**BREMISCHE BÜRGERSCHAFT** **Drucksache 21/341**
Landtag 18.03.2024
21. Wahlperiode

# **Bericht** der Landesbeauftragten für Datenschutz

## 6. Jahresbericht der Landesbeauftragten für Datenschutz nach der Europäischen Datenschutzgrundverordnung über den Datenschutz im Jahr 2023 im Land Bremen

Hiermit erstatte ich der Bürgerschaft (Landtag) und dem Präsidenten des Senats meinen Bericht im Sinne des Artikels 59 der Europäischen Datenschutzgrundverordnung über das Ergebnis der Tätigkeit im Jahr 2023.

Redaktionsschluss war der 31. Dezember 2023.

Dr. Imke Sommer

Die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen

**Inhaltsverzeichnis**

## 1. Über kurz oder lang gewinnt Europa!

Zu Beginn der Adventszeit hat der Europäische Gerichtshof (EuGH) den Bundesgesetzgeber in die Schranken gewiesen und unmissverständlich klargestellt, dass Datenschutz europäisch gedacht werden muss. Dies war das dritte Mal im Berichtsjahr. Inzwischen hat es den Anschein, dass der EuGH einen Paragrafen nach dem anderen aus dem Bundesdatenschutzgesetz (BDSG) tilgt. Die Begründung läuft jeweils darauf hinaus, dass der deutsche Gesetzgeber mit dem BDSG die Grenzen seiner Gesetzgebungsbefugnis überschritten und/oder Regelungen formuliert hat, die das Datenschutzniveau der Europäischen Datenschutzgrundverordnung unterschreiten oder – im Fall der sogenannten Schufa-Entscheidung – zumindest alles darauf hindeutet, dass eine Regelung des BDSG den europarechtlichen Anforderungen nicht genügt. Diese Tendenz war in Bezug auf die BDSG-Regelung zur privaten Videoüberwachung bereits im Jahr 2019 vom Bundesverwaltungsgericht vorweggenommen worden, das erklärt hatte, aufgrund der fehlenden Gesetzgebungsbefugnis des deutschen Gesetzgebers sei "kein Raum für die künftige Anwendung" der entsprechenden Regelung. Die anstehende Evaluierung des BDSG bietet dem Bundesgesetzgeber die Möglichkeit, die vom EuGH monierten Regelungen zu streichen und proaktiv auch auf weitere Regelungen zu verzichten, um es dem EuGH und dem Ansehen Deutschlands als Land mit einem ausgeprägten Grundrechtsschutz zu ersparen, Paragraf für Paragraf für europarechtswidrig erklären zu müssen.

### 1.1 "Deutsche Wohnen SE" – Unternehmen haften für Datenschutzverstöße aller Beschäftigten

Am 5. Dezember 2023 kassierte der Europäische Gerichtshof (EuGH) den Verweis auf § 30 Ordnungswidrigkeitengesetz (OWiG) in § 41 Absatz 1 Bundesdatenschutzgesetz (BDSG). Der EuGH entschied, dass die Verhängung von Geldbußen nach Artikel 83 Datenschutzgrundverordnung (DSGVO) gegen datenschutzrechtlich verantwortliche Unternehmen nicht davon abhängt, dass eine oder mehrere von der datenschutzrechtlichen Aufsichtsbehörde identifizierte natürliche Leitungspersonen gegen die DSGVO verstoßen haben. Vielmehr reicht es aus, dass eine im Namen des Unternehmens handelnde Person einen vorsätzlichen oder fahrlässigen Verstoß gegen die DSGVO begangen hat. Eine datenschutzrechtliche Haftung von Unternehmen besteht dabei schon dann, wenn sich die verantwortlichen Stellen über die Rechtswidrigkeit ihres Verhaltens "nicht im Unklaren sein konnten", unabhängig davon, ob ihnen dabei bewusst war, dass sie gegen die Vorschriften der DSGVO verstießen. Mit dieser Entscheidung bestätigte der EuGH die Sanktionspraxis der bremischen Datenschutzaufsichtsbehörde: Unternehmen haften in datenschutzrechtlicher Hinsicht für Datenschutzverstöße aller Beschäftigten, sofern diese nicht im sogenannten Beschäftigtenexzess zu eigenen Zwecken handeln.

