältnismäßigen Zugriff von Sicherheitsbehörden auf die übermittelten personenbezogenen Daten ausschließen. Das ist seit dem „Schrems II“-Urteil des Europäischen Gerichtshofs rechtlich geklärt. In der Praxis ist diese rechtliche Anforderung schwer einzuhalten, denn die Daten übermittelnden und empfangenden Stellen haben außer einer sicheren Verschlüsselung kaum Instrumente, um den Datenzugriff von Sicherheitsbehörden einzuschränken. Beschwerden, die mein Haus erreichen, richten sich oft gegen die Nutzung von Softwareprodukten US-amerikanischer Hersteller. Verbote der Nutzung vieler solcher Produkte würden Arbeitsprozesse in Unternehmen und Verwaltungen lahmlegen und können deshalb nur das letzte Mittel sein. Zumindest sollten Unternehmen und Verwaltungen aber datenschutzfreundliche Einstellungen der vorhandenen Produkte nutzen und vermeidbare Softwareprodukte mit rechtlichen Mängeln nicht neu einführen. Bisher habe ich in einem Fall eine zweifellos vermeidbare unzulässige Datenübermittlung in einen Drittstaat mit einem Bußgeld geahndet. Die Europäische Kommission

hat im März 2022 eine neue Angemessenheitsentscheidung für die USA angekündigt, die dieses Dilemma auflösen soll.

Ein wichtiges Ereignis zum Ende des Berichtsjahres 2021 war das Inkrafttreten des neuen Telekommunikation-Telemedien-Datenschutz-Gesetzes (TTDSG) am 1. Dezember. Es fasst die Datenschutzbestimmungen aus dem Telemedien- und dem Telekommunikationsgesetz zusammen und setzt die ePrivacy-Richtlinie in diesem Bereich um. Die Landesregierung hat erfreulicherweise eine Anpassung der Zuständigkeitszuweisung für die Datenschutzkontrolle nach dem TTDSG zügig in den Landtag eingebracht. Sie wurde noch vor Ablauf der Legislaturperiode beschlossen. Somit ist die Datenschutzkontrolle in diesem Bereich sichergestellt. Derzeit führen wir gemeinsam mit anderen Ländern eine koordinierte Medienprüfung durch. Nicht transparenter Cookie-Einsatz und irritierende Einwilligungsvoreinstellungen sind im Internet leider noch sehr verbreitet, aber nicht datenschutzgerecht. Eine Orientierungshilfe der Datenschutzkonferenz informiert, was Anbieter*innen von Telemedien nach dem neuen TTDSG hierzu beachten müssen, und ist Grundlage unserer Prüfungen.

Abschließen möchte ich mit einem Hinweis auf das nach wie vor hohe Niveau der Beschwerden, die meine Behörde seit Inkrafttreten der Datenschutz-Grundverordnung jährlich erreichen. Die Beschwerdezahl hat sich im Vergleich zu der Zeit davor verdreifacht. Die Stärkung der Betroffenenrechte ist eine hohe Errungenschaft der Datenschutz-Grundverordnung. Die Bürger*innen haben einen Anspruch, dem meine Behörde gerecht werden muss. Leider ist das angesichts des Beschwerdeaufkommens kaum mehr

zu leisten und wichtige grundsätzliche Aufgaben wie Beratung, Kontrollen und Information kommen viel zu kurz. Trotz dieser Belastung und auch der pandemiebedingten Arbeit im Homeoffice mit den damit verbundenen organisatorischen Hürden, hat meine Behörde viel geleistet. Die für den Bericht ausgewählten Themen und Fälle geben einen Einblick in diese Arbeit.

Bettina Gayk

Frühjahr 2022

# Abkürzungsverzeichnis

| | |
|---|---|
| **Abs.** | Absatz |
| **Art.** | Artikel |
| **BDSG** | Bundesdatenschutzgesetz |
| **BfDI** | Bundesbeauftragter für den Datenschutz und die Informationsfreiheit |
| **DSK** | Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz) |
| **DSG NRW** | Datenschutzgesetz Nordrhein-Westfalen |
| **DS-GVO** | Datenschutz-Grundverordnung |
| **EDSA** | Europäischer Datenschutzausschuss (englisch European Data Protection Board: EDPB) |
| **TTDSG** | Telekommunikation-Telemedien-Datenschutz-Gesetz |
| **TKG** | Telekommunikationsgesetz |

# 1. Überblick

- **Eingaben**

  Im Jahr 2021 haben uns insgesamt rund **11.900 schriftliche Eingaben** erreicht, einschließlich Meldungen nach Art. 33 DS-GVO (sog. Datenpannen). Etwa 450 Eingaben betrafen das Thema Informationsfreiheit. Dazu werden wir im nächsten Jahr berichten.

  Weitere Einzelheiten zu den **Eingaben** und **Beschwerden** sowie **Meldungen von Datenschutzverletzungen, Abhilfemaßnahmen, Europäischen Verfahren** und **Rechtsetzungsvorhaben** finden sich unter 2. im Kapitel „Zahlen und Fakten“.

- **Anlasslose Prüfungen**

  Im Jahr 2021 haben wir zwei Kontrollen bzw. Prüfungen durchgeführt:

  - Kontrolle von Verfahrensrückmeldungen der Staatsanwaltschaften an die Polizeibehörden. Siehe hierzu unter 6.5.

  - Datenschutzprüfung von Energieversorgungsunternehmen. Siehe hierzu unter 10.1.

- **Informationen und Öffentlichkeitsarbeit**

  Unser allgemeines und laufend aktualisiertes Informationsangebot finden Sie auf unserer Internetseite www.ldi.nrw.de. Zwischenzeitlich haben wir den Internetauftritt vollständig überarbeitet und modernisiert.

  Alle Veröffentlichungen der Datenschutzkonferenz sind auf der gemeinsamen Internetseite www.datenschutzkonferenz-online.de abrufbar.

Wir beteiligen uns am **Virtuellen Datenschutzbüro** www.datenschutz.de, das Bürger*innen als erste zentrale Informations- und Anlaufstelle dient. Insbesondere um Jugendliche zu erreichen, beteiligen wir uns zudem an der Webseite **www.youngdata.de**.

- **Vorträge und Erfahrungsaustausche**
  - Jährlicher Erfahrungsaustausch zwischen den Hochschuldatenschutzbeauftragten NRW und der LDI NRW
  - Kommunaler Datenschutzkongress der Kommunalagentur
  - Jährlicher Erfahrungsaustausch zwischen JM NRW und LDI NRW
  - Fachkongress „Digitalisierung (in) der Juristenausbildung“. Teilnahme am Workshop „Digitale Prüfung: Voraussetzungen und Möglichkeiten der Durchführung universitärer und staatlicher juristischer Prüfungen in digitaler Form“
  - Treffen mit dem Bankenverband auf europäischer Ebene (European Banking Federation)
  - Fachtagung Datenschutz der Sparkassenakademie Nordrhein-Westfalen „Datenschutzaufsicht – Aktuelle Themen und Best Practices“
  - Erfahrungsaustausch mit Versicherungsunternehmen
  - Erfahrungsaustausch mit Unternehmen der Kreditwirtschaft

- Austausch zu Datenschutz und Finanzdienstleistungen mit der Verbraucherzentrale Bundesverband e.V
- Vortrag vor dem Verkehrsverbunds Rhein-Ruhr (VRR) zum Thema „Datenschutzrechtliche Rahmenbedingungen bei der Nutzung von Videotechnik im ÖPNV/SPNV – Praktische Tipps zur Umsetzung“
- Austausch mit regionalen Erfahrungsaustauschkreise der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD)
- Austausch mit dem Arbeitskreis der kommunalen Datenschutzbeauftragten in NRW

- **Datenschutzkonferenz und Expertengruppen des Europäischen Datenschutzausschusses**

  Die Beauftragten des Bundes und der Länder besprechen wichtige Datenschutzfragen in der **Datenschutzkonferenz** und streben einheitliche Bewertungen an, die in **Arbeitskreisen** vorbereitet werden. Im Rahmen der Datenschutzkonferenz leitet die LDI NRW die Arbeitskreise

  - Wirtschaft (vormals Düsseldorfer Kreis),
  - Statistik,
  - Kreditwirtschaft und
  - Auskunfteien (gemeinsam mit Hessen).

  Der **Europäische Datenschutzausschuss** hat zu seiner Unterstützung mehrere Ausschüsse – sog. **Ex-**

**pert Subgroups** – gebildet, in denen auch die nationalen Aufsichtsbehörden vertreten sind. Die LDI NRW ist in der

- Key Provisions Expert Subgroup und in der
- Financial Matters Expert Subgroup

des Europäischen Datenschutzausschusses aktiv.

## 2. Zahlen und Fakten

- **Eingabesituation im Überblick**

  Im Jahr **2021** haben uns insgesamt rund **11.900** schriftliche Eingaben erreicht, einschließlich Meldungen nach Art. 33 DS-GVO – sog. Datenpannen. Grundsätzlich nicht erfasst haben wir dabei die zahlreichen telefonischen Anfragen.

  Die Zahl der jährlichen Eingaben liegt damit seit dem Jahr der Geltung der DS-GVO bei etwa 12.000 Eingaben. Im Jahr 2020 waren es etwa 12.150, 2019 waren es insgesamt etwa 12.500 und im Jahr 2018 etwa 12.000.

  Von den Eingaben waren

  - **6.849 Beschwerden** nach Art. 77 DS-GVO,
  - **520** von **Dritten gemeldete Beschwerden**,
  - **1.412 schriftliche Beratungsanfragen**,
  - **33 Begleitungen bei Rechtsetzungsvorhaben,**
  - **9 Genehmigungsverfahren** und
  - **1.841 Meldungen nach Art. 33 DS-GVO** zu sog. Datenpannen,
  - **277 Eingaben ohne Kategorie.**

- **Beschwerden und Beratungsanfragen**

  Im Jahr 2021 haben uns **6.849 Beschwerden** erreicht.

  Eine Beschwerde liegt nach Art. 77 DS-GVO vor, wenn eine Person vorträgt, dass ein sie persönlich verletzender Verstoß gegen datenschutzrechtliche Bestimmungen vorliegt. Eingaben, die auf mutmaßliche Datenschutzverstöße hinweisen, von denen die Einsendenden jedoch nicht selbst betroffen sind, können wir von Amts wegen aufgreifen. Solche **Eingaben von Dritten** haben wir **520** erhalten.

  Schriftliche **Beratungsanfragen** haben wir **1.412** erhalten, sowohl von Verantwortlichen als auch von Auftragsverarbeitern und betroffenen Personen.

- **Meldungen von Datenschutzverletzungen**

  **Meldungen nach Art. 33 DS-GVO** zu sog. Datenpannen haben uns **1.841** erreicht. Im Jahr 2020 waren es 1.775 Meldungen, 2019 waren es 2.235 Meldungen.

  Eine Verletzung des Schutzes personenbezogener Daten, die zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, muss der Verantwortliche unverzüglich und möglichst binnen 72 Stunden der zuständigen Aufsichtsbehörde melden (Art. 33 DS-GVO).

- **Abhilfemaßnahmen**

  Um eine einheitliche Überwachung und Durchsetzung der DS-GVO sicherzustellen, werden den Aufsichtsbehörden in Art. 58 Abs. 2 DS-GVO einheitliche Abhilfebefugnisse eingeräumt.

  Als Maßnahme nach **Art. 58 Abs. 2 Buchstabe i** wurden bei der Zentralen Bußgeldstelle der LDI NRW

**115 neue Verfahren registriert**. **57 Bußgeldbescheide** wurden erlassen und **83 Verfahren** durch Rechtskraft, Einstellung oder Gerichtsentscheidungen **abgeschlossen**.

Von den weiteren in Art. 58. Abs. 2 DS-GVO genannten Abhilfemaßnahmen hat die LDI NRW die folgenden weiteren **680** Maßnahmen ergriffen:

- **551 Hinweise** nach Art. 58 Abs. 1 d),
- **17 Warnungen** nach Art. 58 Abs. 2 a),
- **41 Verwarnungen** nach Art. 58 Abs. 2 b),
- **68 Anweisungen** nach Art. 58 Abs. 2 d),
- **1 Anweisung** nach Art. 58 Abs. 2 e),
- **1 Beschränkung** nach Art. 58 Abs. 2 f),
- **1 Anordnung** nach Art. 58 Abs. 2 g).

Davon erfasst sind Verfahren, die bereits in den Vorjahren eingeleitet wurden, während viele im Jahr 2021 begonnene Verfahren noch nicht beendet und nicht erfasst sind. Oft sind die Verfahren sowohl in zeitlicher als auch in rechtlicher Hinsicht aufwändig. Nicht selten bedarf es vieler Kontakte und eines umfangreichen Schriftwechsels bis es am Ende zu einer Abhilfemaßnahme etwa in Form eines Bußgeldbescheides kommt. Zudem setzt die LDI NRW im Kontakt mit den Verantwortlichen nach wie vor den Schwerpunkt auf Beratung und Sensibilisierung. Häufig werden so ohne eine Abhilfemaßnahme einvernehmliche, konstruktive Lösungen gefunden, die nicht nur den Einzelfall datenschutzgerecht lösen, sondern auch für die zukünftige Praxis der Verantwortlichen und Auftragsverarbeiter einen Gewinn für den Datenschutz bedeuten.

- **Europäische Verfahren**

  Die DS-GVO sieht Verfahren für eine europäische Meinungsbildung und Entscheidungsfindung der Datenschutzaufsichtsbehörden vor. Das einheitliche europäische Recht soll in den Mitgliedstaaten auch einheitlich angewendet werden. Da die Regelungen der DS-GVO oft allgemein gehalten sind, haben die Aufsichtsbehörden die Aufgabe, das neue Recht in der Interpretation und in der Praxis zu harmonisieren. Dazu müssen sich die Behörden abstimmen und – teils verbindliche – Rechtsauffassungen entwickeln. Die Meinungsbildung der europäischen Aufsichtsbehörden findet in Abstimmungsverfahren der Behörden untereinander und im Europäischen Datenschutzausschuss statt.

  Für viele Abstimmungsprozesse wird das Binnenmarkt-Informationssystem (Internal Market Information System, abgekürzt IMI) als IT-Plattform eingesetzt. Die Plattform IMI unterstützt die Verfahren der Zusammenarbeit und Kohärenz über komplexe Module. Wird ein Modul in IMI gestartet, generiert das System eine automatische Benachrichtigung, die bei der empfangenden Behörde bearbeitet werden muss. Arbeitssprache in IMI ist Englisch.

  Unter anderem tauschen sich die betroffenen Aufsichtsbehörden über grenzüberschreitende Fälle aus und stimmen Entscheidungen ab. Geht beispielsweise bei uns eine Beschwerde in Bezug auf eine grenzüberschreitende Datenverarbeitung ein, leiten wir als Eingangsbehörde die ersten notwendigen Schritte über IMI in die Wege. Geht über IMI eine Meldung über eine grenzüberschreitende Datenverar-

beitung ein, prüfen wir, ob wir europaweit federführend sind oder uns als betroffene Behörde an den weiteren Verfahrensschritten beteiligen.

Im Jahr 2021 war die LDI NRW in **1.558 Fällen** mit gestarteten IMI-Modulen befasst. Im Jahr 2020 waren es ebenfalls 1.558 und im Jahr 2019 waren es 1.390 Fälle.

- **Förmliche Begleitung bei Rechtsetzungsvorhaben**

  Im Jahr 2021 wurde die LDI NRW bei 33 **Rechtsetzungsvorhaben** beteiligt. Im Jahr 2020 waren es 44 Vorhaben.

  Unsere Hinweise wurden vielfach aufgegriffen und umgesetzt. Ein Fokus unseres Tätigwerdens in diesem Bereich lag dabei zum einen weiterhin auf der Aufrechterhaltung des bestehenden Datenschutzniveaus in NRW und zum anderen auf der umfassenden Umsetzung der Anforderungen der DS-GVO und der JI-Richtlinie.

  Inzwischen werden im Rahmen der Digitalisierung der Verwaltung vermehrt Gesetzgebungsvorhaben bei uns vorgelegt, die die Einrichtung automatisierter Abrufverfahren zum Gegenstand haben. Bei diesen Gesetzen und Verordnungen achten wir insbesondere darauf, dass die Verantwortlichkeiten für die technischen und organisatorischen Maßnahmen und die Betroffenenrechte zwischen den beteiligten öffentlichen Stellen eindeutig abgegrenzt sind.

  Die LDI NRW ist immer frühzeitig über Entwürfe für Rechts- und Verwaltungsvorschriften zu unterrichten, wenn diese eine Verarbeitung personenbezogener Daten vorsehen (vgl. § 27 Abs. 5 Satz 2, § 57 Abs. 5 Datenschutzgesetz NRW). Dies soll sicherstellen,

dass wir die vorgesehenen Neuregelungen hinreichend gründlich prüfen und ggf. eingehend beratend tätig werden können. Versäumen es die zuständigen Ministerien, diese frühzeitige Beratung zu nutzen, entsteht nicht selten großer Unmut, wenn die LDI NRW nachträglich auf nicht ausreichenden Datenschutz hinweisen muss und sich das Verfahren dadurch verzögert. Es liegt in der Hand der zuständigen Stellen, dies durch ein rechtzeitiges Beratungsersuchen zu vermeiden.

Wir wurden in unterschiedlicher Intensität und in verschiedenen Phasen der Verfahren von der Landesregierung bei den folgenden Gesetzesvorhaben beteiligt:

- Glücksspielstaatsvertrag 2021 nebst Umsetzungsgesetz
- VO zum Ausführungsgesetz NRW Glücksspielstaatsvertrag 2021
- Änderung der Gemeindeordnung NRW
- Änderung Meldedatenübermittlungsverordnung
- Open Data Verordnung
- Gesetzes zur Novellierung des Gesetzes über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen in Nordrhein-Westfalen (SÜG NRW)
- Gesetz zur Anpassung des Polizeigesetzes des Landes Nordrhein-Westfalen und anderer Gesetze an das Telekommunikation-Telemedien-Datenschutz-Gesetz
- Entwurf einer Rechtsverordnung zum Wohnraumstärkungsgesetz

- Entwurf eines Gesetzes über die Beauftragte oder den Beauftragten für den Opferschutz des Landes Nordrhein-Westfalen
- Entwurf eines Gesetzes zur Änderung des Schiedsamtsgesetzes
- Entwurf eines Gesetzes zur Novellierung der nordrhein-westfälischen Landesjustizvollzugsgesetze
- Entwurf eines Sechsten Gesetzes zur Änderung des Justizgesetzes Nordrhein-Westfalen
- Mögliche Änderung der Vollzugsdatenverarbeitungsverordnung
- Neufassung des Teilhabe- und Integrationsgesetzes
- Novellierung des Flüchtlingsaufnahmegesetzes
- Entwurf eines 16. Schulrechtsänderungsgesetzes und Entwurf einer Verordnung zur Anpassung schulrechtlicher Vorschriften sowie Entwurf einer Verordnung zur Änderung der VO-DV I und II sowie der ZustVOSchAuf
- Entwurf einer Verordnung über die Anforderungen an den Sachkundenachweises und die Schulungen für Spielhallen im Land Nordrhein-Westfalen
- LichtbildabrufVO
- VV zum E-Payment
- Gesetz zur Umsetzung der Akademisierung des Hebammenberufes in NRW
- Entwurf für ein Gesetz über die Zulassung von Online-Casinospielen im Land NRW (Online-Casinospiel Gesetz NRW – OCG NRW); Umsetzung des Glücksspielstaatsvertrages 2021

Gegenüber dem Landtag gab die LDI NRW Stellungnahmen zu den folgenden Vorhaben ab:

- Gesetz über den interkollegialen Ärzteaustausch bei Kindeswohlgefährdung - Änderung des Heilberufsgesetzes (HeilBerG) - (GesEntw Drs 17/14280) - Stellungnahmen Stellungnahme 17/4567 und 17/4663
- Gesetz zur Änderung der Gemeindeordnung für das Land Nord-rhein-Westfalen (GO NRW) (GesEntw Drs 17/13064) - Stellungnahme 17/4022
- Gesetz zur Umsetzung des Glücksspielstaatsvertrages 2021 - Stellungnahme 17/3799
- Staatsvertrag zur Neuregulierung des Glücksspielwesens in Deutschland (Glücksspielstaatsvertrag 2021 – GlüStV 2021) (Antr (Staatsvertrag) Drs 17/11683) - Anhörung des Hauptausschusses am 01.03.2021 Stellungnahme 17/3622

Die LDI NRW nahm zudem an einem Fachgespräch des Ausschusses für Digitalisierung und Innovation zum digitalen Verbraucherschutz bei Datenlecks und Cyberangriffen am 23. September 2021 teil.

Schließlich haben wir die uns vom Bundeswirtschaftsministerium eingeräumte Möglichkeit für eine Stellungnahme zum Entwurf für ein TTDSG genutzt.

## 3. Drittlandübermittlung nach „Schrems II“: Überarbeitete Empfehlungen und neue Standardvertragsklauseln

**Übermittlungen in viele Länder außerhalb des europäischen Wirtschaftsraums sind nur zulässig, wenn dafür bestimmte Instrumente wie Standarddatenschutzklauseln verwendet werden. Nach der „Schrems II“-Rechtsprechung sind zudem unter Umständen ergänzende Maßnahmen erforderlich. Der Europäische Datenschutzausschuss (EDSA) hat seine Empfehlungen zu den ergänzenden Maßnahmen überarbeitet. Neu sind modulare Standardvertragsklauseln der Europäischen Kommission, an die auch laufende Verträge angepasst werden müssen.**

Das „Schrems II“-Urteil (C-311/18 vom 16.07.2020) des Europäischen Gerichtshofs (EuGH) hat klargestellt, dass Datenexporteure, die Garantien gemäß Art. 46 DS-GVO nutzen, zusätzliche Prüfungen anstellen und bei Bedarf ergänzende Maßnahmen treffen müssen. Dies betrifft die häufig verwendeten Standarddatenschutzklauseln (von der EU-Kommission Standardvertragsklauseln genannt), aber auch alle anderen Instrumente des Art. 46 DS-GVO, zum Beispiel verbindliche interne Datenschutzklauseln (BCR).

Als Reaktion auf das „Schrems II“-Urteil hat der Europäische Datenschutzausschuss Empfehlungen erarbeitet. Die Empfehlungen des EDSA 01/2020 zu ergänzenden Maßnahmen für Übertragungsinstrumente zur Gewährleistung des EU-Schutzniveaus für personenbezogene Daten geben Datenexporteuren eine Orientierung zu den erforderlichen Prüfungen und Maßnahmen. Die Empfehlungen wurden nach einer

öffentlichen Konsultation überarbeitet und sind in der Version 2.0 veröffentlicht.

Für Datenübermittlungen in die USA und auch in viele andere Länder werden häufig Standardvertragsklauseln verwendet. Die Europäische Kommission hat im Juni 2021 neue Standardvertragsklauseln für Übermittlungen in Drittländer erlassen (Durchführungsbeschluss (EU) 2021/914 der Europäischen Kommission vom 04.06.2021, ABl. EU Nr. L 199/31 vom 07.06.2021).

In den neuen Standardvertragsklauseln werden allgemeine Klauseln mit einem modularen Ansatz kombiniert. Zusätzlich zu den allgemeinen Klauseln sollen Verantwortliche und Auftragsverarbeiter das für ihre Situation geltende Modul auswählen.

Die Europäische Kommission hat differenzierte Übergangsfristen festgelegt: Alte Standardvertragsklauseln durften für eine Übergangszeit bis zum 26. September 2021 für Neuverträge verwendet werden. Bis spätestens 27. Dezember 2022 müssen alle Verträge, die auf Grundlage der alten Standardvertragsklauseln abgeschlossen wurden, auf die neuen Standardvertragsklauseln umgestellt werden. Diese Übergangsfrist unterliegt der Einschränkung, dass die betroffenen Verarbeitungsvorgänge unverändert bleiben und die Anwendung der alten Klauseln gewährleistet, dass die Übermittlung personenbezogener Daten geeigneten Garantien unterliegt.

Wie bei allen Garantien nach Art. 46 DS-GVO müssen Datenexporteure auch bei den neuen Standardvertragsklauseln zusätzliche Prüfungen anstellen und bei Bedarf zusätzliche Maßnahmen treffen. Dementsprechend ist die Europäische Kommission in ihrem

Beschluss unter anderem auf die „Schrems II“-Entscheidung des EuGHs eingegangen. Die Anforderungen, die sich aus der Rechtsprechung des EuGHs ergeben, sind nun ausdrücklich in den Standardvertragsklauseln geregelt. Die Europäische Kommission und der EDSA haben die neuen Standardvertragsklauseln und die Empfehlungen des EDSA 01/2020 zu ergänzenden Maßnahmen für Übertragungsinstrumente aufeinander abgestimmt.

Datenexporteure müssen die Datenübermittlung im Zusammenhang mit dem Recht des Drittlandes und dem Übertragungsinstrument beurteilen, auf das sie sich stützen. Sie müssen ihre Rechenschaftspflicht gemäß Art. 5 Abs. 2 DS-GVO erfüllen und ihren Entscheidungsprozess gründlich dokumentieren.