Der Bundesgesetzgeber sollte darüber hinaus die Äußerung des EuGH in Randnummer 48 der Entscheidung zum Anlass nehmen, den kompletten Absatz 1 des § 41 BDSG zu streichen. Dieser Absatz will deutsche datenschutzrechtliche Aufsichtsbehörden verpflichten, materiellrechtliche Regelungen des OWiG sinngemäß anzuwenden, wenn sie Geldbußen nach der DSGVO verhängen. Im Urteil heißt es: "Die Tatsache, dass die DSGVO den Mitgliedstaaten (…) die Möglichkeit einräumt, Anforderungen an das von den Aufsichtsbehörden anzuwendende Verfahren bei der Verhängung einer Geldbuße vorzusehen, bedeutet jedoch keineswegs, dass sie auch befugt wären, über diese verfahrensrechtlichen Anforderungen hinaus materielle Voraussetzungen vorzusehen (…). Des Weiteren wird (…) bestätigt, dass er (der Unionsgesetzgeber, I.S.) den Mitgliedstaaten insoweit keinen Ermessensspielraum gelassen hat. Für diese materiellen Voraussetzungen gilt daher ausschließlich das Unionsrecht." Dies bedeutet, dass der deutsche Gesetzgeber auf keine der materiellrechtlichen Regelungen im deutschen Ordnungswidrigkeitengesetz verweisen durfte und darf, ohne gegen Europarecht zu verstoßen.

## 1.2 "Schufa"-Entscheidung: Die maßgeblich vertragsrelevante Nutzung von Wahrscheinlichkeitswerten ist als "automatisierte Entscheidung" rechtswidrig

Am 7. Dezember 2023 entschied der Europäische Gerichtshof (EuGH) über die Vereinbarkeit des von der Schufa errechneten Wahrscheinlichkeitswertes mit der Datenschutzgrundverordnung (DSGVO) und formulierte bei dieser Gelegenheit strenge Voraussetzungen an mitgliedstaatliche Normen, die einen europarechtlich zulässigen Rahmen für die Nutzung von Wahrscheinlichkeitswerten bieten könnten. Diese Voraussetzungen können offensichtlich nicht von der entsprechenden Regelung im Bundesdatenschutzgesetz (BDSG) erfüllt werden.

Unter Verweis auf die Sachverhaltsfeststellungen des Verwaltungsgerichts Wiesbaden geht der EuGH davon aus, dass ein unzureichender Schufa-Wahrscheinlichkeitswert der Menschen, die Kreditanträge stellen, in nahezu allen Fällen dazu führt, dass diese Kreditanträge von Banken abgelehnt werden. Damit hängt von diesem Wahrscheinlichkeitswert "maßgeblich" ab, ob Vertragsverhältnisse mit diesen Personen begründet, durchführt oder beendet werden. Aufgrund dieses maßgeblichen Einflusses des die Zahlungsfähigkeit prognostizierenden Wahrscheinlichkeitswerts ist dessen Nutzung als "automatisierte Entscheidung" rechtswidrig, wenn dieser Wert automatisiert durch eine Wirtschaftsauskunftei erstellt und den über den Kreditantrag entscheidenden Banken übermittelt worden ist. Dass es eine nicht bei der Schufa beschäftigte Person ist, die die Kreditentscheidung mitteilt, ändert nach Auffassung des EuGH also nichts daran, dass die

durch den Schufa-Wert maßgeblich beeinflusste Kreditentscheidung als "automatisierte Entscheidung" anzusehen und damit rechtswidrig ist.

Der EuGH weist in dieser Entscheidung auch auf die "durchgreifenden" Bedenken des Verwaltungsgerichts Wiesbaden gegen die Vereinbarkeit des § 31 BDSG mit der DSGVO hin, der Anforderungen an die Verwendung von Wahrscheinlichkeitswerten formuliert. Hierzu heißt es in der Entscheidung, dass mitgliedstaatliche Rechtsvorschriften, die den Erlass einer automatisierten Entscheidung im Einzelfall erlauben, angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten und den Anforderungen der Basisartikel 5 und 6 der DSGVO entsprechen müssen und dass es das Verwaltungsgericht Wiesbaden selbst ist, das prüfen muss, ob diese Voraussetzungen erfüllt sind. Angesichts des laufenden Evaluationsprozesses sollte der Bundesgesetzgeber nicht zögern, § 31 BDSG schon nach diesen Hinweisen des EuGH europarechtskonform zu verändern oder zu streichen.