Für eine rechtmäßige Übermittlung personenbezogener Daten in ein Drittland sind aktualisierte Praxishilfen vorhanden. Im Ergebnis kann nicht jede Übermittlung personenbezogener Daten in jedes Drittland erfolgen. Falls Standarddatenschutzklauseln verwendet werden, müssen Datenexporteure die Neuerungen in den Verträgen umsetzen.

# 4. Internet und Medien

## 4.1 Neues Telekommunikation-Telemedien-Datenschutz-Gesetz und neues Telekommunikationsgesetz in Kraft

**Am 1. Dezember 2021 ist das neue Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien (Telekommunikation-Telemedien-Datenschutz-Gesetz – TTDSG) in Kraft getreten. Es fasst die Datenschutzbestimmungen aus dem Telemedien- und dem Telekommunikationsgesetz zusammen und setzt die Cookie-Regelung aus der Richtlinie (EU) 2002/58 (ePrivacy-Richtlinie) um. Ebenfalls am 1. Dezember 2021 ist das neue Telekommunikationsgesetz (TKG) in Kraft getreten. Im Telemediengesetz (TMG) und im TKG sind nun keine Datenschutzvorschriften mehr enthalten. Wir informieren über die wesentlichen Neuerungen.**

Das TTDSG richtet sich zum einen an Anbieter*innen von öffentlichen Telekommunikationsdiensten, zu denen vor allem Internet- und Mobilfunkanbieter*innen zählen. Für sie gelten die Regelungen der §§ 3 bis 18 TTDSG zum Datenschutz und für den Schutz der Privatsphäre in der Telekommunikation. Zum anderen richtet sich das TTDSG an Anbieter*innen von Telemediendiensten. Dies sind unter anderem öffentliche und nicht-öffentliche Stellen und Privatpersonen, die Websites, Apps oder auch Smart-Home-Anwendungen betreiben. An sie richten sich die in §§ 19 bis 26 TTDSG enthaltenen Regelungen zum Datenschutz sowie zum Schutz der Privatsphäre von Endeinrich-

tungen. Mit Endeinrichtungen sind vor allem internetfähige Geräte, wie Desktop-Computer, Tablets, Smartphones oder Smart-TVs gemeint.

Für die Durchsetzung der Regeln des TTDSG gegenüber Anbieter*innen von Telekommunikationsdiensten und öffentlichen Stellen des Bundes ist der BfDI die zuständige Aufsichtsbehörde. Die Landesdatenschutzbehörden überwachen die Durchsetzung der Regeln des TTDSG gegenüber den übrigen öffentlichen und nicht-öffentlichen Stellen. Ausnahmen gelten außerdem für die Aufsicht von Stellen im Rundfunkbereich.

Eine für Telemedienanbieter*innen- und -nutzer*innen besonders wichtige Vorschrift ist der § 25 TTDSG, der die sog. Cookie-Regelung aus Art. 5 Abs. 3 ePrivacy-Richtlinie umsetzt. Nach § 25 Abs. 1 TTDSG darf das Speichern von Informationen (zu denen insbesondere der Einsatz von Cookies und die Einbindung von Drittdiensten zählen) auf einem Endgerät sowie deren Auslesen grundsätzlich nur mit einer Einwilligung der Nutzer*innen erfolgen. Die Einwilligung muss den Regeln der DS-GVO entsprechen. Dies betrifft sowohl die Informationspflichten gegenüber den Endnutzer*innen als auch die formalen und inhaltlichen Anforderungen.

Nach § 25 Abs. 2 TTDSG ist in jenen Fällen keine Einwilligung erforderlich, in denen der Einsatz der Cookies oder die Einbindung von Drittdiensten unbedingt erforderlich ist, damit zum Beispiel Websitebetreiber*innen einen von Nutzer*innenseite ausdrücklich gewünschten Dienst zur Verfügung stellen können. Da es sich um eine Ausnahmeregelung handelt, ist grundsätzlich von einem engen Verständnis auszugehen und es fallen nur einzelne, klar abgrenzbare

und von der/dem Nutzer*in explizit gewünschte Dienste darunter. Beispiele für Ausnahmen vom Erfordernis der Einwilligung sind etwa Warenkorb-Cookies, Cookies zur Aufzeichnung der Sprach- oder Länderpräferenz der Nutzer*innen, Cookies zur Verwaltung der Zahlung oder Systeme zur Betrugsprävention und Sicherheit sowie Cookies, die für die Nutzung von Kontaktformularen, von Push-Nachrichten oder von Kartendiensten gesetzt werden. Hierbei ist jedoch grundsätzlich zu berücksichtigen, dass die jeweiligen Cookies erst dann gesetzt bzw. ausgelesen werden dürfen, wenn die konkreten Dienste von den Nutzer*innen aktiv „gewünscht“, also angeklickt werden.

Website- und App-Betreiber*innen können sich bei der Verwendung von Cookies seit Inkrafttreten des TTDSG demnach nicht mehr ausschließlich auf die Rechtsgrundlage des Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO berufen, wonach Verarbeitungen von Nutzer*innendaten immer dann ohne Einwilligung erfolgen durften, wenn das berechtigte Interesse der Anbieter*innen den Nutzer*inneninteressen überwog. Vielmehr kann auf das Einholen einer Einwilligung jetzt nur noch dann verzichtet werden, wenn einer der Ausnahmetatbestände des § 25 Abs. 2 TTDSG erfüllt ist. In den meisten Fällen sind die Datenschutzbehörden jedoch auch vor Inkrafttreten des TTDSG, also allein unter Anwendung der DS-GVO, zu ähnlichen Ergebnissen gekommen, zumal die Regelung des Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO seit jeher eng auszulegen ist.

An das Setzen und Auslesen der Cookies bei der Nutzung von Websites, wofür nun der § 25 TTDSG

gilt, schließen sich in der Regel weitere Verarbeitungen an. Hierbei werden zum Beispiel die in den Cookies gespeicherten Nutzungsdaten an Dritte übermittelt oder an anderer Stelle gespeichert. Derartige Verarbeitungsschritte sind nicht mehr nach dem TTDSG, sondern, wie bislang, ausschließlich nach den Regeln der DS-GVO zu beurteilen. Zentrale Rechtsnorm ist dann nach wie vor Art. 6 Abs. 1 DS-GVO. Immer dann, wenn die weitere Verarbeitung der Nutzer*innendaten zum Beispiel websiteübergreifend für Zwecke Dritter erfolgt, ist regelmäßig eine weitere, vorherige Einwilligung der Nutzer*innen nach Art. 6 Abs. 1 Satz 1 Buchstabe a DS-GVO einzuholen. Diese Einwilligung nach DS-GVO kann mit jener nach § 25 TTDSG als sog. gebündelte Einwilligung verbunden werden.

Ebenfalls neu sind die mit § 26 TTDSG eingeführten Regelungen über Dienste für die Einwilligungsverwaltung und Endnutzereinstellungen („Personal Information Management Services“, abgekürzt: PIMS). Anstatt auf jeder einzelnen Webseite mit Einwilligungs-Bannern konfrontiert zu werden, sollen Nutzer*innen über PIMS einmalig die Voraussetzungen für die Einwilligung oder die Ablehnung einer Datenerhebung festlegen können. Die PIMS könnten dann die gespeicherten Informationen automatisch an die Webseiten weitergeben, sodass die lästigen Cookie-Banner obsolet würden. Für die praktische Umsetzung der PIMS, die einer Anerkennung durch eine unabhängige Stelle bedürfen, müssen zunächst noch Rechtsverordnungen zur Regelung der Detailfragen erlassen werden.

Die Datenschutzkonferenz hat am 20. Dezember 2021 als Hilfestellung eine Orientierungshilfe für Anbieter*innen von Telemedien veröffentlicht (OH Telemedien 2021). Diese legt einen Schwerpunkt auf die datenschutzkonforme Umsetzung von § 25 TTDSG.

Auch das neue TKG ist am 1. Dezember 2021 in Kraft getreten. Mit ihm wird der „Europäische Kodex für die elektronische Kommunikation“ von 2018 in deutsches Recht umgesetzt. Im neuen TKG erfolgt unter anderem eine Verschärfung der Kunden*innenschutzvorschriften. Zudem ist der Begriff des Telekommunikationsdienstes im TKG jetzt weiter gefasst, was zu einer etwas anderen Verteilung der Zuständigkeiten zwischen dem BfDI und den Landesdatenschutzbehörden führt. So können jetzt sog. „over the top“- Kommunikationsdienste (auch OTT- Kommunikationsdienste genannt) eindeutig als Telekommunikationsdienste qualifiziert werden. OTT- Kommunikationsdienste sind Dienste, deren Nutzung nicht an einen bestimmten Festnetz- oder Mobilfunkanschluss gebunden ist. Daher fallen Messenger-Dienste wie WhatsApp & Co., Skype oder Threema jetzt eindeutig unter den Begriff des Telekommunikationsdienstes und damit wegen § 9 Abs. 1 BDSG in die Zuständigkeit des BfDI.

Der erweiterte Telekommunikationsdienste-Begriff führt darüber hinaus dazu, dass nun auch Webmail-Dienste (wie Gmail.de, freemail.de oder webmail.de) als Telekommunikationsdienste einzuordnen sind, für deren Datenschutzkontrolle seit dem 1. Dezember 2021 ebenfalls der BfDI zuständig ist. Das war wegen des sog. G-Mail-Urteils des Europäischen Gerichtshofes (EuGH - Urteil vom 13. Juni 2019, Az. C-

193/18) vorher anders zu beurteilen. Auch Videokonferenzdienste, die bis zum 1. Dezember 2021 als Telemediendienste eingeordnet wurden, sind nunmehr als Telekommunikationsdienste zu bewerten. Das führt unter anderem dazu, dass Stellen, die Videokonferenzdienste einsetzen, keinen Auftragsverarbeitungsvertrag mehr mit den Videokonferenzanbieter*innen abschließen müssen und für die aufgrund der Übertragung des Videochats verarbeiteten personenbezogenen Daten nicht mehr verantwortlich sind. Selbstverständlich sind sie nach wie vor dazu verpflichtet, technische und organisatorische Maßnahmen zu treffen, wie zum Beispiel datenschutzfreundliche Grundeinstellungen vorzunehmen.

Durch § 25 TTDSG wird Art. 5 Abs. 3 ePrivacy-Richtlinie endlich umgesetzt. Cookies können nun grundsätzlich nur noch mit Einwilligung der Nutzer*innen gesetzt und ausgelesen werden. Ausnahmen sind lediglich noch unter den engen Voraussetzungen des § 25 Abs. 2 TTDSG möglich. Mit dem neuen TKG wird der Begriff des Telekommunikationsdienstes erweitert, sodass jetzt unter anderem Messenger-Dienste, Webmail-Dienste und Videokonferenzdienste als Telekommunikationsdienste einzuordnen sind.

## 4.2 Sharenting – Kinderfotos im Internet

**Manche Eltern veröffentlichen Fotos ihrer Kinder im Internet. Was auf den ersten Blick wie ein harmloses „Posten“ und „Teilen“ von Urlaubsfotos anmutet, ist unter dem Stichwort „Sharenting“ bekannt. Welche Folgen ein solcher, digitaler Fußabdruck für die Kinder im Einzelfall haben kann, bedenken Eltern oft nicht.**

Uns erreichen immer mehr Eingaben, die sich auf Veröffentlichungen im Internet durch natürliche Personen beziehen. Bildaufnahmen gut erkennbarer Personen sind immer auch personenbezogene Daten. Im Falle eines Uploads im Internet werden diese automatisiert verarbeitet. Mit der Internetveröffentlichung ist eine weltweite und grundsätzlich unbegrenzte Zugriffsmöglichkeit verbunden. Damit wird das sog. Haushaltsprivileg für familiäre und persönliche Tätigkeiten verlassen, das eine Ausnahme von der DS-GVO definiert (siehe ausführlich 25. Bericht unter 4.7). Eltern sind damit datenverarbeitende Stellen, wenn sie Fotos ihrer Kinder im Internet veröffentlichen.

Die DS-GVO statuiert in Erwägungsgrund 38 (EG) in Bezug auf Kinder eine besondere Schutzbedürftigkeit:

*„Kinder verdienen bei ihren personenbezogenen Daten besonderen Schutz, da Kinder sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind.“*

Das Recht am eigenen Bild wird altersunabhängig vom allgemeinen Persönlichkeitsrecht des Kindes

nach Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz geschützt. Seine Ausprägung findet dieser Grundrechtsschutz in den §§ 22 und 23 Kunsturhebergesetz (KunstUrhG). Danach ist für eine Veröffentlichung grundsätzlich die Einwilligung der abgebildeten Person erforderlich. Ist die Person noch minderjährig, wird für eine Einwilligung an die Einsichtsfähigkeit des Kindes angeknüpft. Diese wird in der Regel mit dem 14. Lebensjahr angenommen, kann im Einzelfall aber auch früher vorliegen. Soweit noch keine Einsichtsfähigkeit angenommen werden kann, kommt es regelmäßig auf die Einwilligung beider Elternteile an. Hierzu hatte das OLG Düsseldorf zuletzt entschieden, dass das Verwenden von Fotografien dem Einwilligungserfordernis des Art. 6 Abs. 1 Satz 1 Buchstabe a DS-GVO unterfällt (OLG Düsseldorf, Beschluss vom 20. Juli 2021, Az. 1 UF 74/21).

Das Recht am eigenen Bild ist durch die Internetveröffentlichung im erhöhten Maße gefährdet, da die Fotos weltweit zugänglich gemacht werden. Mithin ist eine verlässliche Löschung von Fotos nicht möglich und eine etwaige Weiterverbreitung kaum kontrollierbar. (siehe hierzu OLG Oldenburg, Beschluss vom 24. Mai 2018 – 13 W 10/18, Rz. 12, so zuletzt auch OLG Düsseldorf, Beschluss vom 20. Juli 2021, Az. 1 UF 74/21, Rz. 8). Dies kann erhebliche Auswirkungen auf die Entwicklung der abgebildeten Kinder haben und zu einer unzulässigen Beschneidung ihrer Rechte führen. Im Internet veröffentlichte Personenfotos können oft nicht restlos gelöscht werden. Das Recht auf Vergessenwerden nach Art. 17 der DS-GVO läuft faktisch leer und die Kinderfotos sind potenziell für immer für einen unbeschränkten Personenkreis verfügbar. „Das tangiert spürbar die Integrität ihrer Persönlichkeit und ihrer Privatsphäre“, so das

OLG Düsseldorf. Sowohl die Nutzung solcher Fotos für Cybermobbing als auch die Aufmerksamkeit pädophiler Personen für Kinderbilder im Internet können zu ernsten seelischen und schlimmstenfalls körperlichen Beeinträchtigung der betroffenen Kinder führen.

Erfolgt die Veröffentlichung auf Initiative der Eltern, die mit der Publikation auch ein eigenes wirtschaftliches Interesse verbinden, besteht ein Interessenkonflikt: Das wirtschaftliche Publikationsinteresse der Eltern kollidiert mit dem Kindeswohl, insbesondere sofern das Kind noch nicht einsichtsfähig ist und nicht selbst über eine Veröffentlichung entscheiden kann.

Die LDI NRW befasste sich in diesem Zusammenhang mit einer Eingabe, in der es um Veröffentlichungen einer sog. „Influencerin“ ging. Sie stellte regelmäßig Fotografien ihrer minderjährigen Kinder auf ihrer Internetpräsenz sowie ihrem Instagram-Account online. Die Veröffentlichungen (Fotos und Text) dienten unter anderem dazu, Produkte verschiedener Unternehmen gegen Vergütung zu bewerben. Im Rahmen der Prüfung der nach § 22 KunstUrhG erforderlichen Einwilligung beider Elternteile ergab sich der vorstehend geschilderte Interessenkonflikt. Dessen Auflösung ist juristisch umstritten und ist bisher gesetzlich nicht gesondert geregelt, soweit keine Einsichtsfähigkeit der betroffenen Minderjährigen vorliegt.

Wir haben die Influencerin über die aktuelle Rechtslage, die damit verbundenen Problemstellungen und nachdrücklich über die besondere Schutzbedürftigkeit der Kinder bei Internetveröffentlichungen informiert. Die verantwortliche Stelle hat seitdem die Auswahl der Fotos mit Kindern dahingehend angepasst, dass diese zumeist nur bildabgewandt gezeigt werden.

Angesichts der kaum kontrollierbaren Weiterverarbeitung von im Internet veröffentlichten Kinderfotografien und der Gefahr einer unberechtigten Nutzung durch Dritte (Pädophilie, Cybermobbing), ist bei der Veröffentlichung von Kinderfotos eine besondere Vorsicht geboten.

Kinder verdienen im Hinblick auf ihre personenbezogenen Daten besonderen Schutz. Es bedarf einer stärkeren präventiven Aufklärung über die Gefahren bei Veröffentlichungen von Kinderfotografien im Internet. Sie ist grundsätzlich nur mit der Einwilligung beider Elternteile zulässig, wenn das Kind noch nicht einsichtsfähig sein sollte. Die bestehende Rechtslage weist aktuell eine Regelungslücke für die Veröffentlichung von Fotos noch nicht einsichtsfähiger Kinder im Internet auf, soweit diese auch im wirtschaftlichen Interesse der Eltern erfolgt. Hier sollte der Gesetzgeber adäquate Regelungen zum Schutz von Kindern treffen.

## 4.3 Richterschelte im Internet

**Im Internet verbreiten viele Menschen ihre persönliche Meinung, oft auch über andere Personen. Enthalten die Veröffentlichungen personenbezogene Daten, sind die Vorgaben der DS-GVO zu beachten.**

Durch eine Eingabe sind wir darauf aufmerksam gemacht worden, dass ein Richter im Internet unter Nennung seines Namens für seine Entscheidungen in einem Gerichtsverfahren angegriffen wird. Begründet werden die Veröffentlichungen von der verantwortlichen Person damit, dass es erforderlich und von der

Meinungsfreiheit gedeckt sei, die Öffentlichkeit im Zusammenhang mit den getroffenen richterlichen Entscheidungen über bestehende Missstände zu unterrichten.

Das Recht auf Meinungsfreiheit findet seine Schranken in den Vorschriften der allgemeinen Gesetze. Dazu zählen auch die Gesetze zum Persönlichkeitsschutz von Betroffenen und deren Recht auf informationelle Selbstbestimmung. Die DS-GVO lässt Datenverarbeitungen, für die es ein überwiegendes berechtigtes Interesse gibt, grundsätzlich zu. Zugleich eröffnet sie damit die Möglichkeit, zwischen Meinungsfreiheit und den Interessen der betroffenen Person abzuwägen. Bei der Beurteilung von Internetveröffentlichungen mit Personenbezug anhand der Vorgaben der DS-GVO sind die Wertungen des Grundgesetzes und die diesbezügliche Rechtsprechung also zu berücksichtigen. Ob es zur Ausübung der Meinungsfreiheit im Rahmen eines berechtigten Interesses erforderlich ist, personenbezogene Daten zu verarbeiten, bemisst sich anhand einer Gesamtabwägung aller im Einzelfall betroffenen Interessen.

Bei Äußerungen ist zunächst deren konkreter Gehalt zu betrachten. Das Gewicht der Meinungsfreiheit ist umso höher, je stärker die Äußerung darauf abzielt, einen Beitrag zur öffentlichen Meinungsbildung zu leisten. Umso geringer ist es, wenn es nur um eine emotionale Verbreitung von Stimmungen gegen einzelne Personen geht. In die Abwägung ist miteinzubeziehen, ob die Privatsphäre der Betroffenen oder ihr öffentliches Wirken Gegenstand der Äußerung ist. Denn die Verfassung setzt einer auf die Person abzielenden, insbesondere öffentlichen Verächtlichmachung oder Hetze äußerungsrechtliche Grenzen.

Ebenfalls kommt es bei der Abwägung darauf an, ob und inwieweit für eine betreffende Äußerung ein konkreter und nachvollziehbarer Anlass bestand und welche Verbreitung und Wirkung sie entfaltet.

Bei einer sachlichen Auseinandersetzung mit dem Thema wird das Recht auf informationelle Selbstbestimmung der Betroffenen in der Regel gegenüber dem Recht auf Meinungsäußerung zurücktreten müssen, auch wenn sie namentlich kritisiert werden. Denn das Persönlichkeitsrecht verleiht keinen Anspruch darauf, nur so in der Öffentlichkeit dargestellt zu werden, wie es genehm ist.

Werden allerdings nicht nur die Entscheidungen eines Richters gerügt, sondern wird dieser unbelegt außerdem beschuldigt, willkürlich zu handeln, Recht missbräuchlich auszuüben sowie Urkundenfälschung und Rechtsbeugung begangen zu haben, sind solche Äußerungen im Internet dazu geeignet, die betroffene Person in ihrem Amt zu schädigen. Entsprechende Datenverarbeitungen sind daher nicht mehr von der Meinungsfreiheit gedeckt

Der Verantwortliche lehnte eine Löschung der Veröffentlichungen ab. Im Rahmen einer Anordnung wurde dem Verantwortlichen aufgegeben, die Internetbeiträge zu löschen. Darüber hinaus wurde ihm untersagt, die ehrverletzenden Äußerungen auf Internetseiten oder in sonstiger Weise zu veröffentlichen. Der Ausgang des Verfahrens bleibt abzuwarten.

Von unseren datenschutzrechtlichen Prüfungen ausgenommen sind personenbezogene Darstellungen im Internet, die dem sog. Medienprivileg nach Art. 85 DS-GVO unterliegen, das Ausnahmen von der An-

wendung einzelner DS-GVO-Regelungen bei Datenverarbeitungen zu journalistischen Zwecken vorsieht. Vorliegend handelte es sich nicht um eine journalistische Tätigkeit.

Werden im Rahmen der Wahrnehmung des Rechts auf freie Meinungsäußerung personenbezogenen Daten veröffentlicht, kommt es regelmäßig zu einem Spannungsverhältnis zwischen der Meinungsfreiheit und dem Datenschutz Betroffener. Zwar darf das Datenschutzrecht nicht dazu dienen, die freie Meinungsäußerung und die Informationsfreiheit, die eine essenzielle Grundlage der Demokratie bilden, auszuhebeln. Aber auch dem Recht auf Meinungsfreiheit sind Schranken durch den Persönlichkeitsschutz und das Recht auf informationelle Selbstbestimmung gesetzt. Regelmäßig ist dabei eine Abwägung der Grundrechte vorzunehmen.

# 5. Schule und Bildung

## 5.1 Gerichtsentscheidungen

### Corona – Befreiung von der Maskenpflicht an Schulen aus medizinischen Gründen

Die Coronabetreuungsverordnung (CoronaBetrVO) sieht seit dem 26. Oktober 2020 vor, dass Personen, die aus medizinischen Gründe in schulischen Gemeinschaftseinrichtungen keine Maske tragen können, das Vorliegen dieser Gründe durch ärztliches Attest nachweisen müssen. Durch seinen Beschluss vom 15. Juli 2021, Az. 13 B 507/21, stellt das OVG NRW klar, dass die zur Glaubhaftmachung eines Ausnahmetatbestands in Bezug auf die Maskenpflicht an Schulen vorzulegenden Atteste nach wie vor die Mindestanforderungen erfüllen müssen, die es in seinem Beschluss vom 24. September 2020 aufgestellt hatte.

Wie unserer Information „Maskenpflicht und Masernschutz – Verarbeitung von Gesundheitsdaten durch Schulen“, abrufbar unter www.ldi.nrw.de, im Einzelnen zu entnehmen ist, obliegt den Schulleitungen die Prüfung und Feststellung, ob Schüler*innen nach der CoronaBetrVO aufgrund des Vorliegens medizinischer Gründe vom Tragen einer Maske befreit sind. Diese sind berechtigt, die hierfür erforderlichen Daten zu verarbeiten. Der Inhalt der auf Verlangen vorzulegenden Atteste muss der Schulleitung und, im Fall einer gerichtlichen Auseinandersetzung, auch dem Gericht nach den Feststellungen des OVG NRW die Prüfung ermöglichen, ob die dargelegten medizinischen Gründe für eine Befreiung von der Maskenpflicht für medizinische Laien plausibel sind. Die LDI NRW teilt die grundlegende Auffassung des OVG

NRW. Die Angabe konkreter Diagnosen in den Attesten halten wir in aller Regel nicht für erforderlich.

**Videoüberwachung während Online-Prüfungen an Hochschulen zulässig**

Mit Beschluss vom 4. März 2021 (Az. 14 B 278/21.NE) hat das OVG NRW entschieden: Videoaufsicht häuslicher Klausurprüfungen ist zulässig. Danach werden die Prüflinge durch aufsichtführende Personen per Webcams während der Prüfung überwacht. Eine Videoüberwachung ist im Hinblick darauf, dass die Hochschulen bei der Durchführung von Prüfungen den prüfungsrechtlichen Grundsatz der Chancengleichheit Geltung verschaffen müssen, geeignet und erforderlich. Dieser Grundsatz verlangt, dass für vergleichbare Prüflinge so weit wie möglich vergleichbare Prüfungsbedingungen gelten, um allen Teilnehmenden gleiche Erfolgschancen zu bieten.

Die LDI NRW teilt die Auffassung, dass eine solche Videoüberwachung in Betracht kommt, hält dabei allerdings eine nähere Differenzierung für geboten. Siehe hierzu unter 5.4.

## 5.2 Veröffentlichungen der Landesbeauftragten

- Nichtteilnahme am Präsenzunterricht zum Schutz vorerkrankter Angehöriger – Verarbeitung von Gesundheitsdaten durch Schulen, abrufbar unter www.ldi.nrw.de.
- Coronaselbsttests - Verarbeitung von Gesundheitsdaten durch Schulen, abrufbar unter www.ldi.nrw.de.

- Ergänzung des Homepagebeitrags „Pandemie und Schule – Datenschutz mit Augenmaß“, abrufbar unter www.ldi.nrw.de.

## 5.3 Einsatz der Plattform „Padlet“ an Schulen

**Die Plattform „Padlet“ ist beim pandemiebedingten Home Schooling zur Unterstützung des Unterrichts sehr beliebt geworden. Das Land hat den Einsatz von „Padlet“ zeitweise ebenfalls unterstützt. Leider kann dieses Produkt eines amerikanischen Anbieters an Schulen nicht datenschutzgerecht genutzt werden.**

Die Schulen sehen vor allem die Vorteile, die der Einsatz der Plattform „Padlet“ bietet. „Padlet“ ist nicht nur der Name der Plattform, sondern bezeichnet auch die einzelne, digitale Pinnwand, die die Lehrkräfte über die Plattform erstellen und im Unterricht mit ihren Schüler*innen interaktiv bearbeiten und um weitere Informationen u.a. aus dem Internet ergänzen können. So pädagogisch interessant das Produkt sein mag, bestehen beim Einsatz von „Padlet“ folgende Datenschutzprobleme:

Zum einen ist „Padlet“ ein Produkt der Wallwisher, Inc., ein Unternehmen mit Sitz in Kalifornien, USA, das nach der eigenen Datenschutzerklärung Daten der Nutzer*innen in die USA transferiert. Das Unternehmen stützt diesen Transfer auf Standarddatenschutzklauseln. Die Berufung auf derartige Klauseln für Datenübermittlungen in die USA ohne hinreichende ergänzende Maßnahmen genügt jedoch nicht. Das hat der Europäische Gerichtshof in seinem „Schrems II“-Urteil (C-311/18 vom 16. Juli 2020) klargestellt.

Zum anderen ist auch der Einsatz diverser Cookies und Tracker auf „Padlet“-Seiten bedenklich, der offenbar ohne vorherige Einwilligung erfolgt. Hinzu kommt, dass dadurch über Indicative, Google Analytics und Google Tag Manager Datenflüsse an Firmen möglich sind, die ebenfalls Daten in nicht-EU/EWR-Staaten, insbesondere in die USA, übermitteln. Wir gehen davon aus, dass die Schulen keine Möglichkeit haben, die ungesicherten Datenübermittlungen in Drittstaaten und Trackingfunktionen zu unterbinden.

„Padlet“ ermöglicht außerdem das Einbinden von Social Media-Elementen (YouTube-Videos, Facebook-, Twitter- und sonstige Buttons). Zwar sind die Schulen, die die Seiten einbinden oder ein „Padlet“ mit einer solchen Einbindung nutzen, nicht für die Inhalte des Videos oder anderer verlinkter Anwendungen verantwortlich. Bei diesen Websites findet aber regelmäßig eine einwilligungsbedürftige Verarbeitung von personenbezogenen Daten statt. Gerade sehr jungen Schüler*innen in Grundschulen, die den Verlinkungen folgen, fehlt regelmäßig die notwendige Einwilligungsfähigkeit nach Art. 8 DS-GVO. Darüber hinaus können sich Schüler*innen nicht freiwillig entscheiden, wenn es um Inhalte geht, die sie im Unterricht nutzen sollen. Einwilligungen sind nur dann eine taugliche Datenverarbeitungsgrundlage, wenn sie freiwillig erteilt werden.

Schließlich wird auf der Website von „Padlet“ darüber informiert, dass die Wallwisher, Inc. Nutzer*innendaten an Dritte übermittelt. Völlig unklar bleibt dabei, auf welcher Rechtsgrundlage welche Daten übermittelt werden.

Viele Schulen gingen davon aus, dass sie die Plattform „Padlet“ bedenkenlos einsetzen konnten, weil

das Schulministerium NRW und die ihm nachgeordneten Behörden Hinweise auf bestehende „Padlets“ gegeben haben oder selbst „Padlets“ veröffentlichten. Die LDI NRW hat das Schulministerium auf ihre Bedenken hinsichtlich des Einsatzes der Plattform „Padlet“ hingewiesen.

Die Schulen sind aufgefordert, den nicht datenschutzgerechten Einsatz der Plattform „Padlet“ zu unterlassen. Anders als zu Beginn der Pandemie stehen den Schulen in der Zwischenzeit datenschutzfreundlichere Alternativen, wie die vom Land NRW angebotene Lernplattform LOGINEO NRW LMS, zur Verfügung.

## 5.4 Online-Prüfungen an Hochschulen

**Zur Aufrechterhaltung des Lehrbetriebs während der Corona-Pandemie greifen Hochschulen auf online-basierte Lehrangebote zurück und führen Online-Prüfungen durch. Mit der Durchführung derartiger Prüfungen ist ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung der Studierenden verbunden. Wichtige Datenschutzbelange sind mit dem prüfungsrechtlichen Grundsatz der Chancengleichheit in Einklang zu bringen.**

Die Verordnung zur Bewältigung der durch das Coronavirus SARS-CoV-2-Epidemie an den Hochschulbetrieb gestellten Herausforderungen (CEHVO) sieht in § 6 Abs. 1 Satz 1 eine Befugnis der Hochschulen in NRW vor, Hochschulprüfungen in elektronischer Form oder in elektronischer Kommunikation (Online-Prüfungen) abzunehmen. Nach § 6 Abs. 3 Satz 1 CEHVO kann das Rektorat einer Hochschule

Regelungen hinsichtlich der Art und Weise der Abnahme von Online-Prüfungen erlassen. Mit der Änderung der Regelung des § 64 Abs. 2 Satz 2 des Gesetzes über die Hochschulen in NRW (HG NRW) wurde die vorbenannte temporäre Befugnis, Online-Prüfungen abzunehmen, in das Stammrecht überführt. Nach § 64 Abs. 2 Satz 3 HG NRW sind hierbei insbesondere Bestimmungen zum Datenschutz zu treffen.

Da weder § 6 CEHVO noch § 64 Abs. 2 Satz 2 HG NRW eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Rahmen der Durchführung von Online-Prüfungen im Sinne von Art. 6 Abs. 3 DS-GVO darstellen, ist insoweit auf die allgemeine Vorschrift des § 8 Abs. 7 HG NRW in Verbindung mit § 3 Abs. 1 DSG NRW zurückzugreifen. Gemäß § 3 Abs. 1 DSG NRW ist die Verarbeitung personenbezogener Daten durch öffentliche Stellen unter anderem zulässig, wenn sie für die Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe der verarbeitenden Stelle erforderlich ist. Dabei ist zu beachten, dass diese Rechtsgrundlage voraussetzt, dass die Verarbeitung der personenbezogenen Daten durch die öffentlichen Stellen erfolgt, das heißt im Verantwortungsbereich der Hochschule. Soweit sich die Hochschule bei der Durchführung von Online-Prüfungen externer Dienstleister bedient, hat sie die in Art. 28 DS-GVO normierten Anforderungen an die Auftragsverarbeitung zu erfüllen und so umzusetzen, dass sie „Herrin der Daten“ und damit Verantwortliche bleibt. Erlässt eine Hochschule zur Durchführung von Online-Prüfungen Regelungen nach Maßgabe des § 6 Abs. 3 CEHVO, hat sie die danach vorgesehenen Datenverarbeitungen auf das zu beschränken, was für die Abnahme der Online-Prüfungen erforderlich ist.

Bei Prüfungen kommt der Wahrung des Grundsatzes der Chancengleichheit besondere Bedeutung zu. Wie auch bei Präsenzklausuren müssen bei Online-Prüfungen Täuschungsmöglichkeiten ausgeschlossen werden. Die Präsenzsituation sollte dabei stets als Vergleich für das Maß der Überwachung herangezogen werden. Es ist ein mit den Persönlichkeitsrechten der Prüflinge nicht vereinbarer permanenter Überwachungsdruck zu vermeiden.

In der Regel ist danach eine Videobeobachtung ausreichend. Wenn die Aufsichtsführenden dabei Auffälligkeiten feststellen, kann eine Aufzeichnung zum Zweck des Nachweises von Täuschungsversuchen oder Störungen des Prüfungsablaufs gestartet werden. Dabei sind insbesondere die Datenschutzinteressen der Prüflinge zu berücksichtigen, die ohne Täuschungsabsicht an der Prüfung teilnehmen und keine Störungen des Prüfungsablaufs geltend machen. Eine dauerhafte, verdachtsunabhängige oder anlasslose Speicherung entsprechender Aufnahmen wäre nicht zulässig.

Auch das sog. automatisierte Proctoring stellt einen besonders schwerwiegenden Eingriff dar, der mangels Verhältnismäßigkeit unzulässig ist. Dabei werden anhand von Bild- und Tonaufzeichnungen verschiedene Parameter wie Tastenanschläge oder Kopf- und Augenbewegungen der Prüflinge daraufhin ausgewertet, ob ein Täuschungsversuch vorgelegen haben könnte. Dies erzeugt ständigen und hohen Überwachungsdruck, den es bei einer Präsenzklausur in dieser Form nicht gäbe. Derzeit wird eine Handreichung für Hochschulen mit weiteren Informationen zu diesem Thema erstellt.

Hochschulen dürfen bei Online-Klausuren nur erforderliche Überwachungsmaßnahmen treffen. Für die Beurteilung der Erforderlichkeit einer Regelung bildet die Präsenzklausur den Vergleichsmaßstab.

# 6. Verwaltung, Inneres und Justiz

## 6.1 Gerichtsentscheidungen

### Das OVG NRW bestätigt: Examenskandidat*innen haben einen Anspruch auf kostenlose Klausurkopien

Mit Urteil vom 8. Juni 2021 (Az. 16 A 1582/20) hat das OVG NRW entschieden: Prüflinge haben gegenüber dem Landesjustizprüfungsamt NRW einen Anspruch auf kostenfreie Überlassung der im zweiten juristischen Staatsexamen angefertigten Klausuren mitsamt Gutachten – entweder in Papierform oder in elektronischem Format. Das Gericht bestätigt damit die Entscheidung des Verwaltungsgerichts Gelsenkirchen (Urteil vom 27. April 2020, Az. 20 K 6392/18) sowie die Auffassung der LDI NRW (siehe 26. Bericht unter 6.7). Das Urteil ist noch nicht rechtskräftig, da das Landesjustizprüfungsamt NRW Revision eingelegt hat.

## 6.2 Veröffentlichungen

- Datenschutz bei Ordnungswidrigkeiten – Ermittlung von Fahrer*innen mittels Lichtbildabgleich, abrufbar unter www.ldi.nrw.de.
- Auskunft aus dem Fahreignungsregister des Kraftfahrtbundesamts (KBA), abrufbar unter www.ldi.nrw.de.

## 6.3 Datenbankübergreifende Analyse und Recherche (DAR) durch die Polizei NRW

**Zur Bekämpfung schwerwiegender Straftaten möchte die Polizei NRW nicht länger verschiedene gesonderte Dateisysteme einzeln auswerten. Vielmehr verspricht sie sich einen höheren Erkenntnis- sowie auch Zeitgewinn durch eine DAR. Zu diesem Zweck setzt sie seit Oktober 2020 die Software Palantir-Gotham mit Echtdaten ein. Die Polizei NRW hat viel Mühe darauf verwendet, die Zugriffsrechte auf die Einzeldatenbanken bei der Abfrage über DAR weitgehend aufrecht zu erhalten. Einige Aspekte der konkreten Anwendung der Software führen aber dazu, dass sie ohne eine gesetzliche Erlaubnis nicht betrieben werden darf.**

Das Landeskriminalamt NRW hatte uns im Januar 2020 über die Vergabe eines Auftrags zur DAR an die Firma Palantir informiert. Nachdem es einige Zeit dauerte, bis uns prüffähige Unterlagen vorlagen, machte die LDI mit Stellungnahme vom 25. Februar 2021 darauf aufmerksam, dass für den Betrieb des Programms eine Rechtsgrundlage notwendig sei (Landtags-Drs.: Stellungnahme 17/508). Wir wiesen darauf hin, dass die bisher im Polizeigesetz NRW und der Strafprozessordnung bestehenden Regelungen für den Einsatz der DAR-Software nicht ausreichen, denn die Daten werden mit DAR systematisch für neue Zwecke verarbeitet, die über das hinausgehen, wofür die Daten originär gespeichert wurden. Das erzeugt eine neue und hohe Eingriffsintensität, die durch die bestehenden Rechtsgrundlagen für die Datenverarbeitung durch die Polizei nicht gedeckt ist.

Um uns einen Eindruck von der konkreten Funktionsweise der eingesetzten Software zu vermitteln, wurde uns diese im Juli 2021 vom Innenministerium NRW und vom Landeskriminalamt NRW präsentiert. Dies bestätigte unsere Einschätzung, dass die Software die Zusammenführung einer Vielzahl vormals zu unterschiedlichen Zwecken erhobener und unter Beachtung des Grundsatzes der Zweckbindung getrennt voneinander gespeicherter Daten und deren anschließende Analyse und Auswertung ermöglicht. Dabei hat das System Vollzugriff auf mehr als zehn verschiedene polizeiliche Dateisysteme. Auch Daten, die aus eingriffsintensiven Maßnahmen, wie beispielsweise Quellen-Telekommunikation oder Funkzellenabfragen, gewonnen wurden, sind einbezogen. Außerdem werden Daten von Personen recherchierbar, die sich selbst nicht strafbar gemacht haben oder als gefährdend in Erscheinung getreten sind, etwa Daten von Zeug*innen oder Anrufer*innen bei der Notrufnummer 110. Erst in der Präsentation wurde deutlich, dass DAR nicht in den vorhandenen Daten recherchiert, sondern alle Daten aus den einbezogenen Datenbanken spiegelt. Damit wird ein eigener und neuer Datenpool erzeugt.

Zusätzlich können externe Dokumente und Daten aus dem bundesweiten polizeilichen Datenverbund sowie aus externen Registern, wie beispielsweise dem Melderegister, in die Analyse hinzugefügt werden. Eine unmittelbare Anbindung externer Datenbanken erfolgt indessen nicht. Die gefundenen Ergebnisse kann die Software auf verschiedene Arten grafisch darstellen.

Bei der Präsentation war erkennbar, dass sich die Polizei NRW bei der Planung der Software durchaus sehr um einen datenschutzgerechten Einsatz bemüht

hat. Dies zeigen unter anderem das dezidierte Rechte-und-Rollenkonzept sowie der Umstand, dass die in den USA ansässige Firma im Rahmen der Wartung keinen Zugriff auf Echtdaten der Polizei NRW erhält. Nach Auswertung der Präsentation hat die LDI NRW das Innenministerium noch einmal eindringlich darauf hingewiesen, dass das Programm einer Rechtsgrundlage bedarf. Die bereits dargelegten Gründe haben sich durch die Präsentation erhärtet.

Inzwischen hat das Innenministerium einen Gesetzentwurf für die Nutzung des Systems zu Gefahrenabwehrzwecken vorgelegt. Abseits der vorrangig zu klärenden Frage der Rechtsgrundlage ist aufgrund der Komplexität der Software, die Prüfung der praktischen Anwendung des Programms noch nicht abgeschlossen.

Trotz eines gut ausgearbeiteten Rechte- und Rollenkonzeptes bedarf der Einsatz des DAR-Systems aufgrund der hohen Eingriffsintensität einer parlamentarischen Legitimation. Nicht die Polizei, sondern der Gesetzgeber muss die Grundentscheidung treffen, welche Straftaten eine solche Schwere aufweisen, dass für deren Abwehr die Zweckbindung der Daten über alle Datenbanken hinweg aufgehoben wird und auch Daten nicht straffällig gewordener Personen recherchefähig gemacht werden dürfen. Die Anwendung des Programms im Einzelnen werden wir weiterhin überwachen. Aktuelle Bestrebungen der Länder, auch den Einsatz solcher Anwendungen für die Strafverfolgung zu legitimieren, werden wir ebenso aufmerksam verfolgen.

## 6.4 Polizei übermittelt unzulässig mehr als 12.500 Telefonnummern

**Im Rahmen von Ermittlungen gegen Polizeibedienstete wegen rechtsextremer Handlungen wurden sämtliche Telefonnummern, die in den Mobiltelefonen der verdächtigten Personen gespeichert waren, ohne jegliche Vorauswahl an über zwanzig Sicherheitsbehörden übermittelt. Wie unsere Überprüfung ergab, war eine Übermittlung in diesem Umfang nicht zulässig.**

Eine bei einem Polizeipräsidium eingerichtete Sonderkommission (besondere Aufbauorganisation – BAO) ermittelte gegen mehrere Polizeibedienstete wegen Delikten im Bereich des Rechtsextremismus. Sie beschlagnahmte dabei insgesamt 46 Mobiltelefone von 24 Verdächtigen. Ohne die rechtsextremen Chats, die auf den beschlagnahmten Geräten gespeichert waren, ausgewertet und so möglicherweise Hinweise auf konkrete weitere Beteiligte an diesen Chats ermittelt zu haben, gab die BAO eine Liste von mehr als 12.500 Telefonnummern an andere Sicherheitsbehörden mit der Bitte um Überprüfung weiter. Betroffen waren also auch mögliche behandelnden Ärzt*innen oder etwaige Bekanntschaften aus Sportvereinen oder anderen Personen, deren Nummern auf den Handys gespeichert sind, ohne dass es Hinweise zu einem Bezug dieser Personen zur rechten Szene überhaupt gab. Die BAO richtete in diesem Zusammenhang eine kriminaltaktische Anfrage an den Verfassungsschutz NRW und das LKA NRW und bat gleichzeitig um Weiterleitung an das Bundeskriminalamt, die Bundespolizei, das Bundesamt für Verfassungsschutz, an alle Landeskriminalämter sowie das Zollkriminalamt. Sie begründete die Maßnahme mit

dem Zweck, rechtsextreme Netzwerke aufdecken zu wollen.

Die Übermittlung sämtlicher auf den Geräten befindlicher Telefonnummern, ohne die dort gespeicherte Kommunikation zunächst ausgewertet zu haben, erwies sich bei der näheren Überprüfung als unzulässig. Eine der gesetzlichen Voraussetzungen für eine solche Weiterverarbeitung der Daten war nämlich das Vorliegen eines konkreten Ermittlungsansatzes hinsichtlich der in Rede stehenden Kontaktdaten. Die Kommunikation, die auf den beschlagnahmten Mobilgeräten gespeichert war, hätte also zunächst dahingehend ausgewertet werden müssen, welche der gespeicherten Kontakte sich an den rechtsextremen Chats beteiligt hatten. Nur diese Telefonnummern durften mit den Datenbanken anderer Sicherheitsbehörden abgeglichen werden, um hierdurch eine etwaige Mitgliedschaft dieser Kontakte an regionalen oder bundesweiten rechtsextremen Netzwerken feststellen zu können.

Ohne eine derartige vorherige Auswertung der beschlagnahmten Chat-Daten, aus der sich entsprechende Hinweise hätten ergeben können, konnten etwaige Ermittlungsansätze jedoch überhaupt nicht erkannt werden. Vielmehr sollten im vorliegenden Fall erst durch den „ins Blaue hinein“ erfolgten Abgleich konkrete Ermittlungsansätze zu Tage gefördert werden.

Schon aus diesem Grund war die Übermittlung sämtlicher Telefonnummern der Kontakte der verdächtigten Personen unzulässig. Damit fehlte es gleichzeitig an der für die Übermittlung stets erforderlichen Verhältnismäßigkeit der Maßnahme. Die gesetzlichen

Übermittlungsvoraussetzungen waren also nicht erfüllt.

Wir haben das betroffene Polizeipräsidium über die Rechtswidrigkeit der Massenübermittlung informiert und gleichzeitig dringend eine Folgenbeseitigung bzw. -abmilderung für die betroffenen Personen empfohlen.

Es ist richtig und wichtig, konsequent gegen rechtsextreme Netzwerke vorzugehen. Dieser legitime Zweck muss aber auch mit legitimen Mitteln verfolgt werden. Personen, die keinerlei Anlass für eine Strafverfolgung gegeben haben und nur zufällig in den Fokus der Polizei geraten, müssen wirksam davor geschützt werden, dass ihre Daten „ins Blaue hinein“ an andere Sicherheitsbehörden übermittelt werden.

## 6.5 Kontrolle von Verfahrensrückmeldungen der Staatsanwaltschaften an die Polizeibehörden

**Wenn in Strafverfahren zunächst von der Polizei ermittelt wurde, ist die Staatsanwaltschaft nach Abschluss des Verfahrens verpflichtet, der Polizei den Verfahrensausgang mitzuteilen, damit diese ihre Datensätze ggf. entsprechend berichtigen kann. Wie unsere stichprobenartige Kontrolle belegt, wird diesen Anforderungen in der Praxis allerdings nicht immer Rechnung getragen.**

Die obligatorischen Rückmeldungen der Staatsanwaltschaften an die Polizei, wie die einzelnen Strafverfahren ausgegangen sind, stellen ein wichtiges Instrument zur Berichtigung der polizeilichen Datenbestände dar. Vor allem bei Verfahrenseinstellungen und Freisprüchen hängt von dem jeweiligen Grund

hierfür die Entscheidung ab, ob die weitere Speicherung der Daten durch die Polizei zulässig ist. Umso wichtiger ist es, dass die Rückmeldung über Verfahrensausgänge an und die etwaige Korrektur der Daten durch die Polizei zeitnah und korrekt erfolgen. Bei unserer Arbeit werden wir jedoch immer wieder auf Fälle aufmerksam, in denen die Rückmeldung an die Polizei nicht, nicht zeitnah oder nicht vollständig erfolgt ist bzw. eine erfolgte Meldung durch die Polizei nicht zeitnah oder umfassend für die Überprüfung der Zulässigkeit der fortgesetzten Speicherung der polizeilichen Daten herangezogen wurde.

Diese Beobachtung haben wir zum Anlass für eine Stichprobenprüfung bei zwei Staatsanwaltschaften genommen. Von beiden Behörden wurden zunächst bestimmte vorausgewählte Strafverfahrensakten angefordert.

Eine Staatsanwaltschaft übersandte uns daraufhin die angeforderten 24 Strafverfahren. In drei dieser Verfahren war eine Rückmeldung an die Polizei nicht erforderlich. Von den verbliebenen 21 Verfahren war in fünf Fällen eine erforderliche Rückmeldung bei Verfahrensbeendigung ursprünglich nicht erfolgt. Sie wurde aus Anlass unserer Prüfung jedoch nachgeholt. Dies stellt immerhin knapp ein Viertel der geprüften Vorgänge dar, in denen eine Mitteilung erforderlich war. Zwischenzeitlich wurde uns zugesagt, die Bediensteten der Staatsanwaltschaft künftig regelmäßig auf die Erforderlichkeit zeitnaher und vollständiger Verfahrensrückmeldungen hinzuweisen.

Im Nachgang zur Kontrolle bei dieser Staatsanwaltschaft haben wir hinsichtlich eines Teils der in Rede stehenden Strafverfahren bei den beteiligten Polizeibehörden überprüft, ob ordnungsgemäß mit den dort

eingegangenen Rückmeldungen umgegangen worden war. Bei einer Behörde wurde ein grundsätzlich unzureichender Umgang mit den Verfahrensrückmeldungen festgestellt. In Fällen, in denen die polizeilichen Daten aufgrund der Art und Weise der Einstellung des Strafverfahrens (erwiesene Unschuld bzw. bereits fehlender Anfangsverdacht) vollständig zu löschen bzw. zu anonymisieren waren, erfolgte eine Löschung lediglich in Bezug auf die Kriminalakte. In den übrigen polizeilichen Datenbanken – insbesondere im Vorgangsverwaltungssystem – blieben die Personen jedoch weiter suchfähig gespeichert. Dies führt dazu, dass die Betroffenen auch bei künftigen Abfragen – beispielsweise im Rahmen einer Verkehrskontrolle – als Treffer angezeigt und somit weiterhin mit einem Delikt in Verbindung gebracht werden, von dem bereits festgestellt wurde, dass es nicht von diesen Personen begangen wurde. Wir haben dieser Behörde unsere Bedenken mitgeteilt. Eine Rückmeldung über die künftige Verfahrensweise steht noch aus.

Die zweite von uns kontaktierte Staatsanwaltschaft verweigert uns zumindest bis zum Ende des Berichtszeitraums eine Übersendung der angeforderten Akten – mit der Behauptung, uns fehle eine diesbezügliche Kontrollkompetenz. Die LDI NRW geht derzeit gegen die Verweigerung der Aktenherausgabe vor und wird ihre Prüfung danach weiter fortsetzen.

Die Verfahrensrückmeldungen von Staatsanwaltschaften an Polizeibehörden sind wichtig, um die polizeilichen Datenbestände zu aktualisieren bzw. zu korrigieren. Die Stichprobenkontrolle hat die aus unserer Beratungspraxis bekannten Defizite zum Teil bestätigt. Wir werden daher derartige Prüfungen fortsetzen und so auf einen durchgehend ordnungsgemäßen Umgang mit Verfahrensrückmeldungen in Strafverfahren sowie auf eine entsprechende Sensibilisierung der beteiligten Behörden hinwirken.

## 6.6 Unberechtigte Abrufe von Grundbuchauszügen durch Rechtsanwält*innen zahlen sich nicht aus

**Wenn Rechtsanwält*innen Grundbuchauszüge im automatisierten Verfahren beim Grundbuchamt elektronisch abrufen, kann dies nur unter bestimmten Voraussetzungen (Vorliegen und Angabe besonderer Abrufgründe) erfolgen. Werden hier Abrufgründe angegeben, die tatsächlich nicht vorliegen, stellt dies einen erheblichen Missbrauch des Zugangs zu Grundbuchinformationen dar, der sanktioniert wird.**

Ein Rechtsanwalt wollte einer nicht zum automatisierten Abrufverfahren zugelassenen Rechtsanwaltskollegin bei der Bearbeitung ihres Mandats helfen. Er rief unter seinem Namen für fremde Zwecke eines Mandates der Kollegin im automatisierten Verfahren Grundbuchauszüge ab. Hintergrund war ein Gerichtsverfahren wegen streitiger Wegerechte, in dem die Rechtsanwältin den Gegner der betroffenen Grundstückseigentümer*innen vertrat. Die Grundbuchauszüge wurden nach dem Abruf von dem Kollegen an die Rechtsanwältin übermittelt, die diese im Rahmen

ihres Mandats dann in das Gerichtsverfahren einbrachte.

Grundbuchauszüge sind in der Rechtsberatung oftmals ein relevantes Nachweisdokument mit wichtigen Informationen zum Grundstück. Für die Einsichtnahme ist dem Grundbuchamt deshalb ein berechtigtes Interesse (§ 12 Abs. 1 Satz 1 Grundbuchordnung - GBO) nachzuweisen. Das automatisierte Abrufverfahren nach §§ 133 ff. GBO ermöglicht zugelassenen Teilnehmer*innen die unmittelbare Online-Einsicht in das elektronische Grundbuch. Die Nutzung ist nur für hierfür zugelassene Verfahrensteilnehmer*innen erlaubt. Zusätzlich muss ein besonderes Interesse am elektronischen Abruf vorliegen, wie zum Beispiel eine Vielzahl von Datenabfragen oder Eilbedürftigkeit. Die Einhaltung der Grundsätze einer ordnungsgemäßen Datenverarbeitung muss von den Verfahrensteilnehmer*innen vor ihrer Zulassung zugesichert werden.

Nutzungsberechtigt sind u. a. Rechtsanwält*innen, die die Grundbuchdaten für eigene Zwecke verarbeiten. Die Teilnahme am automatisierten Abrufverfahren ist für sie allerdings eingeschränkt. Vor der jeweiligen Recherche müssen Rechtsanwält*innen den Grund des berechtigten Interesses an dem automatisierten Abruf durch Auswahl einer der in § 133 Abs. 4 GBO genannten Gründe darlegen (sog. Darlegungserklärung). Die Nutzung des Abrufverfahrens ist danach für Maßnahmen der Zwangsvollstreckung, bei dinglicher Berechtigung am Grundstück sowie beim Vorliegen einer Vollmacht der Eigentümer*innen zulässig.

Die abrufende Person oder Stelle muss das Vorliegen der zum Abruf berechtigenden Umstände durch Verwendung elektronischer Zeichen versichern und im

Falle einer Stichprobenkontrolle durch Vorlage entsprechender Nachweise (schriftliche Eigentümerzustimmung, Kopie des zur Zwangsvollstreckung geeigneten Titels) belegen.

In dem uns zur Kenntnis gebrachten Fall hatte der Anwalt, der zum Online-Abruf aus dem Grundbuch zugelassen war, kein eigenes berechtigtes Interesse an dem Abruf. Der Fall wurde an die Zentrale Bußgeldstelle der LDI abgegeben. Das Verfahren dort ist noch nicht abgeschlossen

Grundbuchauszüge beinhalten personenbezogene Daten von Grundstückseigentümer*innen. Für die Einrichtung des automatisierten Abrufverfahrens durch Rechtsanwält*innen muss sichergestellt sein, dass das Grundbuch nur in dem Umfang elektronisch eingesehen werden kann, den die Grundbuchordnung zulässt. Die zugelassenen Verfahrensteilnehmer*innen müssen das Vorliegen der besonderen Abrufgründe im Hinblick auf die schutzwürdigen Belange der betroffenen Personen prüfen und dokumentieren.

# 7. Gesundheit und Soziales

## 7.1 Datenschutz in Corona-Testzentren

**Während der Corona-Pandemie wurde innerhalb kürzester Zeit eine Vielzahl von Testzentren eingerichtet. Die Einhaltung datenschutzrechtlicher Vorgaben blieb dabei häufig auf der Strecke.**

Zur Pandemiebekämpfung wurden zahlreiche Testzentren eingerichtet, um flächendeckend mit Schnelltests das Vorliegen von Sars-Cov2-Infektionen festzustellen. Leider haben viele Betreiber*innen von Testzentren den Datenschutz vernachlässigt.

Teilweise wurden bereits bei der Terminvereinbarung Daten erhoben, die für die Durchführung der Testung nicht erforderlich waren. Erforderlich für die Ausstellung eines Zertifikates über einen Schnelltest sind Name, Anschrift, Geburtsdatum, nähere Angaben zum Testverfahren und zum Ergebnis der Testung, vgl. § 5 Abs. 5 Coronateststrukturverordnung (CoronaTeststrukturVO) in Verbindung mit Anlage 2 zur CoronaTeststrukturVO. Weitere Angaben sind zumeist nur für bestimmte Zwecke erforderlich und dürfen – falls keine gesetzliche Vorgabe vorliegt – nur auf freiwilliger Basis erhoben werden. Dies gilt zum Beispiel für Personalausweisnummern, die nur für die Einreise in bestimmte Länder benötigt werden.

Zudem wurden Betroffenen oft keine hinreichenden Datenschutzinformationen nach Art. 13 DS-GVO mitgeteilt. Hierzu gehören unter anderem der Name des Verantwortlichen, die Zwecke der Datenverarbeitung sowie die Speicherdauer. Dies gilt auch für Online-Terminvereinbarungen, bei denen personenbezogene Daten erhoben werden. Das heißt, Informationen zur

Datenverarbeitung müssen spätestens im Zeitpunkt der Buchung eines Termins zur Verfügung gestellt werden. Dies wurde von den Betreiber*innen der Testzentren häufig nicht hinreichend umgesetzt.

Schließlich bestand oftmals Unklarheit über die Voraussetzungen der Löschung von personenbezogenen Daten im Zusammenhang mit einer Testung. Sowohl den Betreiber*innen als auch den Nutzer*innen der Testzentren war teilweise nicht bekannt, dass sofortigen Löschungsverlangen gesetzliche Aufbewahrungspflichten der Testzentren nach § 5 Abs. 5 CoronateststrukturVO sowie § 7 Abs. 5 Coronavirus-Testverordnung (TestV) entgegenstehen. Nach § 7 Abs. 5 TestV sind die Auftrags- und Leistungsdokumentationen bis zum 31. Dezember 2024 unverändert zu speichern.

Die Betreiber*innen von Teststellen müssen bei der Verarbeitung personenbezogener Daten im Rahmen der Testung den Datenschutz konsequent umsetzen, denn sie arbeiten unter anderem mit besonders schützenswerten Gesundheitsdaten.

## 7.2 Veröffentlichungen zur Corona-Pandemie

**Städte und Gemeinden veröffentlichen seit Beginn der Corona-Pandemie diverse Informationen zur aktuellen Lage in ihren Gemeindegebieten. Hierbei ist darauf zu achten, dass kein Personenbezug hergestellt werden kann.**

Im Rahmen ihrer Öffentlichkeitsarbeit informieren Städte und Gemeinden über die aktuelle Corona-Situation vor Ort. Hierzu veröffentlichen sie unter ande-

rem aktuelle Zahlen zur Anzahl von Corona-Infizierten, Quarantänemaßnahmen und Belegungen in Intensivstationen. So lange diese Angaben keinen Rückschluss auf einzelne Personen zulassen, ist dies datenschutzrechtlich unproblematisch. Die DS-GVO ist lediglich für die Verarbeitung von personenbezogenen Daten anwendbar, also solchen Informationen, die sich auf eine identifizierbare natürliche Person beziehen. Demzufolge sind zum Beispiel Angaben, dass einige Lehrer*innen einer bestimmten Schule mit Corona infiziert sind, mangels Individualisierbarkeit möglich. Anders stellt es sich dar, wenn eine Personengruppe so eng gefasst wird, dass anhand einzelner Merkmale Rückschlüsse auf bestimmte Personen möglich sind. Gerade in sehr kleinen Gemeinden mit geringen Einwohnerzahlen kann etwa die Angabe, dass eine 96-jährige Person wegen einer Corona-Infektion auf der Intensivstation liegt, zu einer Identifikation führen. Die Offenlegung dieses Gesundheitsdatums ist für die Erfüllung des kommunalen Informationsauftrages in der Regel nicht erforderlich.

Städte und Gemeinden haben im Rahmen ihrer Öffentlichkeitsarbeit genau zu prüfen, ob die Kriterien für die Angabe ihrer Fallzahlen Rückschlüsse auf einzelne Personen zulassen. Wenn dies der Fall ist, sollte von einer Veröffentlichung abgesehen werden, es sei denn, der kommunale Informationsauftrag kann die Veröffentlichung im Einzelfall rechtfertigen.

## 7.3 Übermittlung von Jugendamtsakten an den Petitionsausschuss

**Die Übermittlung von Sozialdaten an den Petitionsausschuss des Landtags NRW ist auf Grundlage sozialdatenschutzrechtlicher Vorschriften und unter Beachtung der besonderen Regelungen zur Kinder- und Jugendhilfe im achten Sozialgesetzbuch (SGB VIII) grundsätzlich zulässig.**

Sozialdaten dürfen nur unter Wahrung des Sozialgeheimnisses verarbeitet werden. Das heißt, dass jede Person Anspruch darauf hat, dass die sie betreffenden Sozialdaten gemäß § 67 Abs. 1 SGB X von Leistungsträgern nicht unbefugt erhoben, verarbeitet oder genutzt werden. Nach § 69 Abs. 5 SGB X in Verbindung mit § 67c Abs. 3 SGB X ist eine Übermittlung zulässig, wenn sie für die Wahrnehmung von Aufsichts- und Kontrollbefugnissen über die verantwortliche Stelle erforderlich ist. Hierzu zählt auch die Kontrolltätigkeit des Petitionsausschusses. Nach Art. 41a Abs. 2 der Verfassung für das Land Nordrhein-Westfalen sind die Landesregierung und die Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie Behörden und sonstige Verwaltungseinrichtungen, soweit sie unter der Aufsicht des Landes stehen, verpflichtet, dem Petitionsausschuss auf sein Verlangen alle erforderlichen Auskünfte zu erteilen und Akten zugängig zu machen.

Das Jugendamt hat dazu alle Sozialdaten darauf hin zu prüfen, ob diese zur Aufgabenerfüllung mit Blick auf den Anforderungsgrund des Petitionsausschusses erforderlich sind. Hinzu kommt, dass zusätzlich stets zu prüfen ist, ob eine besondere Übermittlungsschranke greift, wie zum Beispiel §§ 64 Abs. 2, 65

SGB VIII für den Bereich der Jugendhilfe. Durch diese Schranke werden Sozialdaten von einer Übermittlung ausgenommen, die Mitarbeiter*innen eines Trägers der öffentlichen Jugendhilfe zum Zwecke persönlicher und erzieherischer Hilfe anvertraut worden sind. Das Jugendamt hat daher vor Weitergabe personenbezogener Sozialdaten aus Jugendamtsakten auch die besondere Schranke des § 65 SGB VIII eigenverantwortlich und konkret zu prüfen und die dieser Schranke unterfallenden Informationen ggf. unkenntlich zu machen. Andere für den Untersuchungsgegenstand relevante Daten bzw. Teile der Akten sind – wenn und weil nicht anvertraut – von dieser Schranke grundsätzlich nicht betroffen.

Die Verantwortung für die Zulässigkeit der Bekanntgabe von Sozialdaten durch ihre Weitergabe an den Petitionsausschuss liegt beim Jugendamt (§ 67d Abs. 1 Satz 1 SGB X). Dies umfasst auch die Prüfungskompetenz hinsichtlich der besonderen Schranke des § 65 SGB VIII. Diese Prüfung kann an den Petitionsausschuss nicht delegiert werden. § 65 SGB VIII ist insoweit eine besondere Schranke, die auch hinsichtlich der Aufgaben eines Petitionsausschusses oder anderer Aufsichtsbehörden greift.

## 7.4 Nachweise zum Gesundheitsschutz in Kindertageseinrichtungen

**Bei der Aufnahme eines Kindes in eine Kindertageseinrichtung haben die Sorgeberechtigten bestimmte Nachweise zum Masernschutz und zu Vorsorgeuntersuchungen des Kindes vorzulegen. Bei Einrichtungsleitungen ebenso wie bei den Eltern besteht Unsicherheit darüber, wie mit diesen Informationen umzugehen ist.**

Datenschutzbewusste Eltern wendeten sich an uns, weil sie verunsichert waren, ob Leitungen von Kindertageseinrichtungen berechtigt sind, Kopien der vorzulegenden Nachweise anzufertigen und diese für die Dauer des Betreuungsverhältnisses aufzubewahren. Die klare Antwort ist, dass Kopien nicht gefertigt und aufbewahrt werden dürfen. Es reicht aus, dass die Einrichtung sich die Dokumente vorlegen lässt und das Datum der Vorlage notiert. Eine Aufbewahrung von Kopien ist nicht erforderlich und auch gesetzlich nicht vorgesehen.

Zur Gesundheitsvorsorge in Kindertageseinrichtungen ist in § 12 Abs. 1 Kinderbildungsgesetz (KiBiz) geregelt, dass bei der Aufnahme in die Tageseinrichtung ein Nachweis über eine altersentsprechend durchgeführte Gesundheitsuntersuchung des Kindes zu erbringen ist. Das Gesetz sieht vor, dass dies durch Vorlage des Kinderuntersuchungsheftes oder einer entsprechenden ärztlichen Bescheinigung erfolgt. Zum Kinderuntersuchungsheft gehört eine sog. Teilnahmekarte. Auf dieser wird ärztlich bescheinigt, dass das Kind an der jeweiligen Vorsorgeuntersuchung teilgenommen hat. Anders als im Innenteil des

Untersuchungsheftes finden sich auf der Teilnahmekarte keine Angaben zum Gesundheitszustand des Kindes. Die Teilnahmekarte trägt dem Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 Buchstabe c DS-GVO Rechnung und ist ausreichend, um den nach § 12 Abs. 1 KiBiz geforderten Nachweis gegenüber der Kindertageseinrichtung zu erbringen.

Zur Dokumentation, dass die Eltern eines Kindes ihrer Vorlagepflicht nachgekommen sind, darf die Einrichtungsleitung vermerken, wann der Nachweis über die Gesundheitsuntersuchung oder bzw. und ein Impfnachweis vorgelegt wurden. Die Anfertigung einer Kopie des jeweiligen Nachweises ist hingegen nicht erforderlich und somit datenschutzrechtlich nicht zulässig.

# 8. Videoüberwachung

## 8.1 Gerichtsbeschlüsse zur Videoüberwachung durch Polizeibehörden

Das Verwaltungsgericht Köln hat in seinem nicht rechtskräftigen Beschluss (Beschluss vom 8. April 2021, Az. 20 L 2344/20) zwar den Antrag einer klagenden Person auf Erlass einer einstweiligen Verfügung abgelehnt, der das Verbot einer polizeilichen Videoüberwachung erreichen wollte. Dem Polizeipräsidium Köln hat das Gericht aber auferlegt, Eingänge zu Wohn- und Geschäftshäusern, den Eingang des Gesundheitsamtes und die Kennzeichen der den Videobereich befahrenden Fahrzeuge unkenntlich zu machen. Die Entscheidung des Gerichts spiegelt im Wesentlichen auch unsere seit längerem vertretene Auffassung wider.

In einem nicht rechtskräftigen Beschluss (Beschluss vom 18. Januar 2021, Az. 20 L 2340/19) hat das Verwaltungsgericht Köln dem Polizeipräsidium Köln im Wege der einstweiligen Anordnung zumindest bis zum Abschluss des Hauptsacheverfahrens die Videoüberwachung am Breslauer Platz untersagt. Dabei kommt das Gericht zu der Einschätzung, dass es sich beim Breslauer Platz nicht um eine Örtlichkeit im Sinne des § 15 a Abs. 1 Satz 1 Nr. 1 Polizeigesetz NRW, also nicht um einen Kriminalitätsschwerpunkt, handele.

## 8.2 Kfz-Kennzeichenüberwachung beim Parken

**Bereits im vorherigen Bericht haben wir datenschutzrechtliche Aspekte der Parkraumbewirtschaftung angesprochen. In diesem Bericht widmen wir uns nunmehr der Frage der Zulässigkeit der Kfz-Kennzeichenerfassung zur Erfassung der Parkdauer.**

Sowohl auf kostenlosen wie auch kostenpflichtigen Parkplätzen von Supermärkten, in Einkaufszentren und auch an Flughäfen werden immer öfter zur Parkraumbewirtschaftung Kfz-Kennzeichen durch Videotechnik erfasst. Hierdurch sollen Tickets bzw. Schranken abgelöst werden oder die zulässige maximale Parkdauer kontrolliert werden. Zwar ist das Parken vor Supermärkten oder Einkaufszentren nach wie vor oft kostenlos. Allerdings nur für einen bestimmten Zeitraum und nur zum Zwecke des Einkaufens. Darauf wird in Allgemeinen Geschäftsbedingungen (AGB) hingewiesen, die auf Schildern oder in Aushängen vor Ort bekannt gemacht werden. Bei Verstößen wird eine Vertragsstrafe gegenüber den Kfz-Halter*innen geltend gemacht. Auch bei generell kostenpflichtigen Parkflächen wird Kfz-Kennzeichenerfassung zunehmend beliebter, denn das Ein- und Ausfahren wird dadurch erheblich erleichtert. Die Parkraumbewirtschaftung wird oft nicht mehr durch die Eigentümer*innen der Parkflächen selbst durchgeführt, sondern privaten Dienstleister*innen übertragen. Diese können entweder als sog. Auftragsverarbeiter für die Besitzer*innen der Parkfläche als Verantwortliche tätig sein oder – wenn dem Dienstleistungsunternehmen die Aufgabe der Parkraumbewirtschaftung komplett übertragen wurde – selbst Verantwortliche nach Art. 4 Nr. 7 DS-GVO sein.

Die LDI NRW erhält viele Beschwerden zu dem Thema. Die Beschwerdeführer*innen (KfZ-Halter*innen oder Fahrer*innen) kritisieren die Erfassung der Kennzeichen insbesondere dann, wenn sie eine Zahlungsaufforderung erhalten haben. Die Fallgestaltungen weichen sowohl in praktischer wie technischer Hinsicht voneinander ab und müssen im Einzelfall von uns überprüft werden. Nachfolgend kann nur auf einige grundsätzliche Datenschutzanforderungen eingegangen werden. Zivilrechtliche Fragen bleiben dabei außer Betracht, etwa die Geltung der AGB; Vertragsstrafen und deren Geltendmachung oder die Beauftragung von Dienstleistungsunternehmen.

Kfz-Kennzeichen sind wegen der Möglichkeit der Halter*innenermittlung in aller Regel personenbeziehbare Daten. Für deren Verarbeitung muss eine Rechtsgrundlage nach Art. 6 Abs. 1 DS-GVO gegeben sein. Zumeist wird die Kennzeichenerfassung – insbesondere bei sog. Kurzparker*innen – auf Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO gestützt. Hiernach muss die Datenverarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich sein, sofern nicht die Interessen Betroffener am Schutz der eigenen personenbezogenen Daten überwiegen.

Als berechtigtes Interesse des datenschutzrechtlich Verantwortlichen ist beispielsweise die Inkassosicherheit anerkannt, also die Gewährleistung der reibungslosen Zahlung für den Parkvorgang. Die Kfz-Kennzeichenerfassung müsste zum Zweck der Inkassosicherheit „erforderlich“ sein. Dies ist nur dann der Fall, wenn belegbare Vorkommnisse in der Vergangenheit die Annahme rechtfertigen, dass auch künftig schwer-

wiegende Beeinträchtigungen der geschützten Interessen drohen. Die Erforderlichkeit des Einsatzes dieses Mittels ist zudem nur dann zu bejahen, wenn es hierfür kein anderes gleich wirksames Mittel gibt, das weniger stark in das Recht auf informationelle Selbstbestimmung der davon Betroffenen eingreift und objektiv zumutbar ist.

Verantwortliche haben daher vor dem Einsatz von Kennzeichenerfassungssystemen zunächst zu ermitteln und in ihrem Datenschutzkonzept substantiiert und nachvollziehbar darzulegen, ob und – wenn ja – in welcher Höhe in der Vergangenheit Einnahmeverluste durch das Erschleichen der Dienstleistung Parken auf der in Rede stehenden Fläche eingetreten sind. Sind derartige Schäden nachvollziehbar dargelegt, müssen diese im Verhältnis zum jeweiligen Gesamtumsatz der oder des Verantwortlichen eine nicht nur unerhebliche Höhe aufweisen.

Bei der Wahrung der Inkassosicherheit kann bei Ticketverlust nicht auf den Erwerb eines teureren Ersatztickets als milderes Mittel verwiesen werden. Neben dem Umstand des Verlusts sind auch Auswirkungen auf andere schutzwürdige Belange bzw. berechtigte Interessen des Verantwortlichen oder eines Dritten zu berücksichtigen. Beispielweise können die Ermittlung der exakten Parkdauer und die dadurch mögliche rechtssichere Erfassung und Abrechnung der konkreten Parkzeiten eine Verbesserung des Kundenservice darstellen. Für Kund*innen, die ein Ticket verlieren, wäre eine erhöhte Ticketpauschale außerdem ein nicht gerechtfertigter Nachteil.

Im Rahmen der Interessenabwägung nach Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO kann insbesondere durch folgende technische und organisatorische

Anforderungen gewährleistet werden, dass die berechtigten Interessen des Verantwortlichen überwiegen:

- Die Daten dürfen nur für den angegebenen Zweck verwendet werden. Insbesondere darf eine Verknüpfung mit Halter*innendaten nur unter Einhaltung der Voraussetzungen des § 39 Straßenverkehrsgesetz stattfinden.

- Staatliche Stellen dürfen keinen Zugriff auf die Daten haben, wobei mögliche Zugriffsbefugnisse nach besonderen Gesetzen unberührt bleiben.

- Die Löschung der Daten muss sichergestellt sein und die Speicherdauer darf grundsätzlich nicht mehr als 72 Stunden betragen. Längere Speicherfristen können in Ausnahmefällen, etwa bei typischerweise längerfristigen Parkaufenthalten (zum Beispiel an Flughäfen) erforderlich sein. Die Erforderlichkeit ist hierbei im Einzelfall durch die Verantwortlichen zu begründen.

- Die IT-Sicherheit nach dem Stand der Technik muss gewährleistet sein und die Datenverarbeitung muss in einem geschlossenen System stattfinden. Die Verknüpfung der Daten mit anderen Systemen des Verantwortlichen muss ausgeschlossen sein.

- Die Aufnahmen müssen außerhalb des zur Kennzeichenerfassung erforderlichen Bildausschnitts so unscharf wie möglich sein, so dass die Identifikation von Personen ausgeschlossen ist.

- Hinweisschilder müssen frühzeitig, das heißt vor dem Einfahren in den von der Kamera erfassten Bereich, erkennbar sein, damit der Kunde die

Möglichkeit hat einen anderen Parkplatz zu suchen, wenn er eine Kennzeichenerfassung ablehnt. Hierbei kann es in Einzelfällen – wegen der tatsächlichen Gegebenheiten vor Ort – auch zulässig sein, dass das sofortige Löschen des Kennzeichens nach der Ausfahrt aus dem Parkhaus erfolgt. Empfohlen wird, sich bei der konkreten Ausgestaltung der Schilder an den Mustern der Orientierungshilfe Videoüberwachung durch nichtöffentliche Stellen zu orientieren; diese genügen den Anforderungen der Art. 12 ff. DS-GVO. Die Muster sind auf www.ldi.nrw.de abrufbar.

- Ferner sollte das Wort „Videoüberwachung“ durch „Kfz-Kennzeichenerfassung“ ersetzt werden. Piktogramme allein reichen nicht aus.

Bei nachvollziehbarer Begründung kann eine Kfz-Kennzeichenerfassung zur Parkraumbewirtschaftung im Interesse der Inkassosicherheit datenschutzrechtlich zulässig sein. Durch technisch-organisatorische Maßnahmen ist der Eingriff in die Datenschutzrechte Betroffener zu minimieren. Die hier genannten Anforderungen können als Orientierung für eine erste Einschätzung dienen.

# 9. Datenschutz am Arbeitsplatz

## 9.1 Weitergabe von Daten aus dem betrieblichen Eingliederungsmanagement an die Personalstelle und den Betriebsrat

**Das sog. Betriebliche Eingliederungsmanagement (BEM) wirft wichtige Fragen zur zulässigen Verwendung von (Gesundheits-) Daten der Beschäftigten auf. Dies zeigt ein aktueller Fall, der unter anderem zur Verhängung eines Bußgeldes führte.**

Arbeitgeber*innen sind gemäß § 167 Abs. 2 Neuntes Buch Sozialgesetzbuch (SGB IX) dazu verpflichtet, Beschäftigten, die innerhalb eines Jahres länger als sechs Wochen ununterbrochen oder wiederholt arbeitsunfähig sind, ein sog. Betriebliches Eingliederungsmanagement anzubieten. Ziel sind Wiederherstellung der Arbeitsfähigkeit und der Erhalt des Arbeitsplatzes. Die Teilnahme an diesem Verfahren ist für die betroffenen Beschäftigten freiwillig. Bei der Durchführung eines BEM-Verfahrens werden Gesundheitsdaten verarbeitet. Diese unterliegen als besondere Kategorien personenbezogener Daten nach Art. 9 DS-GVO einem besonderen Schutz. Sie dürfen nur einem eingeschränkten, am BEM-Verfahren beteiligten Personenkreis zugänglich gemacht und nicht in die Personalakte aufgenommen werden. Arbeitgeber*innen dürfen nicht auf die Inhalte der BEM-Akte zugreifen.

Der Betriebsrat eines Unternehmens teilte der LDI NRW in Abstimmung mit dessen Datenschutzbeauftragten mit, dass der Arbeitgeber in mehreren Fällen sensible Daten im Sinne des Art. 9 Abs. 1 DS-GVO aus BEM-Gesprächen an den Betriebsrat zur Unterrichtung nach § 80 Abs. 1 Betriebsverfassungsgesetz

(BetrVG) weitergegeben habe. Es handelte sich dabei um Mitteilungen über beabsichtige krankheitsbedingte Kündigungen von mehreren Beschäftigten zur Anhörung des Betriebsrats nach § 102 BetrVG. Darin habe der Arbeitgeber erstmals aus Protokollen zitiert, die im Zuge von Maßnahmen des BEM gemäß § 167 Abs. 2 SGB IX erstellt wurden. Diese Protokolle enthielten Angaben zu krankheitsbedingten Fehltagen, eine Fehlzeitenquote und in neun Einzelfällen Gesundheitsdaten aus dem BEM-Verfahren, zum Beispiel bezüglich psychischer Probleme, Magen- und Darmerkrankungen, Bandscheibenvorfällen und Rückenproblemen.

Das BEM-Verfahren wurde durch drei hierfür besonders geschulte Mitarbeiter*innen aus der Personalabteilung des Unternehmens durchgeführt. Die BEM-Akten wurden getrennt von den Personalakten aufbewahrt. Andere Mitarbeiter*innen und Führungskräfte der Personalabteilung erhielten allerdings Kenntnis von den Inhalten der BEM-Gespräche, soweit aufgrund ihrer konkreten Tätigkeit eine Notwendigkeit hierzu bestand.

Der Arbeitgeber war der Auffassung, zur Verarbeitung der BEM-Daten zur Erfüllung seiner arbeits- und sozialrechtlichen Verpflichtung (§ 26 Abs. 3 BDSG) sowie zur Unterrichtung des Betriebsrates im Verfahren zur betriebsbedingten Kündigung im Rahmen der Mitbestimmung berechtigt bzw. sogar verpflichtet gewesen zu sein. Den Datenschutzbeauftragten des Unternehmens hatte er in seine Entscheidung zur Verarbeitung und Weitergabe der Daten nicht eingebunden.

Die Prüfung ergab, dass der Arbeitgeber durch die Personalstelle neben den Sozialdaten der betroffenen

Beschäftigten Informationen zu krankheitsbedingten Fehlzeiten und auch den hierdurch verursachten Kosten sowie zur Prognose einer Erkrankung verarbeiten und an den Betriebsrat im Rahmen der Mitbestimmung weitergeben darf. Nicht weitergegeben werden dürfen jedoch weitergehende Angaben zur Gesundheit der Betroffenen.

Der Arbeitgeber wurde hierüber in Kenntnis gesetzt. Er schloss sich den getroffenen Feststellungen an und teilte mit, künftig Gesundheitsdaten von Beschäftigten nicht mehr zu verarbeiten und an den Betriebsrat weiterzugeben.

Zur Ahndung der erfolgten, nicht unerheblichen Datenverstöße wurde gegen den Arbeitgeber ein Bußgeld verhängt. Dabei wurde zu Gunsten des Arbeitgebers berücksichtigt, dass die Verarbeitung und die Weitergabe der Gesundheitsdaten der Betroffenen für diese keine negativen Folgen hatten.

Im Rahmen eines BEM-Verfahrens dürfen Gesundheitsdaten aus der BEM-Akte nicht in die Personalakten der betroffenen Beschäftigten übernommen werden. Sie müssen in einer separaten BEM-Akte räumlich und funktional getrennt von der Personalakte aufbewahrt werden. In die Personalakte dürfen nur solche Angaben aufgenommen werden, die zum Nachweis des ordnungsgemäßen BEM-Verfahrens erforderlich sind. Hierzu gehören Angaben, ob und wann die Durchführung eines BEM angeboten wurde, ob die betroffene Person hiermit einverstanden war oder das BEM abgelehnt hat und welche konkreten Maßnahmen angeboten und umgesetzt wurden.

Im BEM-Verfahren erhobene Gesundheitsdaten dürfen zudem nicht für andere Zwecke, beispielsweise zur Vorbereitung einer krankheitsbedingten Kündigung, genutzt und an den Betriebsrat weitergeben werden. Im Falle einer Kündigung darf zur Unterrichtung des Betriebsrats nach §§ 80 Abs. 1, 102 BetrVG nur der Nachweis erbracht werden, dass ein BEM-Verfahren den betroffenen Beschäftigten als milderes Mittel angeboten und ggf. auch durchgeführt wurde.

## 9.2 Angaben zu Abwesenheitsgründen in Dienstplänen

**In einer Rettungs- und Feuerwache hingen für alle Beschäftigten einsehbare Dienstpläne aus, aus denen auch krankheitsbedingte Abwesenheiten erkennbar waren; diese waren mit einem „K“ gekennzeichnet. Dagegen wandte sich ein Beschäftigter mit einer Datenschutzbeschwerde.**

Gemäß § 18 Abs. 1 Satz 1 DSG NRW dürfen personenbezogene Daten von Beschäftigten nur unter bestimmten Voraussetzungen verarbeitet werden, etwa wenn dies zur Durchführung des Beschäftigungsverhältnisses oder zum Zweck der Personalplanung und des Personaleinsatzes erforderlich ist. Für die Planung des Personaleinsatzes und zur Übersicht, welche Beschäftigten jeweils im Dienst sind, ist es jedoch nicht erforderlich, auch die Gründe für Abwesenheiten im Dienstplan zu erfassen. Allein die Information über tagesaktuelle An- und Abwesenheiten reicht aus, um die Personalplanung an diese anzupassen.

Wir haben die Dienststelle daher auf die fehlende Rechtsgrundlage für die von ihr vorgenommene Verarbeitung der Abwesenheitsgründe hingewiesen. Diese hat daraufhin die Dienstpläne in Zusammenarbeit mit dem Datenschutzbeauftragten geändert: Abwesenheiten werden nunmehr lediglich mit „A“ und ohne Angabe weiterer Gründe kenntlich gemacht. Zudem werden die Dienstpläne so aufbewahrt, dass sie nur noch von denjenigen einsehbar sind, die diese Informationen dienstlich benötigen.

Bei der Erstellung von Dienstplänen sind nur solche personenbezogenen Daten zu erfassen, die tatsächlich für die Planung des Personaleinsatzes erforderlich sind. Angaben zu konkreten Abwesenheitsgründen sind nicht erforderlich.

# 10. Wirtschaft

## 10.1 Datenschutzprüfung von Energieversorgungsunternehmen

**Schrittweise und branchenbezogen überprüfen wir die Umsetzung der DS-GVO in der Wirtschaft. Nach den Querschnittsprüfungen von Banken und Versicherungen, haben wir in 2021 die Prüfung von Energieversorgungsunternehmen abgeschlossen.**

Die Auswahl der überprüften Versorgungsunternehmen mit Sitz in Nordrhein-Westfalen erfolgte zufällig. Jedes ausgewählte Unternehmen erhielt einen umfassenden Fragebogen mit unterschiedlichen Fraggruppen. Der Fragenbogen ist im Anhang abgedruckt.

Bei einigen wenigen Unternehmen fiel das Ergebnis der Prüfung sehr erfreulich aus. Im Ergebnis konnten wir hier feststellen, dass der Datenschutz in der gesamten Organisation der jeweiligen Unternehmen verantwortungsvoll praktiziert wird. Datenschutzthemen werden in regelmäßigen Abständen und anlassbezogen zur Unternehmensleitung kommuniziert. Besonders positiv fiel auf, dass die Mitarbeiter*innen durch Schulungen, Informationsmaterial und digitale Konzepte für den Umgang mit personenbezogenen Daten gut sensibilisiert werden.

Aus dem positiven Gesamteindruck dieser Energieversorgungsunternehmen leiten wir folgende bereichsübergreifende „Best Practices“ ab:

- Statistik zu den Datenschutzbeschwerden und Analyse der Defizitschwerpunkte;

- besonders geschulte Teams für die Bearbeitung von Datenschutzansprüchen und -beschwerden;
- strukturiertes Schulungskonzept mit Pflichtschulungen zur DS-GVO für alle Mitarbeiter*innen mit zusätzlichen Wiederholungsschulungen im zweijährigen Rhythmus (teilweise als Webinare und elektronische Fortbildung);
- konzerninterne Kommunikationsplattform für Datenschutzfragen (Wiki) mit Zugriff auf datenschutzrelevante Fachinformationen;
- Checklisten zur Durchführung von Datenschutzchecks sowie Checklisten für Auftragsverarbeiter zur Dokumentation der dortigen technischen und organisatorischen Maßnahmen;
- Angebot eines konzerninternen Newsletters zum Datenschutz.

Bei den übrigen Energieversorgern ließen Inhalt und Umfang der Antworten leider erkennen: Datenschutz wird von den Unternehmen eher als lästige Nebenpflicht angesehen. Einige Unternehmen waren nicht in der Lage, die wesentlichen unternehmensspezifischen Datenverarbeitungen transparent darzustellen. Teilweise wurde ausschließlich auf den Abschluss von Auftragsverarbeitungsverträgen verwiesen ohne sich der eigenen Verantwortlichkeit bewusst zu sein. Sicherheitsrichtlinien, Sicherheitskonzepte, Verträge z. B. zur Auftragsverarbeitung, Löschkonzepte sowie ein umfassendes Beschwerdemanagement wurden unzureichend dokumentiert. Aufgrund der gravierenden Mängel sah sich die LDI NRW daher gezwungen, umfassende Unterlagen nachzufordern, gezielte Fra-

gen an die Geschäftsführungen zu richten sowie umfangreiche datenschutzrechtliche Hinweise nach Art. 58 Abs. 1 Buchstabe d DS-GVO zu erteilen. Hier fehlt offenbar die Erkenntnis, dass Datenschutzverletzungen teuer werden und zu Reputationseinbußen führen können. Diese Unternehmen werden wir daher weiter gezielt im Auge behalten.

Im Rahmen der Querschnittsprüfung ergaben sich bei keinem der geprüften Unternehmen Hinweise darauf, dass Informationssysteme geführt werden, die personenbezogene Hinweise enthalten, wie etwa zum Wechselverhalten von Kund*innen („Bonushopping“). Auch ein Abgleich von personenbezogenen Daten mit anderen Energieversorgungsunternehmen konnte nicht festgestellt werden.

Bei den Energieversorgungsunternehmen gab es einige Datenschutzleuchttürme, aber leider auch solche, die den Datenschutz vernachlässigen. Diese müssen insbesondere in den Bereichen Management der Betroffenenrechte, Schulungen von Mitarbeiter*innen, Outsourcen von Datenschutzaufgaben an externe Dienstleister*innen mehr tun und sich ihrer datenschutzrechtlichen Verantwortung bewusst sein. Hier besteht Optimierungsbedarf. Wir bleiben dran!

## 10.2 Kein Datenschutzverstoß bei Rückzahlung der NRW-Corona-Soforthilfe 2020

**Annähernd 190 Betroffene wandten sich an uns mit der Befürchtung, die Entscheidung über die Rückzahlung von Corona-Hilfen erfolge automatisiert und damit datenschutzwidrig.**

Die Betroffenen trugen vor, dass im Rahmen des Rückmeldeverfahrens zur Corona-Soforthilfe 2020 die Entscheidung über die Höhe der Rückzahlungen möglicherweise automatisiert erfolge, und vermuteten deshalb einen Datenschutzverstoß. Da automatisierte Entscheidungen im Einzelfall ohne Einschaltung von Sachbearbeitungen nach Art. 22 DS-GVO nicht erlaubt sind, war der Förderprozess insoweit zu überprüfen.

Im Ergebnis traf zwar zu, dass die konkrete Berechnung des Schlussbescheides automatisiert erfolgte, nachdem die Antragstellenden die Daten zur Berechnung des Liquiditätsengpasses selbst eingegeben hatten. Die Entscheidung im Schlussbescheid kann aber nicht isoliert von dem Ausgangsbescheid zur vorläufigen Gewährung der Soforthilfe 2020 gesehen werden. Dieser Bescheid, durch den der Höchstbetrag zur Verfügung gestellt wurde, wurde von einzelnen Sachbearbeiter*innen veranlasst. Auf dieser Grundlage und unter Eingabe der persönlichen Daten zur Ermittlung ihres Liquiditätsengpasses wurde dann der Schlussbescheid erstellt. Dieser ist im Zusammenhang mit dem Ausgangsbescheid zu sehen, bei dessen Erlass Sachbearbeiter*innen mitgewirkt hatten. Ein Verstoß gegen Art. 22 DS-GVO ist nicht gegeben.

Durch unsere Prüfung konnten wir ein Missverständnis aufklären und die Befürchtungen der Empfänger*innen der Coronahilfen entkräften.

## 10.3 Standardvertragsklauseln für Verantwortliche und Auftragsverarbeiter

**Von der EU-Kommission festgelegte Muster-Vertragsklauseln helfen dabei, Auftragsverarbeitungsverträge rechtssicher zu gestalten.**

Seit Inkrafttreten der DS-GVO haben sich zahlreiche Fragen zur Auftragsverarbeitung ergeben. Um ein europaweit einheitliches Verständnis dieses Rechtsinstituts sicherzustellen, hat der Europäische Datenschutzausschuss (EDSA) Leitlinien erarbeitet. Die finale Fassung dieser „Guidelines 07/2020 on the concepts of controller and processor in the GDPR“ (Version 2.0 vom 07. Juli 2021) ist unter www.edpb.europa.eu abrufbar.

Ein weiteres Instrument, um die einheitliche und richtige Anwendung von Art. 28 DS-GVO zu gewährleisten, sind die von der EU-Kommission im Juni 2021 veröffentlichten Standardvertragsklauseln. Hierbei handelt es sich um standardisierte und vorformulierte Musterklauseln, die auf freiwilliger Basis in vertragliche Vereinbarungen aufgenommen werden können. Die EU-Kommission hat gemäß Art. 28 Abs. 8 DS-GVO von ihrem Recht Gebrauch gemacht, europaweit einheitliche Mustervertragsklauseln festzulegen, die die inhaltlichen Anforderungen des Art. 28 Abs. 3 und 4 DS-GVO an Auftragsverarbeitungsverträge präzisieren. Die Verwendung abgestimmter Vertragsklauseln erleichtert die Handhabung für die Vertragsparteien und hilft ihnen, ihren jeweiligen datenschutzrechtlichen Pflichten nachzukommen. Der Abschluss individuell ausgehandelter Verträge ist Verantwortlichen und Auftragsverarbeitern weiterhin unbenom-

men. Gleichwohl kann sich durch eine vollständige oder teilweise Verwendung der Musterklauseln der (Kosten-)Aufwand der Beteiligten für die Vertragserstellung verringern.

Bei der Formulierung ihrer Standardvertragsklauseln hat die EU-Kommission sowohl die im Rahmen einer öffentlichen Konsultation geäußerten Belange von Interessenvertreter*innen als auch die gemeinsame Stellungnahme des EDSA und des Europäischen Datenschutzbeauftragten berücksichtigt. An der Erarbeitung der Stellungnahme im EDSA haben auch wir gemeinsam mit anderen nationalen Aufsichtsbehörden mitgewirkt.

Die Standardvertragsklauseln zur Verwendung zwischen Verantwortlichen und Auftragsverarbeitern sind – auch in deutscher Sprache – unter www.eur-lex.europa.eu abrufbar.

Gleiches gilt für die weiteren Standardvertragsklauseln, die die EU-Kommission speziell für internationale Datentransfers festgelegt hat. Siehe hierzu unter 3.

Die EU-weit geltenden Standardvertragsklauseln erleichtern nicht nur den Beteiligten die Gestaltung ihrer Verträge gemäß Art. 28 Abs. 3 und 4 DS-GVO, sondern gewährleisten auch eine weitere Harmonisierung und mehr Rechtssicherheit bei der Auftragsverarbeitung.

## 10.4 Zertifizierung – ein langer Weg für guten Datenschutz

**Auch fast vier Jahre nach Inkrafttreten der DS-GVO gibt es in Deutschland noch keine akkreditierten Zertifizierungsstellen. Mit ihren einheitlichen Anforderungen an Zertifizierungkriterien will die Datenschutzkonferenz das Erstellen von Zertifizierungsprogrammen erleichtern.**

Art. 42 und 43 DS-GVO legen die Grundsteine für einheitliche europäische Akkreditierungs- und Zertifizierungsverfahren. Zertifizierungsstellen, die nach der DS-GVO tätig werden wollen, müssen sich zunächst für diese Tätigkeit akkreditieren lassen. Für diese Akkreditierung muss eine Prüfung durchlaufen werden, die in mehreren Schritten stattfindet. Die Deutsche Akkreditierungsstelle und die jeweils zuständige Datenschutzbehörde arbeiten dabei zusammen.

Zu den ersten Schritten gehört die Fachprüfung des Konformitätsbewertungsprogramms und der entsprechenden Zertifizierungskriterien durch die zuständige Aufsichtsbehörde anhand der ISO/IEC 17065 und der ergänzenden Anforderungen. Erfolgreich abgeschlossen wird die Fachprüfung der Aufsichtsbehörde mit der Genehmigung der Zertifizierungskriterien.

Die deutschen Aufsichtsbehörden, die sich in der Datenschutzkonferenz abstimmen, haben einheitliche Anforderungen an Zertifizierungskriterien aufgestellt. Die Anwendungshinweise sind auf der Homepage der DSK www.datenschutzkonferenz-online.de abrufbar.

Wir bewerten Zertifizierungsprogramme auf der Basis dieser Anforderungen. Programmeigner sowie die zu akkreditierenden Zertifizierungsstellen können sich

schon bei der Erstellung ihrer Dokumente hieran orientieren. Erfahrungen und Erkenntnisse der Aufsichtsbehörden fließen auch weiterhin in die Anforderungen ein, die bei Bedarf angepasst werden.

Die LDI NRW hat in zwei Fällen bereits eingereichte Kriterien als für grundsätzlich genehmigungsfähig bewertet – vorbehaltlich der Stellungnahme durch den EDSA. Weitere Anträge liegen vor. Vorbehaltlich des weiteren Akkreditierungsprozesses werden demnächst erste Zertifizierungsstellen in Deutschland datenschutzrechtliche Zertifizierungen nach der DS-GVO anbieten können.

Erfolgreiche Zertifizierungen sollen die Einhaltung der DS-GVO bei Verarbeitungsvorgängen nachweisen. Das kann die Glaubwürdigkeit und seriöse Geschäftsführung von Unternehmen stärken und damit einen Marketingvorteil erzeugen. Die Verfahren bedeuten auch mehr Transparenz für alle, deren Daten verarbeitet werden. Eine erfolgreiche Zertifizierung garantiert zwar nicht, dass jede einzelne Verarbeitung DS-GVO-konform ist. Sie schafft aber ein Umfeld, dass Datenschutzkonformität fördert. Ein nach der DS-GVO erteiltes Zertifikat kann außerdem bei aufsichtsbehördlichen Kontrollen von Vorteil sein und die Prüfung erleichtern.

Das Papier „Anforderungen an datenschutzrechtliche Zertifizierungsprogramme“ ist eine Praxishilfe bei der Erstellung eines Zertifizierungsprogramms und zeigt Interessierten, worauf es bei der aufsichtsbehördlichen Überprüfung ankommt. Es soll Datenschutzzertifizierungen in Deutschland voranbringen.

## 10.5 Fotos in Immobilienanzeigen

**Die Veröffentlichung von Fotos oder 360-Grad-Rundumsichten von vermieteten Wohnräumen im Internet auf Immobilienportalen oder Webseiten von Wohnungs- und Makler*innenunternehmen bei Verkauf oder Neuvermietung führt immer wieder zu Beschwerden von betroffenen Mieter*innen. Die LDI NRW hat in zahlreichen Fällen erfolgreich darauf hingewirkt, dass Makler*innen- und Wohnungsunternehmen hier sensibel verfahren.**

Viele Mieter*innen sind überrascht und verärgert, wenn Fotos ihrer eingerichteten Wohnung im Internet auf Immobilienportalen oder in Exposés von Maklerunternehmen veröffentlicht werden. Auf den Fotos sind teilweise auch persönliche Gegenstände und Familienfotos oder Personenporträts zu sehen. Auch Personen, deren Immobilie an das zu verkaufende oder vermietende Objekt angrenzt, beschweren sich, weil auf den veröffentlichten Bildern Menschen oder deren persönliche Wertgegenstände wie hochwertige Kunstskulpturen oder Fahrzeuge – teilweise mit erkennbarem Kfz-Kennzeichen – zu sehen sind.

Wir weisen die Unternehmen in diesen Fällen darauf hin, dass bei Fotos oder 360-Grad-Rundumsichten von vermieteten Immobilien, die zur Vermarktung im Internet oder in Exposés verwendet werden sollen, ein Personenbezug vermieden werden muss. Zumindest sind personenbezogene Details zu verpixeln. Dies sollten Verantwortliche bereits bei der Herstellung der Fotos beachten, denn Neuaufnahmen sind zeitaufwändig.

Mit unserer Beratung stoßen wir zumeist auf Einsicht, so dass die Unternehmen unseren Empfehlungen folgen.

Wohnungen und das Wohnumfeld zählen zum höchstpersönlichen Schutzbereich. Personenbezüge sollten bereits bei der Anfertigung von Fotos und 360-Grad-Rundumsichten für Immobilienanzeigen vermieden werden.

## 10.6 Weitergabe von Daten einer Wohnungseigentümergemeinschaft an außenstehende Dritte

**Eine Wohnungseigentümergemeinschaft (WEG) ist eine besonders schutzwürdige Vertrauensgemeinschaft. Für die Weitergabe von Daten der Miteigentümer*innen an außenstehende Dritte ist das bei der Interessenabwägung zu berücksichtigen.**

Mehrere Mitglieder einer WEG erhielten von einem Makler eine Verkaufsanfrage für ihre Wohnungen. Ein anderer Miteigentümer der WEG hatte den Makler dazu beauftragt. Die Adressdaten der Miteigentümer*innen hatte der Eigentümer aus der WEG-Liste von der Hausverwaltung erhalten und diese dann an den Makler weitergegeben. Sämtliche Miteigentümer*innen wurden von ihm angeschrieben und nach einer Verkaufsabsicht gefragt. Eine Miteigentümerin fühlte sich dadurch belästigt und beschwerte sich bei der LDI.

Nicht zu beanstanden ist die Herausgabe der Eigentümerliste an die Mitglieder einer WEG durch die Hausverwaltung, weil Miteigentümer*innen einen Anspruch darauf haben zu wissen, wer zur WEG gehört.

Auch ein werbendes Anschreiben einer Makler*innenfirma an sich ist nicht zu beanstanden. Mit postalischer Werbung ist auch außerhalb einer Kundenbeziehung grundsätzlich zu rechnen.

Die Weitergabe der Daten der Miteigentümer*innen an die Makler*innenfirma ist jedoch eine unzulässige Datenverarbeitung. Bei einer Weitergabe dürfte gemäß Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO einem berechtigten Interesse der Miteigentümer*innen keine überwiegende Rechtsposition der Betroffenen gegenüberstehen. Zwar hatte der ankaufsinteressierte Miteigentümer hier ein berechtigtes wirtschaftliches Interesse am Ankauf weiterer Wohnungen. Jedoch handelt es sich bei einer WEG um eine Art „Vertrauensgemeinschaft“: Andere Miteigentümer*innen müssen grundsätzlich nicht damit rechnen, dass etwa ihre Adressdaten oder Informationen über ihre Eigentümer*instellung an Außenstehende weitergegeben werden. Sie sind deshalb in dieser Hinsicht schutzwürdig. Auch hätten dem ankaufsinteressierten Miteigentümer andere, datensparsamere Möglichkeiten zur Verfügung gestanden, um seine Anfrage an die WEG-Mitglieder zu richten, beispielsweise per Aushang oder mündliche Information in der WEG-Versammlung. Das Interesse der betroffenen Miteigentümer*innen überwiegt hier. Die LDI hat auf den Datenschutzverstoß hingewiesen und empfohlen, in der nächsten WEG-Versammlung die postalischen Verkaufsanfragen zu thematisieren und ggfs. einen gemeinsamen Beschluss über ein für alle Seiten akzeptables Vorgehen zu fassen.

Miteigentümer*innen einer WEG haben ein überwiegendes Interesse daran, dass ihre Daten nicht an Außenstehende weitergeben werden (Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO). Datenübermittlungen an Dritte zur Abfrage von Verkaufsabsichten sind nicht zulässig. Die Verkaufsabsicht ist daher auf anderen Wegen zu erfragen.

## 10.7 Nutzung von E-Mail-Adressen zu Werbezwecken

**Werbemails werden meist auf eine elektronische Einwilligung mittels des sog. Double-Opt-In-Verfahrens gestützt. Betroffene bestreiten oft, solche Einwilligungen abgegeben zu haben oder können sich daran nicht mehr erinnern.**

Auf E-Mail-Werbung spezialisierte Unternehmen erwerben oder mieten von Adresshändler*innen E-Mail-Adresslisten. Diese Adressbestände nutzen sie dann für E-Mail-Werbekampagnen für Produkte anderer Unternehmen. Die LDI erreichen sehr viele Beschwerden über derartige Werbemails, weil die Betroffenen nach eigener Aussage keinerlei Beziehung zu den werbenden Unternehmen hatten und sich nicht vorstellen können, wieso dort die Mailadresse bekannt ist.

E-Mail-Adressen sind personenbezogene oder zumindest personenbeziehbare Daten. Sie dürfen zur Direktwerbung nur genutzt werden, wenn dafür eine Rechtsgrundlage nach Art. 6 Abs. 1 DS-GVO gegeben ist. Dabei sind auch die Regelungen des Gesetzes gegen den unlauteren Wettbewerb (UWG) beachtlich. Unerwünschte E-Mail-Werbung bei Verbraucher*innen stellt eine unzumutbare Belästigung im

Sinne des § 7 Abs. 2 Nr. 3 UWG dar. Die sog. „Händlerprivilegierung“ nach § 7 Abs. 3 UWG als Ergebnis einer Interessenabwägung nach Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO liegt nur vor, wenn eine Geschäftsbeziehung zwischen Werbenden und Betroffenen besteht. Dies ist bei den vorliegenden Beschwerden gerade nicht der Fall.

Meist berufen sich die werbetreibenden Unternehmen als datenschutzrechtlich Verantwortliche darauf, dass ihnen eine Einwilligung nach Art. 6 Abs. 1 Satz 1 Buchstabe a DS-GVO vorliege. Bei dem Double-Opt-In-Verfahren bestätigt der Einwilligende in einer gesonderten Mail an ihn durch Anklicken eines Links seine Einwilligung. Als angebliche Nachweise legen sie jeweils eine IP-Adresse mit Zeitstempel vor (auch für das Double Opt-In); dies sehen sie als ausreichend an. Manche dieser Nachweise sind mehrere Jahre alt oder können nicht zurückverfolgt werden, da zum Beispiel die Unternehmen, die diese IP-Adresse ursprünglich erhoben haben sollen, nicht mehr bestehen.

Verantwortliche haben nach Art. 5 Abs. 1 und 2 DS-GVO zudem die Einhaltung wesentlicher Grundsätze für die Verarbeitung personenbezogener Daten, wie zum Beispiel Transparenz und Aufklärung Betroffener, nachzuweisen. Das Vorliegen vorheriger informierter Einwilligungen der Nutzer*innen ist dementsprechend zu dokumentieren.

Für das elektronische Erklären einer Einwilligung ist zur Verifizierung der Willenserklärung der betroffenen Person das Double-Opt-In-Verfahren geboten, wobei die Nachweis-Anforderungen des Art. 5 Abs. 2 DS-GVO und des Bundesgerichthofes (BGH, Urteil vom

10. Februar 2011 - I ZR 164/09) bei der Protokollierung zu berücksichtigen sind. Das Verfahren muss dabei gerade bezüglich des für die Werbung benutzten Kommunikationsmittels den Nachweis der Einwilligung führen können. Das bloße Abspeichern einer IP-Adresse und die Behauptung, dass von dieser IP-Adresse aus eine Einwilligung erteilt worden sei, genüget dem BGH nicht. Die Einwilligung muss vollständig nachweisbar sein, auch hinsichtlich ihres Wortlauts. Für den Nachweis des Einverständnisses ist es erforderlich, dass der Werbende die konkrete Einverständniserklärung jedes einzelnen Verbrauchers vollständig dokumentiert. Im Fall einer elektronisch übermittelten Einverständniserklärung setzt das deren Speicherung und die jederzeitige Möglichkeit voraus, sie auszudrucken. Zu protokollieren ist das gesamte Opt-In-Verfahren.

Die DS-GVO enthält keine spezifischen Vorgaben zur Dauer der Wirksamkeit einer Einwilligung. Wie lange die Einwilligung gültig ist, hängt vom Kontext, dem Umfang der ursprünglichen Einwilligung und den Erwartungen der betroffenen Partei ab. Siehe hierzu Europäischer Datenschutzausschuss, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 (Version 1.1, Rn. 110), abrufbar unter www.edpb.europa.eu.

Der BGH hatte bereits vor Anwendbarkeit der DS-GVO durch Urteil vom 1. Februar.2018 (III ZR 196/17) zur insoweit gleichlautenden damaligen Rechtslage klargestellt, dass eine erteilte Einwilligung grundsätzlich nicht zeitlich abläuft: „Eine zeitliche Begrenzung einer einmal erteilten Einwilligung sieht weder die Richtlinie 2002/58/EG noch § 7 UWG vor. Hieraus ergibt sich, dass diese – ebenso wie eine

Einwilligung nach § 183 BGB – grundsätzlich nicht allein durch Zeitablauf erlischt. (…).“

Aus den Grundsätzen der Transparenz, der Verarbeitung nach Treu und Glauben und der Speicherbegrenzung aus Art. 5 Abs. 1 Buchstabe a und e DS-GVO kann sich aber ergeben, dass sich Verantwortliche nicht mehr auf eine Einwilligung berufen können, wenn sie diese über längere Zeit nicht genutzt haben und die betroffenen Personen nicht mehr mit einer Verarbeitung ihrer Daten auf Grundlage der Einwilligung rechnen müssen. Vor dem Hintergrund des Grundsatzes der transparenten Verarbeitung gemäß Art. 5 Abs. 1 Buchstabe b DS-GVO empfiehlt der EDSA daher als bewährte Praxis, die Einwilligung in angemessenen Zeitabständen zu erneuern. Wenn alle Informationen erneut erteilt werden, hilft dies sicherzustellen, dass die betroffene Person gut darüber informiert bleibt, wie ihre Daten verwendet werden und wie sie ihre Rechte ausüben kann. Siehe hierzu Europäischer Datenschutzausschuss, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 (Version 1.1, Rn. 111), abrufbar unter www.edpb.europa.eu.

Im Sinne einer transparenten Datenverarbeitung ist Werbetreibenden insbesondere zu empfehlen, bei länger als zwei Jahre ungenutzten Einwilligungen vorsorglich eine Erneuerung der Information oder auch der Einwilligungen selbst vorzunehmen. Wenn sich die Verarbeitungsvorgänge beträchtlich ändern oder weiterentwickeln, ist die ursprüngliche Einwilligung nicht länger für derartige Verarbeitungen gültig. Dann muss eine neue Einwilligung eingeholt werden. Siehe hierzu Europäischer Datenschutzausschuss, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung

2016/679 (Version 1.1, Rn. 110), abrufbar unter www.edpb.europa.eu.

Zu der rechtlichen Einschätzung der LDI bezüglich der Voraussetzungen der Nachweisbarkeit der elektronischen Einwilligung ist beim Verwaltungsgericht Düsseldorf derzeit ein Verfahren anhängig. Der Abschluss des Verfahrens soll mehr Klarheit für die Voraussetzungen und das Feststellen einer wirksamen elektronischen Einwilligung bringen.

Oft waren die Beschwerden berechtigt, die wir zu den geschilderten Konstellationen erhielten, da eine Geschäftsbeziehung nicht bestand und auch eine elektronische Einwilligung nicht nachgewiesen werden konnte.

## 10.8 Werbliche Nutzung von Zahlungsverkehrsdaten in der Kreditwirtschaft

**Kontoauszüge enthalten viele interessante Informationen über Bankkund*innen. Eine Auswertung dieser und weiterer Zahlungsverkehrsdaten für Werbezwecke dürfen Banken und Kreditinstitute regelmäßig nur mit einer Einwilligung ihrer Kund*innen vornehmen.**

Werbung zu treiben ist ein legitimes wirtschaftliches Interesse. Für die LDI NRW stellt sich in verschiedenen Fallkonstellationen dabei immer wieder die Frage, welche Daten ihrer Kund*innen Unternehmen für ihre Werbung unter welchen Voraussetzungen nutzen dürfen. Besonders brisant ist die Frage der Werbenutzung der Kund*innendaten von Kreditinstituten, denn wenige Datensammlungen sagen so viel

über das Konsumverhalten und Privatleben der jeweiligen Personen aus, wie deren Zahlungsverkehrsdaten.

Wer kauft wo für welche Beträge ein? Wer leistet welche Mitgliedsbeiträge in welchen Vereinen, Parteien oder sonstigen Organisation? Wer hat ein Haus oder eine Eigentumswohnung? Wer zahlt wie viel Miete? Wer hat welche Zeitung oder kostenpflichtige App abonniert oder Rechnungen an behandelnde Ärzt*innen beglichen? Wer leistet Unterhaltszahlungen an wen? Wer erhält Sozialleistungen? Wer tätigt zu welcher Zeit Bankgeschäfte online oder in der Geschäftsstelle? All das lässt sich anhand der sog. Zahlungsverkehrsdaten ablesen. Diese Daten geben einen umfassenden Einblick in das Privatleben der Kund*innen von Kreditinstituten und sind gerade deswegen so interessant für die Werbung.

Datenschutzrechtlich ist zu beurteilen, ob und in welchem Umfang Kreditinstitute Zahlungsverkehrsdaten ihrer Kund*innen für Werbezwecke auf gesetzlicher Rechtsgrundlage gemäß Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO im eigenen berechtigten Interesse verarbeiten können. Dieses gilt es, mit dem Interesse der Kund*innen am Schutz der eigenen Daten abzuwägen. Praktisch geht es bei dieser rechtlichen Bewertung darum, welche Kontodaten Banken für Werbezwecke nutzen dürfen, ohne dass sie dafür eine Einwilligung ihrer Kund*innen benötigen.

Die Teilnahme am Wirtschaftsleben läuft heute fast ausschließlich über Girokonten. Ein Kreditinstitut erlangt daher über das Girokonto Daten mit hoher Persönlichkeitsrelevanz. Gerade in der Zusammenführung auf dem Girokonto und der möglichen Auswer-

tung lassen sich umfangreiche Schlüsse auf das Privatleben der betroffenen Person ziehen. Aus der Gesamtheit der über das Girokonto abgewickelten Daten kann schnell ein umfassendes Persönlichkeitsprofil entwickelt werden.

Deshalb ist das Interesse der Kund*innen von Kreditinstituten am Ausschluss der Verarbeitung ihrer Zahlungsverkehrsdaten für Werbezwecke sehr hoch im Vergleich zum wirtschaftlichen Interesse der Kreditwirtschaft. Zahlungsverkehrsdaten werden wegen des Umfangs und der aussagekräftigen Informationen, die über das Girokonto abgewickelt werden, als besonders privat und schützenswert empfunden. Bei einem Missbrauch dieser Daten sind zudem negative wirtschaftliche Folgen für betroffene Personen möglich. Daher kann die werbliche Nutzung der Zahlungsverkehrsdaten grundsätzlich nicht auf Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO gestützt werden. Wollen Kreditinstitute Zahlungsverkehrsdaten zu Werbezwecken verarbeiten, müssen sie sich daher grundsätzlich um eine informierte, freiwillige und widerrufliche Einwilligung ihrer Kund*innen nach Art. 6 Abs. 1 Satz 1 Buchstabe a in Verbindung mit Art 7 DS-GVO bemühen. Eine entsprechende Einwilligungserklärung hatte die Sparkassen-Finanzgruppe mit dem DSK-Arbeitskreis Kreditwirtschaft bereits im Jahre 2019 abgestimmt.

Aber auch das berechtigte Interesse der Kreditinstitute im Sinne des Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO an der Verarbeitung von Kund*innendaten zum Zwecke der Direktwerbung ist angemessen zu würdigen. Schon vor Inkrafttreten der DS-GVO war die Nutzung von bestimmten Daten (im Wesentlichen Name, Adressen, Gruppenzugehörigkeit, Beruf und

Geburtsjahrgang) für Werbezwecke nach §§ 28, 29 Bundesdatenschutzgesetz – alte Fassung (BDSG a. F.) grundsätzlich gesetzlich erlaubt. Diese gesetzliche Wertung kann für die Interessenabwägung auch heute noch ein Maßstab sein. Insofern haben Kreditinstitute ein berechtigtes Interesse an der werblichen Nutzung sog. Stammdaten. Für die entsprechende Datenverarbeitung bedarf es dann keiner Einwilligung.

Ob auch die werbliche Nutzung weiterer Daten aus dem Vertragsverhältnis, wie zum Beispiel Höhe und Anzahl der Umsatzdaten, Saldo/Kontostand zu einem bestimmten Stichtag, Höhe des Geldeingangs auf rechtlicher Grundlage ohne Einwilligung der Kund*innen zulässig ist, wird derzeit in einer Arbeitsgruppe des DSK-Arbeitskreises Kreditwirtschaft beraten. Wir werden zu diesen Beratungen weiter berichten.

Kreditinstitute können nur in einem engen Rahmen Kund*innendaten auf gesetzlicher Grundlage für Werbezwecke nutzen. Insbesondere Zahlungsverkehrsdaten dürfen nicht ohne vorherige Einwilligung der Kund*innen für Werbung ausgewertet und genutzt werden.

## 10.9 Automatische Aktualisierung von Kreditkartendaten im Online-Handel

**Die Kreditkartenorganisationen Mastercard und Visa bieten im Online-Handel einen Service zur automatischen Aktualisierung der bei Händler*innen hinterlegten Kreditkartendaten an. Kreditkartennutzer*innen hatten Sorge, dass dies zu unzulässigen Übermittlungen ihrer Kreditkartendaten führen könnte und ein Missbrauch der Daten möglich sei.**

Die LDI NRW erreichten verschiedene Anfragen zum Aktualisierungsservice der Kreditkartenorganisationen Mastercard und Visa. In NRW hatte die Sparkassen-Finanzgruppe ihre Kundschaft über eine anstehende Änderung der Allgemeinen Geschäftsbedingungen ihrer Kreditkartenverträge informiert. Danach sollte eine Klausel ergänzt werden, wonach die Sparkassen den Online-Shops automatisch geänderte Informationen zu den Kreditkartendaten zukommen lassen. Einige Sparkassen*kundinnen hatten Zweifel an der Rechtmäßigkeit des Datenflusses von der Sparkasse über die Kreditkartenorganisationen Mastercard/Visa an die Online-Shops, die als Vertragspartner*innen der Kreditkartenherausgeber*innen autorisiert sind, Zahlungen mit der Karte entgegen zu nehmen.

Unsere Prüfung zeigte, dass die Datenflüsse rechtmäßig waren. Es liegt sogar im Interesse der Karteninhaber*innen, dass eine neu erteilte bzw. aktualisierte Karte für die vorgesehenen Zahlungsvorgänge verwendet werden kann. Wird die Aktualisierung nicht

durchgeführt, würde eine Zahlung möglichweise blockiert, obwohl die karteninnehabende Person sich dessen nicht bewusst ist.

Das Problem bestand aber in der unklaren Beschreibung der neuen Datenverarbeitungsprozesse in der neuen Klausel der Kreditkartenbedingungen. Durch unsere Intervention und mit Unterstützung der Datenschutzaufsichtsbehörden in Bayern, Berlin und Hessen konnten wir eine Klarstellung in den Kreditkartenbedingungen der Sparkassen-Finanzgruppe erreichen. Kartendaten werden nur bei den Online-Shops automatisch aktualisiert, bei denen die Karteninhaber*innen zuvor die Kreditkartendaten hinterlegt haben, z. B. für wiederkehrende Zahlungen bei den am jeweiligen Service teilnehmenden Online-Shops. Es ist also nicht allein ausreichend, dass die Kund*innen ihre Karten eingesetzt haben. Eine automatische Weiterleitung an eine große Anzahl von Online-Shops auf Vorrat erfolgt nicht.

Der Vollständigkeit halber zu erwähnen ist, dass die an dem Aktualisierungsservice teilnehmenden Online-Shops die Kreditkarteninformationen nur speichern dürfen, wenn die betroffene Person ihre Einwilligung nach Art. 6 Abs. 1 Satz 1 Buchstabe a, Art. 7 DS-GVO rechtswirksam erteilt hat. Zur regelmäßig erforderlichen Einwilligung der betroffenen Person für die Speicherung der Kreditkartendaten beim Online-Shop hatte der Europäische Datenschutzausschuss in seiner Empfehlung 02/2021 zur Rechtsgrundlage für die Speicherung von Kreditkartendaten ausschließlich zum Zweck der Erleichterung weiterer Online-Transaktionen Stellung genommen. Die Empfehlung ist unter www.edpb.europa.eu abrufbar.

Durch das kooperative Vorgehen der Datenschutzaufsichtsbehörden konnte für die Verbraucher*innen mehr Klarheit über die Datenverarbeitungsprozesse beim Einsatz ihrer Kreditkarten erreicht werden.

## 10.10 Die Teilnahme an einem entgeltlichen Glücksspielangebot per Telefon

**Wer öffentliche Glücksspiele vermittelt, muss den Jugendschutz gewährleisten, aber auch datenschutzkonform handeln. Besondere Herausforderungen stellen sich beim telefonischen Abschluss eines entgeltlichen Glücksspielvermittlungsvertrages im Hinblick auf die erforderliche Altersverifikation und die Abfrage der Bankdaten. Zudem sind die Vorgaben zur Einwilligung in die Aufzeichnung des Telefonats zu beachten.**

Anlässlich einer Beschwerde befasste sich die LDI NRW mit der Altersverifikation bei der Teilnahme an einem entgeltlichen Glücksspielangebot. Die Beschwerdeführerin hatte sich aufgrund einer Werbung bei einem glücksspielvermittelnden Unternehmen telefonisch gemeldet, um sich über ein kostenpflichtiges Glücksspielangebot zu informieren. In der Werbesendung wurde sie darüber informiert, dass für den Abschluss eines Glücksspielvertrages erforderliche zusätzliche Informationen zu ihrem Spielwunsch erhoben werden, ihre Bankverbindung für Abrechnungszwecke gespeichert und ihre Volljährigkeit anhand von Name, Anschrift und Geburtsdatum über anerkannte Dienstleister überprüft wird, wenn sie sich während des Anrufs für das Glücksspielangebot entscheidet. Noch während des Telefonats erfolgte die Altersverifikation. Als auch die Bankverbindung abgefragt wurde, wollte die Beschwerdeführerin diese

nicht angeben, so dass das Telefonat beendet wurde, ohne dass die Vertragsunterlagen zugeschickt wurden. Das Telefongespräch wurde aufgezeichnet. Zu Beginn des Telefonats wurde sie gefragt, ob das Telefongespräch zu Dokumentationszwecken aufgezeichnet werden darf. Die Einwilligung sah das Unternehmen durch die Fortsetzung des aktiven Telefonats als erteilt an.

Wir waren gebeten, den Zeitpunkt der Altersverifikation einschließlich der Erhebung der Bankdaten vor Vertragsschluss und die Rechtmäßigkeit der Gesprächsaufzeichnung datenschutzrechtlich zu prüfen.

Bei Veranstaltungen und Vermittlungen von Glücksspielen ist die Altersverifikation der Kundschaft gesetzlich verpflichtend vorgegeben, um eine Teilnahme Minderjähriger auszuschließen. Deshalb ist vor Vertragsschluss das Alter mitspielender Personen zu überprüfen. Eine dazu erforderliche Datenverarbeitung ist rechtmäßig, weil der Datenverarbeiter einer entsprechenden Rechtspflicht unterliegt. Für die erforderliche Identitätsprüfung und Altersverifikation stellen verschiedene Unternehmen, unter anderem die Riser-ID Services GmbH, die Schufa-Holding AG oder die Deutsche Post AG, entsprechende Dienstleistungen zur Verfügung, die das Wettspielunternehmen zur Erfüllung der eigenen gesetzlichen Verpflichtung nutzen durfte.

Auch war die Initiierung der Abfrage zur Altersverifikation bereits während des laufenden Telefonats erforderlich. Die Kundin hatte ihr Interesse zur Teilnahme am Wettspiel bekundet und der Vertragsschluss sollte eingeleitet werden. Überwiegende Interessen der am Gewinnspiel interessierten Person

standen dem nicht entgegen. Der vom glücksspielvermittelnden Unternehmen implementierte automatisierte Prozess sieht vor, die entsprechenden Vertragsunterlagen während des Anrufs an die spielinteressierte Person zu versenden. Dies dient der Effizienz des Bestellprozesses; mögliche Fehler bei der Erfassung der Daten der spielinteressierten Personen können so vermieden werden. Vertragsunterlagen dürfen nur an nachweislich volljährige Personen versendet werden. Denn sind die Vertragsunterlagen einmal versendet, hängt der Vertragsschluss nur noch von der Zahlung des Teilnahmeentgeltes ab.

Die Abfrage der Bankverbindung war erforderlich, um den Spielvermittlungsvertrag durchzuführen (Art. 6 Abs. 1 Satz 1 Buchstabe b DS-GVO). Die Altersverifizierung vor der Abfrage der Bankverbindung entspricht dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchstabe c DS-GVO). Es werden nur die Anrufenden nach ihrer Bankverbindung gefragt, die bestätigt haben, dass sie an dem angebotenen Glücks- und Gewinnspiel teilnehmen.

Das Verfahren zur Einwilligung in die Telefonaufzeichnung hat das glücksspielvermittelnde Unternehmen aufgrund eines entsprechenden Hinweises der LDI NRW umgestellt. Die Fortsetzung des Telefonats allein reicht entgegen der ursprünglichen Handhabung nicht mehr aus. Vielmehr muss die spielinteressierte Person gemäß der DS-GVO ihre Einwilligung zur Aufzeichnung des Anrufs zusätzlich verbal äußern. Dies beschreibt der Beschluss der Datenschutzkonferenz „Aufzeichnung von Telefongesprächen“ vom 23. März 2018. Danach ist die Aufzeichnung von Telefongesprächen in aller Regel nur mit Einwilligung der anrufenden Personen zulässig. Eine

datenschutzrechtlich wirksame Einwilligung im Sinne von Art. 4 Nr. 11 DS-GVO setzt voraus, dass die anrufende Person vor Beginn der beabsichtigten Aufzeichnung gefragt wird, ob sie mit der Aufzeichnung einverstanden ist, und falls sie einverstanden ist, gebeten wird, das Einverständnis beispielsweise durch Aussprechen eines „Ja“ oder durch eine aktive bestätigende Handlung (etwa durch das Betätigen einer Telefontaste) eindeutig zum Ausdruck zu bringen.

Die bereits vor Vertragsschluss durch ein Unternehmen durchgeführte Altersverifikation der nachweislich am Glücksspiel Interessierten ist datenschutzkonform. Gleiches gilt für die Erhebung der Bankverbindung zur Bezahlung des Angebots nach erfolgter Altersverifikation, aber vor Vertragsschluss. Anrufende Personen müssen ihre Einwilligung zur Aufzeichnung des Anrufs zusätzlich verbal äußern oder durch eine aktiv bestätigende Handlung zum Ausdruck bringen.

## 10.11 Der datenschutzrechtliche Auskunftsanspruch wird nicht vererbt!

**Die DS-GVO gilt nicht für personenbezogene Daten Verstorbener (vgl. Erwägungsgrund 27 DS-GVO). Erben haben zivilrechtliche Auskunftsansprüche zu Daten des Erblassers im Zusammenhang mit der Erbschaft und daneben eigene Auskunftsansprüche über Daten mit Bezug zu ihrer Person.**

Eine erbberechtigte Person hatte gegenüber einem Kreditinstitut Auskunft über alle Informationen zu den Konten des verstorbenen Elternteils sowie zu allen darin enthaltenen Vermögenswerten, insbesondere

auch zu den Käufen und Verkäufen von Wertpapierpositionen geltend gemacht. Die erbberechtigte Person berief sich dabei auf das Urteil des BGH zum digitalen Nachlass eines Facebook-Kontos (Urteil vom 12. Juli 2018, Az. III ZR 183/17).

Allerdings ist mit diesem Urteil keine Aussage über die Reichweite des datenschutzrechtlichen Auskunftsrechts nach Art. 15 DS-GVO verbunden. Vielmehr hatte der BGH die Frage des Übergangs eines Nutzungsvertrags eines sozialen Netzwerks bei Tod der Person zu beurteilen, die das Facebook-Konto angelegt hat. Es ging also um die zivilrechtliche Fragestellung, ob ein Vertrag über ein Benutzerkonto bei einem sozialen Netzwerk vererbbar ist oder nicht. Es ging um den sog. digitalen Nachlass.

Davon zu trennen ist der datenschutzrechtliche Auskunftsanspruch nach Art. 15 DS-GVO. Auch anderweitige erbrechtliche Auskunftsansprüche stehen neben dem datenschutzrechtlichen Auskunftsanspruch, erweitern diesen aber nicht.

Der Auskunftsanspruch der verstorbenen Person gemäß Art. 15 DS-GVO ist nicht vererbbar, sondern ein höchstpersönliches Recht, das nur zu Lebzeiten ausgeübt werden kann. Die Anwendbarkeit der DS-GVO auf Informationen zu einer Person endet mit deren Tod (vgl. Erwägungsgrund 27 DS-GVO). Das Recht auf informationelle Selbstbestimmung ist im Schutz der allgemeinen Handlungsfreiheit gemäß Art. 2 Abs. 1 GG begründet, die nur von Lebenden wahrgenommen werden kann. Erbende haben daher nicht per se einen Anspruch auf Auskunft nach Art. 15 DS-GVO zu sämtlichen Daten der Person, die sie beerben.

In dem uns vorliegenden Fall konnte die erbberechtigte Person das Recht auf Auskunft nach Art. 15 DS-GVO insoweit aber geltend machen, als dass es sich infolge der Erbschaft bei den von dem Kreditinstitut verarbeiteten Informationen um Daten mit Bezug auf ihre eigene Person handelte. So können Erbende Auskunft nach Art. 15 DS-GVO über die Daten der verstorbenen Person verlangen, wenn es sich zugleich um Daten handelt, die ihr eigenes Erbe betreffen. Es können auch Daten aus der Zeit vor dem Erbfall insoweit auskunftspflichtig sein, als sie für die eigene Erbschaft relevant sind. Der datenschutzrechtliche Anspruch tritt also neben zivilrechtliche Auskunftsansprüche. Handelt es sich zugleich um Daten Dritter (zum Beispiel um Miterbende), hat die für die Datenverarbeitung verantwortliche Stelle sorgfältig zu prüfen, wie deren Rechte geschützt werden können (vgl. Art. 15 Abs. 4 DS-GVO).

Die Entscheidung des BGH zum Facebook-Konto (Urteil vom 12. Juli 2018, Az.: III ZR 183/17) trifft eine rein zivilrechtliche Aussage zum digitalen Nachlass, hat das datenschutzrechtliche Recht auf Auskunft aber nicht ausgeweitet. Mit der Erbschaft erhalten Daten der verstorbenen Person einen Bezug zu den erbenden Personen. In dem Umfang, in dem personenbezogene Daten des Verstorbenen für die eigene Erbschaft relevant sind, haben Erben einen eigenen datenschutzrechtlichen Auskunftsanspruch.

# 11. Datensicherheit

## 11.1 Unzureichender Schutz von Schnelltest-Ergebnissen vor unbefugtem Zugriff

**Viele Betreiber*innen von Corona-Testzentren bieten ihren Kund*innen neben der Vor-Ort-Ausgabe des schriftlichen Testergebnisses die Möglichkeit, das Resultat auf den Webseiten abzurufen. Die Maßnahmen der Verantwortlichen zur Gewährleistung eines gesicherten Zugriffs auf diese online bereitgestellten Dokumente waren bei verschiedenen Betreiber*innen nicht ausreichend, sodass nach Prüfung der LDI NRW zusätzliche technische und organisatorische Maßnahmen durch die Verantwortlichen umgesetzt wurden.**

Die Dienstleistungen von vielen neu eröffneten Corona-Testzentren werden in der COVID-19-Pandemie zahlreich durch die Bürger*innen in Anspruch genommen. Um Wartezeiten vor Ort für die Kund*innen der Testzentren zu vermeiden und einen komfortablen Zugang auf die Testergebnisse zu ermöglichen, bieten viele Testzentren ihren Kund*innen einen Online-Zugriff auf die Testdokumente an. Die Testergebnisse enthalten unter anderem Gesundheitsdaten der Betroffenen und somit personenbezogene Daten besonderer Kategorie im Sinne des Art. 9 Abs. 1 DS-GVO. Der Zugriff auf die so bereitgestellten Datensätze ist damit besonders zu schützen.

Uns haben Beschwerden von Betroffenen und Mitteilungen von Dritten erreicht, welche mangelhafte technische und organisatorische Maßnahmen der Webdienste für den Abruf der Testergebnisse dargelegt haben. Aufgrund von fehlenden oder mangelnden

technischen Sicherheitsvorkehrungen konnten über die Webseiten verschiedener Testzentren auch Schnelltest-Ergebnisse anderer Personen abgerufen werden.

Der Zugang zu den Dokumenten wird den Kund*innen in der Regel durch einen individualisierten Link ermöglicht. Dieser Link enthält eine einzigartige Zeichenreihenfolge zur Authentifikation der Person. Bei der Generierung solcher individuellen Identifikationsmerkmale hat der Verantwortliche zu beachten, dass das Merkmal eine ausreichend hohe Entropie aufweist, um eine geeignete Authentifizierung der Benutzer*innen zu ermöglichen und ein Erraten des Merkmals zu verhindern. Insbesondere sind derartige Merkmale nicht nach einem Muster zu erstellen, das eine erkennbare Regelmäßigkeit aufweist und somit durch unbefugte Dritte nachvollzogen werden kann. Sollten eine systematisch gezielte Abfrage von Testergebnissen oder eine kontinuierliche Angabe inkorrekter Identifikationsmerkmale erkannt werden, ist eine Beschränkung des Zugriffs umzusetzen, indem die betroffenen Anfragen beispielsweise gefiltert oder progressiv verzögert werden. Die Bereitstellung der Testergebnisse auf der Onlinepräsenz der Testzentren ist auf den Zeitraum der Zweckerfüllung zu beschränken, sodass das Risiko eines unbefugten Zugriffs minimiert wird. Des Weiteren kann durch die Abfrage eines zusätzlichen niedrigschwelligen Identifikationsmerkmals, wie die Postleitzahl, vor Anzeige der Testergebnisse eine unbeabsichtigte Offenbarung vermieden werden.

Die festgestellten mangelhaften technischen und organisatorischen Maßnahmen konnten nach unseren Hinweisen durch die Verantwortlichen in der Regel

kurzfristig korrigiert werden, oder der Zugang zu den betroffenen Systemen mit Sicherheitsmängeln wurde eingestellt.

Sofern der Abruf von sensiblen personenbezogenen Daten – insbesondere der von Gesundheitsdaten – über Webseiten erfolgen soll, müssen diese mit Sicherheitsmechanismen nach dem Stand der Technik entwickelt und vor der Inbetriebnahme hinsichtlich der IT-Sicherheit geprüft werden. Der Zeitdruck, unter dem in der Pandemie Strukturen aufgebaut werden mussten, sollte dennoch nicht dazu führen, dass Gesundheitsdaten technisch unzureichend geschützt werden.

## 11.2 Datenpannen bei Auftragsverarbeitern – Welche Pflichten obliegen wem?

**Unternehmen, die für die Datenverarbeitung ganz oder teilweise Dienstleistungsunternehmen als Auftragsverarbeiter einsetzen, haben unter Umständen eigene Pflichten, wenn sich bei den Auftragsverarbeitern Datenpannen ereignen. Sind in einem solchen Fall auch ihre Daten betroffen, ist es vor allem für kleine und mittlere Unternehmen oft nicht klar, was sie in einem solchen Fall tun müssen.**

Grundsätzlich gilt: Auch bei der Beauftragung eines Auftragsverarbeiters im Sinne des Art. 4 Nr. 8 DS-GVO verbleiben die gesetzlichen Pflichten der DS-GVO weitgehend beim Verantwortlichen im Sinne des Art. 4 Nr. 7 DS-GVO. Dies gilt insbesondere für den Fall einer Datenpanne bei einem Auftragsverarbeiter. Dem Verantwortlichen obliegen dann weiterhin die

Dokumentations-, Melde- und Benachrichtigungspflichten nach Art. 33, 34 DS-GVO hinsichtlich der im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten gemäß Art. 33 Abs. 1, Abs. 5 und Art. 34 Abs. 1 DS-GVO.

Auftragsverarbeiter müssen deshalb beim Bekanntwerden einer Datenpanne die betroffenen Verantwortlichen unverzüglich hierüber informieren (vgl. Art. 33 Abs. 2 DS-GVO). Spätestens mit dieser Information wird den Verantwortlichen die Datenpanne bekannt und sie müssen ihre Melde- und Benachrichtigungspflichten nach Art. 33, 34 DS-GVO innerhalb der gesetzlichen Fristen prüfen. Sollten hierzu Informationen fehlen, so sind diese beim Auftragsverarbeiter anzufordern.

Gemäß Art. 28 Abs. 3 Buchstabe f DS-GVO muss der mit dem Auftragsverarbeiter geschlossene Vertrag zur Auftragsverarbeitung den Auftragsverarbeiter verpflichten, den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten nach Art. 33, 34 DS-GVO zu unterstützen. Die vom Auftragsverarbeiter zur Verfügung gestellten Informationen müssen es den Verantwortlichen erlauben

- den Vorfall und ihre Betroffenheit nachzuvollziehen,
- eine Bewertung der möglichen Folgen für die betroffenen Personen sowie des Risikos für ihre Rechte und Freiheiten vorzunehmen
- und die weiteren in Art. 33 Abs. 3 DS-GVO geforderten Informationen zusammenzutragen.

Weiterhin sollte der Auftragsverarbeiter eine Stelle benennen, an die sich Verantwortliche für Rückfragen wenden können. Verantwortliche und Auftragsverarbeiter sollten diese Punkte bei der Vertragsgestaltung berücksichtigen.

Eine Meldung des Auftragsverarbeiters an die zuständige Aufsichtsbehörde, kann dann erforderlich sein, wenn von der Datenpanne auch personenbezogene Daten betroffen sind, die der Auftragsverarbeiter selbst als Verantwortlicher verarbeitet.

Nach Einschätzung der LDI NRW kann bei einer Datenpanne bei Auftragsverarbeitern unter den folgenden Bedingungen anstelle der Meldungen durch die einzelnen Verantwortlichen eine Sammelmeldung durch eine zentrale Stelle treten, solange die von der Sammelmeldung umfassten Verantwortlichen

1. der Aufsicht der LDI NRW unterliegen,
2. gemäß Art. 33 Abs. 2 DS-GVO über den Vorfall informiert wurden,
3. die zentrale Stelle dazu berechtigt haben, für sie die Meldung an die zuständigen Aufsichtsbehörden abzugeben,
4. bei der Risikobeurteilung beteiligt wurden und
5. bei der Auswahl und Umsetzung von Maßnahmen zur Abhilfe, Abmilderung und Vermeidung eines erneuten Auftretens der Datenpanne sowie der ggf. zu erfolgenden Benachrichtigung der betroffenen Personen einbezogen wurden – insbesondere bezüglich Maßnahmen, die im Einflussbereich der Verantwortlichen liegen.

In einer solchen Sammelmeldung müssen die nach Art. 33 Abs. 3 DS-GVO geforderten Informationen differenziert für die einzelnen Verantwortlichen als Anlage beigefügt werden.

Im Jahr 2021 konnten wir einen Anstieg von Meldungen aufgrund von Datenpannen bei Auftragsverarbeitern feststellen. In einzelnen Fällen erfolgten Meldungen von Verantwortlichen nicht oder verspätet, da sich diese ihrer Pflichten nach Art. 33, 34 DS-GVO nicht bewusst waren. In anderen Fällen war keine Meldung an uns erforderlich, da nur ein geringes Risiko für die Rechte und Freiheiten der betroffenen Personen vorlag und daher eine Dokumentation des Vorfalls genügte.

Zwei Datenpannen bei Auftragsverarbeitern haben wir zum Anlass genommen, Verantwortliche zu kontaktieren, von denen keine Meldung zur Datenpanne eingegangen war. Wir wollten wissen, ob sich die Verantwortlichen ihrer Pflichten nach Art. 33, 34 DS-GVO bewusst sind.

Im ersten Fall lag eine Sicherheitslücke bei einem Dienstleister vor, der für Online-Händler*innen eine Lösung zur Verknüpfung von Warenwirtschaftsystemen mit Online-Marktplätzen anbietet. Wir haben 22 Online-Händler*innen in unserer Zuständigkeit kontaktiert, deren Rückmeldungen noch ausgewertet werden. Im zweiten Fall lag eine Datenpanne bei einem Dienstleister vor, der vorwiegend für Kommunen tätig ist. Hier wurden sieben Kommunen kontaktiert. Unsere Prüfung hat ergeben, dass der IT-Dienstleister die Kommunen umfänglich über die Datenpanne informiert hat. Die sieben Kommunen haben uns ihre interne Dokumentation nach Art. 33 Abs. 5 DS-GVO

vorgelegt, die jeweils eine nachvollziehbare Risikobewertung umfasste. Die Kommunen kamen in ihren Risikobewertungen zu der Einschätzung, dass kein mehr als nur geringes Risiko für die betroffenen Personen bestand. Damit war eine Meldung bei LDI NRW und eine Benachrichtigung der betroffenen Personen nicht erforderlich.

Die LDI NRW wird bei bekanntgewordenen Datenpannen bei Auftragsverarbeitern unter Berücksichtigung der Umstände sowie des Risikos für die Rechte und Freiheiten natürlicher Personen weitere solche Prüfungen durchführen. Dies gilt insbesondere für Datenpannen, bei denen eine Benachrichtigung der betroffenen Personen angezeigt ist.

Auftragsverarbeiter müssen Datenpannen unverzüglich ihren betroffenen Auftraggeber*innen mitteilen und dabei alle Informationen zur Verfügung stellen, die diese benötigen, um ihren Pflichten nach Art. 33, 34 DS-GVO nachzukommen. Verantwortliche müssen bei einer Datenpanne eines Auftragsverarbeiters das Risiko für die bei ihnen betroffenen Personen bewerten und ihren Dokumentations-, Melde- und Benachrichtigungspflichten nachkommen.

## 11.3 Über 300 Datenverlustmeldungen aufgrund der Sicherheitslücke Hafnium – Maßnahmen zum Umgang mit den Gefahren von Zero-Day-Exploits

**Zero-Day-Exploits sind Sicherheitslücken in Systemen bzw. Produkten, die bereits von Hacker*innen ausgenutzt werden, für die aber noch keine Sicherheitsaktualisierungen von Anbieter*innen bzw. Hersteller*innen zur Verfügung stehen. Eine solche Lücke im Produkt Microsoft Exchange hatte auch in NRW weitreichende Konsequenzen.**

Im Dezember 2020 haben Sicherheitsforscher*innen eine Sicherheitslücke im Produkt Microsoft Exchange entdeckt und ein Beispielprogramm entwickelt, das die Lücke ausnutzt, einen sog. „Proof-of-Concept“. Microsoft wurde von den Sicherheitsforscher*innen informiert. Im Januar 2021 kam es zu den ersten Angriffen, die auf diese Sicherheitslücke zurückzuführen sind. Erst Anfang März 2021 stellte Microsoft einen Sicherheitspatch zur Verfügung.

In der Zwischenzeit wurden viele über das Internet erreichbare Exchange-Server automatisiert über die Sicherheitslücke angegriffen und kompromittiert. Bei den betroffenen Servern wurde eine Hintertür angelegt, über die diese kontrolliert werden konnten. Dabei gab es insbesondere die Möglichkeit auf dem Server verfügbare E-Mails und Adressbücher auszulesen. Da die Hacker*innengruppe „Hafnium“ die Sicherheitslücke im großen Stil ausnutzte, wird die Sicherheitslücke als „Hafnium-Exploit“ bezeichnet.

Das Ausmaß der Ausnutzung der Sicherheitslücke stellte in diesem Fall ein Novum dar, da eine Vielzahl von Verantwortlichen und Auftragsverarbeitern das

betroffene Produkt einsetzten und die Hacker*innengruppe Hafnium automatisiert angreifbare Server ermittelt und mit der Hintertür versehen hat. Der LDI NRW gingen allein zu dieser Sicherheitslücke über 300 Meldungen nach Art. 33 DS-GVO ein. In den uns bekannt gewordenen Fällen fand überwiegend über die Installation der Hintertür und den Abruf des auf dem Server vorliegenden Adressbuchs hinaus kein weiterer unbefugter Zugriff auf die Systeme statt. Nur in einzelnen Fällen, bei denen die Sicherheitslücke über einen Monat nicht geschlossen wurde, wurden die Systeme mittels einer Ransomware verschlüsselt. Die betroffenen Systeme wurden von den Verantwortlichen und Auftragsverarbeitern soweit möglich aktualisiert und bereinigt oder neu aufgesetzt.

Seit Jahren ist eine zunehmende Professionalisierung der Hacker*innengruppen zu beobachten. Die Gruppen suchen nach neuen Sicherheitslücken und entwickeln für bekannt gewordene Sicherheitslücken in kurzer Zeit Werkzeuge, um diese automatisiert ohne großen zusätzlichen Aufwand ausnutzen zu können. Über öffentlich zugängliche Suchmaschinen können Systeme mit bestimmten Eigenschaften gefunden werden, die aus dem Internet heraus erreichbar sind. So können Angreifer*innen Systeme identifizieren, die potenziell über eine noch nicht geschlossene Sicherheitslücke verfügen und diese kompromittieren. Die Hacker*innengruppen reagieren inzwischen so schnell auf Sicherheitslücken, dass sie diese immer häufiger im großen Stil ausnutzen können, ohne dass Verantwortliche und Auftragsverarbeiter dies zunächst bemerken.

Verantwortliche und Auftragsverarbeiter müssen deswegen zum Schutz der von ihnen verarbeiteten personenbezogenen Daten Maßnahmen treffen bzw. verstärken. Anti-Viren-Software und andere Software zur Erkennung von Schadsoftware und ungewöhnlichen Aktivitäten auf Endgeräten (sog. Endpoint-Protection-Software) helfen bei Zero-Day-Exploits nicht zuverlässig, weil die Anbieter Informationen zur Erkennung etwaiger Schadsoftware oder von Angriffsmustern erst zeitverzögert bereitstellen können, nachdem ihnen die Sicherheitslücke bekannt wurde. Zum Schutz ihrer Systeme müssen Verantwortliche und Auftragsverarbeiter daher weitere Maßnahmen treffen, um das Vorliegen von Sicherheitslücken in ihren Systemen auszuschließen und unbefugte Zugriffe aus dem Internet heraus zu verhindern. Hier bietet sich ein sog. „Defense-in-Depth-Ansatz“ an, bei dem mehrere Sicherheitsmaßnahmen so eingesetzt werden, dass das Versagen einer Maßnahme nicht dazu führt, dass etwaige Angriffe ermöglicht werden (siehe auch 26. Bericht unter 11.2).

Um über Sicherheitslücken in den eingesetzten Systemen bzw. Produkten rechtzeitig informiert zu sein, müssen regelmäßig die Hinweise und Warnungen von Produkthersteller*innen, Dienstleister*innen und des Bundesamts für Sicherheit in der Informationstechnik (BSI) gesichtet und bewertet werden. Verfügbare Sicherheitsaktualisierungen müssen zeitnah eingespielt werden, um Sicherheitslücken zu schließen. Sofern keine Sicherheitsaktualisierungen zu bekannten Sicherheitslücken verfügbar sind, sollte unter Berücksichtigung des Risikos für die Rechte und Freiheiten der betroffenen Personen erwogen werden, die Systeme abzuschalten bzw. vom Internet zu tren-

nen. Systeme, die für eine längere Zeit angreifbar waren, sollten auch nach dem Einspielen der Sicherheitsaktualisierungen auf eine möglicherweise unbemerkt erfolgte Infektion mit Schadsoftware geprüft werden. Sofern eine solche Infektion festgestellt wird, muss das betroffenen System möglichst bereinigt oder neu aufgesetzt werden.

Wie wichtig die Prüfung hinsichtlich unbemerkter Infektionen mit Schadsoftware ist, zeigte ein Ransomware-Angriff auf das Universitätsklinikum Düsseldorf im September 2020. Das Klinikum hatte zwar kurzfristig die Sicherheitsaktualisierung zu einer Sicherheitslücke in einem Produkt der Firma Citrix installiert, jedoch hatten Angreifer*innen zuvor unbemerkt die Lücke ausgenutzt und eine Hintertür in den Systemen des Klinikums hinterlassen. Über diese Hintertür starteten die Angreifer*innen die Verschlüsselung der Systeme, nachdem die Sicherheitslücke bereits geschlossen war. In der Folge war der Klinikbetrieb erheblich gestört und es konnten vorübergehend keine neuen Patient*innen aufgenommen werden.

Um die eigenen Systeme vor den Gefahren von Zero-Day-Exploits zu schützen, sollten die über das Internet unmittelbar erreichbaren Systeme auf ein Minimum reduziert werden. Dies kann beispielsweise über den Einsatz von virtuellen privaten Netzwerken (VPN) erfolgen, die einen Zugriff auf die Systeme erst nach einer zuvor erfolgten Authentifizierung erlauben und vor einem direkten Zugriff schützen. Weitere Maßnahmen sollten erwogen werde. In Betracht kommen das Einschränken des IP-Adressraums, über den Zugriffe zugelassen werden, und Überwachungssysteme (sog. „Intrusion-Detection-Systeme“), die Zu-

griffe auf ungewöhnliche Muster hin prüfen und gegebenenfalls entsprechende Maßnahmen veranlassen (Sperren der IP-Adresse; Alarmierung der IT-Sicherheitsabteilung).

Die wachsende Bedrohungslage hinsichtlich der Ausnutzung von Zero-Day-Exploits macht deutlich, dass Verantwortliche und Auftragsverarbeiter verstärkt Maßnahmen zur Wartung und Überwachung der von ihnen eingesetzten Systeme bzw. Produkte treffen müssen. Dafür müssen sie die Zuständigkeiten für diese Aufgaben klar regeln und entsprechende Prozesse implementieren. Zudem müssen aus dem Internet erreichbare Schnittstellen geschützt und gehärtet werden, um die Ausnutzung von Sicherheitslücken frühzeitig erkennen und verhindern zu können. Im Falle eines erfolgreichen Angriffs empfehlen wir, die betroffenen Systeme neu aufzusetzen bzw. auf einen sicheren vorherigen Stand zurückzusetzen, um auszuschließen, dass nach einer Bereinigung der Systeme ggf. weiterhin unbemerkt installierte Hintertüren vorhanden sind.

# Anhang – Veröffentlichungen der Datenschutzkonferenz 2021

Neben den hier abgedruckten Entschließungen und Beschlüssen der Datenschutzkonferenz sind alle weiteren Veröffentlichungen auf der Homepage der Datenschutzkonferenz www.datenschutzkonferenz-online.de abrufbar.

## Entschließungen der Datenschutzkonferenz 2021

Mit Entschließungen nimmt die Datenschutzkonferenz zu datenschutzpolitischen Fragen öffentlich Stellung. Entschließungen werden sowohl in den Konferenzen, als auch zwischen den Konferenzen gefasst.

- **29.03.2021 – Coronavirus: Impfnachweis, Nachweis negativen Testergebnisses und Genesungsnachweis in der Privatwirtschaft und im Beschäftigungsverhältnis gehören gesetzlich geregelt!**

  Darf die Teilnahme an privatwirtschaftlichen Angeboten wie Restaurant- oder Konzertbesuche davon abhängig gemacht werden, dass die Besucher und Besucherinnen eine erfolgte Anti-Corona-Impfung oder eine überstandene Infektion nachweisen bzw. ein negatives Testergebnis vorlegen? Neben dieser etwa im Zusammenhang mit dem auf EU-Ebene geplanten „digitalen grünen Zertifikat“ vieldiskutierten Frage erreichen die Datenschutzaufsichtsbehörden fortlaufend Beratungsanfragen von Arbeitgebern, die Gesundheitsdaten wie die Körpertemperatur oder den Impfstatus von Beschäftigten erheben und verarbeiten wollen.

  Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) weist darauf hin, dass die Verarbeitung von Gesundheitsdaten zu privatwirtschaftlichen Zwecken (sei es im allgemeinen Wirtschaftsbereich oder im Be-

schäftigungsbereich) den Anforderungen der europäischen Datenschutz-Grundverordnung (DSGVO) genügen muss. Informationen über den Impfstatus einer Person sind ebenso Gesundheitsdaten wie das Ergebnis eines Coronatests oder der Nachweis einer überstandenen Infektion. Gesundheitsdaten stehen unter dem besonders strengen Schutz der DSGVO und dürfen nur unter eng zu verstehenden Ausnahmen verarbeitet werden.

In aller Regel geboten sind konkrete gesetzliche Regelungen, die eine Verarbeitung solcher Gesundheitsdaten ausdrücklich zulassen, wie es etwa nach § 20 Infektionsschutzgesetz bei der Masernschutzimpfung im Bereich von Kindertageseinrichtungen der Fall ist. Derartige Regelungen zur Nachweispflicht einer Impfung, einer Genesung bzw. eines negativen Tests, um den Zugang zu privatwirtschaftlichen Veranstaltungen oder Einrichtungen zu ermöglichen, fehlen bislang im Zusammenhang mit der Coronapandemie weitestgehend.

In Ermangelung einer gesetzlichen Grundlage bedarf es somit in der Regel einer Einwilligung der Restaurant- oder Konzertbesucher, Arbeitnehmer etc. in die Erhebung und Verarbeitung ihrer Gesundheitsdaten, wobei vor allem im Beschäftigungsbereich die Freiwilligkeit der Einwilligung regelmäßig problematisch ist.

Ohne eine gesetzliche Regelung muss stets im Einzelfall geprüft werden, inwieweit die Verarbeitung von Daten über den Impfstatus oder im Rahmen einer Testung datenschutzrechtlich zulässig ist. Diese Einzelfallbetrachtung ist aufgrund der anzustellenden komplexen juristischen Abwägungen für alle Beteiligten mit großem Aufwand und rechtlichen Unsicherheiten verbunden. Ein uneinheitliches Vorgehen, etwa durch unterschiedliche Regelungen in den Kommunen, könnte zudem zu einer für die Bürgerinnen und Bürger schwer überblickbaren Praxis führen.

Um dies zu vermeiden und für die Datenerhebung und -verarbeitung im privatwirtschaftlichen Bereich Rechtsklarheit, Rechtssicherheit und eine einheitliche Lösung zu erreichen, bedarf es

nach Ansicht der DSK einer auf die konkrete pandemische Lage bezogenen, zeitlich befristeten gesetzlichen Regelung. Hierin ist klar und transparent zu regeln, wer, von wem und unter welchen Voraussetzungen Impfdaten, Testergebnisse, Nachweise zu einer überstandenen Infektion und andere Gesundheitsdaten im privatwirtschaftlichen Kontext nutzen darf. Dabei muss das Gesetz den strengen Vorgaben des Artikels 9 Abs. 2 DSGVO genügen.

Die DSK fordert den Gesetzgeber auf, kurzfristig ein entsprechendes Gesetzgebungsverfahren in die Wege zu leiten.

- **29.04.2021 – Chancen der Corona-Warn-App 2.0 nutzen**

  Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) erinnert angesichts der bereits seit mehr als einem Jahr andauernden Pandemie und der damit auch im Bereich des Datenschutzes einhergehenden Grund-rechtseingriffe an das grundlegende rechtsstaatliche Erfordernis, diese Eingriffe fortlaufend kritisch zu bewerten und zu evaluieren. Die DSK bittet im Zuge einer solchen Evaluation und Anpassung infektionsschutzrechtlicher Instrumente durch Bund und Länder die mit der Version 2.0 der Corona-Warn-App (CWA) eröffneten datensparsameren Möglichkeiten der pseudonymisierten Clustererkennung und Kontaktbenachrichtigung eingehend und zeitnah zu prüfen.

  Die DSK empfiehlt den Ländern, die Nutzung der CWA jedenfalls als ergänzende Möglichkeit zur Benachrichtigung potentiell infizierter Personen und zur Clustererkennung in ihren Konzepten zur Pandemiebekämpfung zu berücksichtigen.

  Seit dem Update auf die Version 2.0 verfügt die CWA über eine entsprechende Funktion, die genutzt werden kann, um sich an Orten oder Veranstaltungen, wo viele Menschen zusammenkommen, zu registrieren. Auch wenn hierbei – anders als bei anderen Apps – keine personenbezogenen Daten erhoben und später an

ein Gesundheitsamt übermittelt werden können, kann die pseudonymisierte Clustererkennung der CWA einen erheblichen Beitrag zur Unterbrechung von Infektionsketten leisten.

Durch die unmittelbare Vernetzung der CWA-Nutzenden werden Personen, die einem potentiellen Infektionsrisiko ausgesetzt waren, unmittelbar und somit schneller als über die Gesundheitsämter informiert. Zudem ist aufgrund der hohen Akzeptanz der CWA mit mittlerweile über 27 Millionen Downloads die Wahrscheinlichkeit hoch, dass Personen auf diese Möglichkeit der aus datenschutzrechtlicher Sicht zu bevorzugenden pseudonymen digitalen Registrierung zurückgreifen.

Die Förderung der Nutzung der CWA zur Clustererkennung könnte dazu führen, dass die App von noch mehr Personen genutzt werden würde. Dies wiederum würde auch die Chance der Erkennung und Warnung vor Risikobegegnungen außerhalb der Nutzung der Clustererkennung weiter erhöhen und damit aktiv zur Pandemiebekämpfung beitragen.

## Beschlüsse der Datenschutzkonferenz 2021

Beschlüsse der Datenschutzkonferenz sind Positionen, die die Auslegung datenschutzrechtlicher Regelungen bzw. entsprechende Empfehlungen betreffen.

- **15.03.2021 – „Energieversorgerpool“ darf nicht zu gläsernen Verbraucher*innen führen**

  Bei Auskunfteien und Energieversorgern gibt es Überlegungen, einen sog. Energieversorgerpool zu schaffen. In diesem zentralen Datenpool sollen auch Positiv-daten der Kund*innen gespeichert und an andere Energieversorger übermittelt werden. Positivdaten sind Daten über Verträge, bei denen die Belieferten keinen Anlass zu Beanstandungen geben, sich also vertragskonform verhalten.

  Informationen über die Anzahl abgeschlossener Verträge und die jeweilige Vertragsdauer können Hinweise darauf geben, ob Verbraucher*innen eine längere Vertragsbeziehung zu einem Stromversorger beabsichtigen oder etwa regelmäßig Angebote für Neukund*innen nutzen. Verbraucher*innen, die regelmäßig das für Sie kostengünstigste Angebot am Markt wählen und dazu den Anbieter wechseln möchten, könnten dann von Versorgungsunternehmen bei preislich attraktiven Angeboten ausgeschlossen werden.

  Jede Bürgerin und jeder Bürger hat jedoch das Recht, den Wettbewerb zwischen den Energieversorgern zu nutzen und am Markt nach günstigen Angeboten zu suchen. Der Wunsch, vermeintliche „Schnäppchenjäger“ in einem zentralen Datenpool zu erfassen, um sie bei Vertragsanbahnung als solche identifizieren und ggf. von Angeboten ausschließen zu können, stellt kein berechtigtes Interesse i. S. d. Art. 6 Abs. 1 Satz 1 lit. f) DS-GVO dar. Es war gerade das Ziel des Gesetzgebers, durch die Liberalisierung des Energiemarktes einen wirksamen und unverfälschten Wettbewerb bei der Versorgung mit Elektrizität und Gas zu

ermöglichen. Der Versuch, preisbewusste und wechselfreudige Verbraucher*innen zu identifizieren und sie ggf. von bestimmten Angeboten auszuschließen, liefe dieser Zielsetzung zuwider.

Selbst wenn die Interessen der Unternehmen als berechtigt angesehen würden, überwiegen in derartigen Fällen die schutzwürdigen Interessen und Grundrechte der Kund*innen. Vertragstreue Verbraucher*innen dürfen zu Recht erwarten, dass keine über den Vertragszweck hinausgehende Verarbeitung ihrer Daten erfolgt, die ggf. ihre Möglichkeiten einschränkt, frei am Markt agieren zu können.

Die Speicherung und Übermittlung von Positivdaten durch einen Energieversorgerpool würde erheblich zu gläsernen Verbraucher*innen beitragen und wäre nach Art. 6 Abs. 1 Satz 1 lit. f) DS-GVO rechtswidrig.

- **22.09.2021 –Verarbeitung von Positivdaten von Privatpersonen aus Verträgen über Mobil-funkdienste und Dauerhandelskonten durch Auskunfteien**

  Die DSK beschließt Folgendes:

  Nach erneuter Prüfung der Rechtslage wird der Beschluss der DSK vom 11.06.2018 aufrechterhalten, so dass weiterhin

  1. die Übermittlung und Verarbeitung von sog. Positivdaten an bzw. durch Handels- und Wirtschaftsauskunfteien grundsätzlich nicht auf Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO gestützt werden kann und
  2. es für eine Übermittlung und Verarbeitung von sog. Positivdaten regelmäßig einer wirksamen Einwilligung der betroffenen Person unter Beachtung der hohen Anforderungen an die Freiwilligkeit bedarf.

Begründung:

Die DSK hat mit Beschluss vom 11. Juni 2018 festgestellt, dass Handels- und Wirtschaftsauskunfteien sog. Positivdaten zu Privatpersonen grundsätzlich nicht auf Grundlage des Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO erheben können. Dabei sind Positivdaten Informationen, die keine negativen Zahlungserfahrungen oder sonstiges nicht vertragsgemäßes Verhalten zum Inhalt haben, sondern zum Beispiel die Informationen über die Tatsache, dass ein Vertrag abgeschlossen wurde. Bei solchen Positivdaten überwiegt regelmäßig das schutzwürdige Interesse der betroffenen Personen, selbst über die Verwendung ihrer Daten zu bestimmen. Werden die Daten von einem Verantwortlichen an eine Auskunftei übermittelt, ist insoweit bereits die Übermittlung dieser Daten nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO regelmäßig unzulässig. Ebenso unzulässig ist die Verarbeitung dieser Daten durch die Auskunftei.

Die DSK hatte nun zu überprüfen, ob für die verbreitete Praxis der Übermittlung und Verarbeitung von Positivdaten zu Verträgen über Mobilfunkdienste und Dauerhandelskonten von Privatpersonen eine andere Bewertung erforderlich ist. Diese Praxis betrifft längerfristige Verträge, die durch Vorausleistungsverpflichtungen oder Finanzierungs- bzw. Stundungselemente als kreditorische Risiken betrachtet werden, aber keine Vertragsstörungen aufweisen. Sie werden bei der Bildung von Scorewerten der betroffenen Personen, die Handel oder Kreditwirtschaft zur Bonitätsprüfung heranziehen, regelmäßig neben einer Vielzahl weiterer Sachverhalte einbezogen.

Im Rahmen dieser Überprüfung hatten Unternehmen und Verbände bis zum 31. August 2021 Gelegenheit, Stellungnahmen zu den aufgeworfenen Rechtsfragen abzugeben. Nach sorgfältiger Auswertung der eingegangenen Stellungnahmen kommt die DSK zu dem Ergebnis, dass für die Übermittlung der Positivdaten durch die Mobilfunkdiensteanbieter und die Handelsunternehmen

zwar berechtigte Interessen bestehen, die Qualität der Bonitätsbewertungen zu verbessern und die beteiligten Wirtschaftsakteure vor kreditorischen Risiken zu schützen. Besondere Umstände, die – wie bei Kreditinstituten insbesondere auf Grund ihrer spezifischen Verpflichtungen nach dem Kreditwesengesetz – entsprechend dem Beschluss der DSK vom 11.06.2018 regelmäßig ein die Interessen, Grundrechte und Grundfreiheiten der betroffenen Person überwiegendes Interesse der Verantwortlichen oder Dritter an der Verarbeitung bestimmter Positivdaten vermitteln würden, konnte die DSK im Rahmen ihrer Über-prüfung jedoch nicht feststellen. Eine von der oben genannten Grundregel abweichende Bewertung ist daher nicht begründbar: Auch bei Positivdaten zu Verträgen über Mobilfunkdienste und Dauerhandelskonten kommt den Interessen, Grundrechten und Grundfreiheiten der betroffenen Person, selbst darüber zu bestimmen, ob sie die sie betreffenden Positivdaten für eine Übermittlung durch Mobilfunkdienstleister und Handelsunternehmen und eine Verarbeitung durch Auskunfteien zur Bonitätsbewertung preisgeben will, entscheidende Bedeutung zu. Hierbei fällt besonders ins Gewicht, dass ansonsten unterschiedslos große Datenmengen über übliche Alltagsvor-gänge im Wirtschaftsleben erhoben und verarbeitet würden, ohne dass die betroffenen Personen hierzu Anlass gegeben haben. Deshalb können weder Verantwortliche noch Dritte ein überwiegendes Interesse an diesen Verarbeitungen geltend machen.

Eine gegen den Willen der betroffenen Person stattfindende Datenverarbeitung von Positivdaten über Mobilfunkdienstverträge und Dauerhandelskonten durch Vertragspartner und Auskunfteien ist daher unbeschadet anderweitiger Anforderungen nicht nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO gerechtfertigt. Ihre datenschutzkonforme Übermittlung und Verarbeitung ist nur auf der Grundlage einer Einwilligung der betroffenen Person zulässig, für die die allgemeinen Anforderungen gewahrt werden müssen. Insbesondere darf die Erteilung der Einwilligung in die Speicherung

des Positivdatums nicht zur Bedingung des betroffenen Vertragsabschlusses gemacht werden.

- **19.10.2021 – Verarbeitungen des Datums „Impfstatus“ von Beschäftigten durch die Arbeitgeberin oder den Arbeitgeber**

  Arbeitgeberinnen und Arbeitgeber dürfen das Datum „Impfstatus“ ihrer Beschäftigten ohne eine ausdrückliche gesetzliche Ermächtigung grundsätzlich nicht verarbeiten – auch nicht im Rahmen der COVID-19-Pandemie.

  Als Rechtsgrundlage kommt für die Verarbeitung des Datums „Impfstatus“ von Beschäftigten § 26 Absatz 3 Satz 1 des Bundesdatenschutzgesetzes (BDSG) nicht zum Tragen.

  Bei dem Datum „Impfstatus“ handelt es sich um ein Gesundheitsdatum gemäß Artikel 4 Nummer 15 Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DS-GVO) und damit um eine besondere Kategorie personenbezogener Daten, Artikel 9 Absatz 1 DS-GVO. Deren Verarbeitung ist grundsätzlich verboten und nur ausnahmsweise erlaubt.

  In Einzelfällen ist eine Verarbeitung des Datums „Impfstatus“ auf Grundlage gesetzlicher Regelungen möglich:

  - Bestimmte – im Gesetz genannte – Arbeitgeberinnen und Arbeitgeber aus dem Gesundheitsbereich (Krankenhäuser, Arztpraxen usw.) dürfen unter den in §§ 23a, 23 Absatz 3 des Infektionsschutzgesetzes (IfSG) genannten gesetzlichen Voraussetzungen den Impfstatus ihrer Beschäftigten verarbeiten;
  - Bestimmte – im Gesetz genannte – Arbeitgeberinnen und Arbeitgeber, zum Beispiel Trägerinnen und Träger von Kindertageseinrichtungen, ambulante Pflegedienste usw., dürfen unter den in § 36 Absatz 3 IfSG genannten Voraussetzungen den Impfstatus ihrer Beschäftigten im Zusammenhang mit COVID-19 verarbeiten;

- Arbeitgeberinnen und Arbeitgeber dürfen den Impfstatus derjenigen Beschäftigten verarbeiten, die ihnen gegenüber einen Anspruch auf Geldentschädigung (Lohnersatz) nach § 56 Absatz 1 IfSG geltend machen. Dessen Voraussetzungen können im Einzelfall auch im Fall einer möglichen Infektion mit COVID-19 sowie einer sich anschließenden Quarantäne vorliegen. Anspruchsvoraussetzung ist unter anderem, ob die Möglichkeit einer Schutzimpfung bestand.
- Arbeitgeberinnen und Arbeitgeber dürfen den Impfstatus von Beschäftigten auch verarbeiten, soweit dies durch Rechtsverordnungen zur Pandemiebekämpfung auf Basis des IfSG vorgegeben ist.

Die Verarbeitung des Datums „Impfstatus“ von Beschäftigten auf der Grundlage von Einwilligungen ist nur dann möglich, wenn die Einwilligung freiwillig und damit rechtswirksam erteilt worden ist, § 26 Absatz 3 Satz 2 und Absatz 2 BDSG. Aufgrund des zwischen Arbeitgeberinnen und Arbeitgebern sowie ihren Beschäftigten bestehenden Über- und Unterordnungsverhältnisses bestehen regelmäßig Zweifel an der Freiwilligkeit und damit Rechtswirksamkeit der Einwilligung von Beschäftigten.

Im Zusammenhang mit der Abfrage des Datums „Impfstatus“ sind weiter zu beachten:

- Grundsatz der „Datenminimierung“, Artikel 5 Absatz 1 Buchstabe c DS-GVO: Zunächst muss geprüft werden, ob die reine Abfrage des Impfstatus zur Zweckerreichung bereits ausreichend ist. Dann ist keine Speicherung erforderlich. Soll der Impfstatus gespeichert werden, dürfen keine Kopien von Impfausweisen oder vergleichbaren Bescheinigungen (im Original oder als Kopie) in die Personalakte aufgenommen werden. Es ist ausreichend, wenn vermerkt wird, dass diese jeweils vorgelegt worden sind.
- Grundsatz der „Speicherbegrenzung“, Artikel 5 Absatz 1 Buchstabe e DS-GVO, Recht auf Löschung, Artikel 17 DS-GVO: Sobald der Zweck für die Speicherung des Impfstatus

entfallen ist, muss dieses personenbezogene Datum gelöscht werden.
- Grundsatz der „Rechenschaftspflicht“, Artikel 5 Absatz 2 DS-GVO: Arbeitgeberinnen und Arbeitgeber müssen – sofern einschlägig – auch die Freiwilligkeit einer Einwilligung nachweisen können, Artikel 7 Absatz 1 DS-GVO.

- **24.11.2021 – Zur Möglichkeit der Nichtanwendung technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO auf ausdrücklichen Wunsch betroffener Personen[1]**

  1. Die vom Verantwortlichen nach Art. 32 DSGVO vorzuhaltenden technischen und organisatorischen Maßnahmen beruhen auf objektiven Rechtspflichten, die nicht zur Disposition der Beteiligten stehen.
  2. Ein Verzicht auf die vom Verantwortlichen vorzuhaltenden technischen und organisatorischen Maßnahmen oder die Absenkung des gesetzlich vorgeschriebenen Standards auf der Basis einer Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO ist nicht zulässig.
  3. Unter Beachtung des Selbstbestimmungsrechts der betroffenen Person und der Rechte weiterer betroffener Personen kann es in zu dokumentierenden Einzelfällen möglich sein, dass der Verantwortliche auf ausdrücklichen, eigeninitiativen Wunsch der informierten betroffenen Person bestimmte vorzuhaltende technische und organisatorische Maßnahmen ihr gegenüber in vertretbarem Umfang nicht anwendet.
  4. Kapitel V der DSGVO (Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen) bleibt hiervon unberührt.

[1] Der Beschluss wurde durch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder gegen die Stimme Sachsens beschlossen.

# Anhang zum Beitrag 10.1 Datenschutzprüfung von Energieversorgungsunternehmen

## 1. Allgemeine Informationen

- Name, Rechtsform, Anschrift Ihres Unternehmens:
- Ansprechpartner (Name, Funktion, Telefon, E-Mail)
- Datenschutzbeauftragter (Name, Telefon, E-Mail)

## 2. Datenschutzorganisation

2.1 Welche Unternehmensbereiche sind mit dem Thema Datenschutz betraut?

2.2 Beschreiben Sie bitte das Zusammenwirken der einzelnen Stellen in datenschutzrechtlichen Angelegenheiten unter Beifügung eines aussagekräftigen Organigramms

2.3 Sofern es einen Datenschutzbeauftragten gibt, wie und in welcher Häufigkeit berichtet er an die Geschäftsführung?

## 3. Umsetzung der DS-GVO

3.1 Welche Unternehmensbereiche waren oder sind maßgeblich in die Umsetzung der DS-GVO involviert?

3.2 Kreuzen Sie bitte die wesentlichen Maßnahmen an, die Sie im Rahmen der Umsetzung getroffen haben.

- ☐ Sensibilisierungsmaßnahmen
- ☐ interne Datenschutz-Richtlinie
- ☐ Erstellung von Datenschutzhinweisen zur Erfüllung der Informationspflicht
- ☐ Löschkonzept
- ☐ Neuverhandlung Auftragsverarbeitungsverträge
- ☐ Prozess Datenschutz-Folgenabschätzung
- ☐ Anpassung und Erweiterung interner Vorgaben zur Dokumentation

- ☐ Dokumentation der Umsetzung der DS-GVO
- ☐ Überarbeitung/Erstellung von Betriebsvereinbarungen
- ☐ Benennung eines internen bzw. Beauftragung eines externen Datenschutzbeauftragten
- ☐ Prozesse für Betroffenenrechte
- ☐ Prozesse für Beschwerdebearbeitung
- ☐ Prüfung vertraglicher Grundlagen für internationalen Datentransfer
- ☐ Überprüfung/Neuverhandlung der Verträge mit externen Dienstleistern
- ☐ Dokumentation der internen Datenschutzorganisation
- ☐ Prozess für die Meldung von Datenpannen
- ☐ Sonstige:

3.3 Erläutern Sie bitte kurz den Umsetzungsstatus, falls noch nicht bzw. nicht vollständig umgesetzt. Benennen Sie bitte auch die Gründe.

3.4 Hat Ihre Internen Revision oder eine vergleichbare Einheit die Einführung und Umsetzung der DS-GVO in Ihrem Unternehmen geprüft?

**4. Zulässigkeit der Datenverarbeitung**

4.1 Bitte listen Sie die wesentlichen unternehmensspezifischen Datenverarbeitungen auf und ordnen Sie diesen die Rechtsgrundlagen zu, auf die Sie die Verarbeitung personenbezogener Daten stützen (Artikel 6, 9 DS-GVO inklusive Spezialnormen).

4.2 Sofern Sie auf Basis von Einwilligungen personenbezogene Daten verarbeiten, fügen Sie bitte exemplarisch Ihr(e) Muster bei.

**5. Beschwerde-Bearbeitung**

5.1 Listen Sie bitte die mit der Bearbeitung datenschutzrechtlicher Beschwerden befassten Stellen Ihres Unternehmens auf.

5.2 Anhand welcher Kriterien stuft Ihr Unternehmen die Rückmeldung eines Kunden als datenschutzrechtliche Beschwerde ein (Beschwerdedefinition)?

5.3 Wie unterscheidet sich die Bearbeitung einer datenschutzrechtlichen Beschwerde von der Bearbeitung einer sonstigen Beschwerde?

**6. Betroffenenrechte**

6.1 Wie stellen Sie sicher, dass den Betroffenenrechten auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Nachberichtspflicht und Datenübertragbarkeit angemessen nachgekommen wird? Bitte kreuzen Sie zutreffendes an.

- ☐ Regelungen der Verantwortlichkeiten, Zuständigkeiten und des Kommunikationsverlaufs im Unternehmen
- ☐ Prozesse zur Beantwortung von Anfragen der Betroffenen (einschließlich Erkennen als Anfrage zu einem Betroffenenrecht z. B. durch Schlüsselwörter, Identifikation der Betroffenen, Bearbeitungsdauer, Rückmeldung an Betroffene u.a.)
- ☐ Verwenden von Mustern für Antwortschreiben
- ☐ Prozesse zur Sicherstellung der Einhaltung von Fristen
- ☐ Prozesse zur Nachverfolgung des Fortschritts der Bearbeitung
- ☐ Verfahren zur Reaktion, wenn ein(e) Betroffene(r) mit der Beantwortung nicht zufrieden ist
- ☐ Sensibilisierung der Mitarbeiter

6.2 Skizzieren Sie bitte überblicksartig Ihre wesentlichen Prozesse zu den o.g. Betroffenenrechten. Legen Sie bitte möglichst Nachweise (z. B. Verfahrensbeschreibungen, Mustertexte etc.) bei, die eine Überprüfung Ihrer Angaben ermöglichen.

6.3 Wie kommen Sie Ihren Informationspflichten gegenüber Kunden gem. Art. 13 bzw. 14 DS-GVO nach (z.B. Homepage, Postversand, E-Mail-Link, Aushang)? Bitte fügen Sie exemplarisch Ihre Muster-Texte bei.

6.4 Zu welchem Zeitpunkt informieren Sie Ihre Kunden i.S.v. 6.3?

6.5 Wie werden Missstände und Schwachstellen im Umgang mit Betroffenenrechten kontinuierlich verbessert und die Verbesserungsmaßnahmen auf ihre Wirksamkeit hin überprüft?

**7. Sensibilisierungsmaßnahmen**

7.1 Stellen Sie sicher, dass Ihre Mitarbeiterinnen und Mitarbeiter für den Umgang mit personenbezogenen Daten hinreichend sensibilisiert sind?

☐ Ja
☐ Nein

7.2 Benennen Sie, wenn zutreffend, die wesentlichen Sensibilisierungsmaßnahmen und machen Sie Angaben zum Ausführungsturnus.

**8. Rechenschaftspflicht**

8.1 Wie können Sie die Einhaltung der Grundsätze der Datenverarbeitung nachweisen? Benennen Sie die Art der Dokumentation, die Sie für diesen Zweck vorhalten.

8.2 Welche Aspekte bereiten ggf. Schwierigkeiten?

**9. Bereichsspezifische Fragen (Versorgungswirtschaft)**

9.1 Werden Informationssysteme geführt, welche personenbezogene Hinweise zu den jeweiligen Kunden speichern, wie z.B. das Wechselverhalten der Kunden?

9.2 Findet ein Abgleich/Austausch von personenbezogenen Daten (wie z.B. Zahlungsverhalten, Vertragstreue) mit anderen Energieversorgungsunternehmen statt? Wenn ja, auf welche Rechtsgrundlage wird dieser Abgleich/Austausch gestützt?

**10. Sonstiges**

Haben Sie Anregungen an die Aufsicht?