## 1.3 Wir brauchen ein europafestes Beschäftigtendatenschutzgesetz!

Schon am 30. März 2023 hatte der Europäische Gerichtshof (EuGH) dem Verwaltungsgericht Wiesbaden unumstößliche Argumente geliefert, den mit § 26 Absatz 1 Bundesdatenschutzgesetz identischen § 23 Absatz 1 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes (HDSIG) wegen Unvereinbarkeit mit der Datenschutzgrundverordnung (DSGVO) nicht anzuwenden. Zwar können die mitgliedstaatlichen Gesetzgeber "spezifischere Vorschriften" zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext vorsehen. Dazu dürfen die mitgliedstaatlichen Regelungen jedoch den Text der DSGVO nicht lediglich wiederholen, sondern müssen "einen zu dem geregelten Bereich passenden Regelungsgehalt haben (…), der sich von den allgemeinen Regeln der DSGVO unterscheidet, müssen (…) auf den Schutz der Rechte und Freiheiten der Beschäftigten hinsichtlich der Verarbeitung ihrer personenbezogenen Daten im Beschäftigungskontext abzielen und geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person umfassen. Dabei ist insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und die Überwachungssysteme am Arbeitsplatz vorzugehen." Nach Formulierung dieser fundamentalen Voraussetzungen mitgliedstaatlicher Regelungen weist der EuGH darauf hin, dass Bestimmungen "wie § 23 Absatz 1 HDSIG" die in der DSGVO aufgestellte Bedingung für die allgemeine Rechtmäßigkeit der Verarbeitung zu wiederholen scheinen, ohne eine spezifischere Vorschrift im Sinne von Artikel 88 Absatz 1 DSGVO hinzuzufügen. Eine bessere Steilvorlage für die schnelle Verabschiedung eines von der Konferenz der unabhängigen

Datenschutzaufsichtsbehörden des Bundes und der Länder seit langer Zeit geforderten Beschäftigtendatenschutzgesetzes konnte der EuGH nicht liefern!

## 1.4 Europäischer Gerichtshof zu Protokolldaten

Am 22. Juni 2023 entschied der Europäischer Gerichtshof (EuGH) in der Rechtssache C-579/21 über einen von einem finnischen Gericht vorgelegten Sachverhalt zum Thema Offenlegungspflicht für Protokolldateien. Im Land Bremen war die Frage, ob sich das Auskunftsrecht Betroffener auch auf Protokolldaten über Abfragen in polizeilichen Datenbanken bezieht, im Berichtsjahr und in den Vorjahren diskutiert worden. Leider lagen der Landesbeauftragten für Datenschutz und Informationsfreiheit (LfDI), die in dieser Sache im August selbst vor dem Verwaltungsgericht Bremen erschien, die Informationen über dieses einmal wieder datenschutzfreundliche Urteil des EuGH noch nicht vor, sodass sie dieses nicht in die Verhandlung einbrachte. Ob das Verwaltungsgericht anderenfalls der Auffassung der LfDI gefolgt wäre, werden wir nie erfahren.

Hier sei gleichwohl die Argumentation des EuGH wiedergegeben: Das Auskunftsrecht nach Artikel 15 Absatz 1 Datenschutzgrundverordnung bezieht sich auch auf "Informationen, die Abfragen personenbezogener Daten einer Person betreffen und die sich auf den Zeitpunkt und die Zwecke dieser Vorgänge beziehen. (…) Dagegen sieht diese Bestimmung kein solches Recht in Bezug auf Informationen über die Identität der Arbeitnehmer dieses Verantwortlichen vor, die diese Vorgänge unter seiner Aufsicht und im Einklang mit seinen Weisungen ausgeführt haben, außer wenn diese Informationen unerlässlich sind, um der betroffenen Person es zu ermöglichen, die ihr durch diese Verordnung verliehenen Rechte wirksam wahrzunehmen, und vorausgesetzt, dass die Rechte und Freiheiten dieser Arbeitnehmer berücksichtigt werden."

## 1.5 Ausblick

Die Landesbeauftragte für Datenschutz und Informationsfreiheit, die mittlerweile fast 15 Jahre datenschutzpolitische Diskussionen überblickt, ist zuversichtlich, dass sich der auch an den datenschutzbezogenen Entscheidungen des Europäischen Gerichtshofes des Jahres 2023 ablesbare Trend fortsetzen wird: Im Land Bremen, bundesweit und überall in der Europäischen Union ist nur der genaue Zeitpunkt unklar, an dem das europäische Grundrecht auf Datenschutz gewinnt!

Dr. Imke Sommer

## 2. Zahlen und Fakten

Die Datenschutzgrundverordnung macht es den Aufsichtsbehörden in Artikel 59 zur Pflicht, jährlich über ihre Tätigkeit zu berichten. Um die Transparenz und Vergleichbarkeit innerhalb der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) und für die Öffentlichkeit zu erhöhen, hat die DSK beschlossen, in die jeweiligen Tätigkeitsberichte ein zusätzliches Kapitel aufzunehmen, in dem nach gemeinsam vereinbarten Kriterien Informationen zu bestimmten Kennwerten der jeweiligen Aufsichtsbehörde aufgeführt sind. Die vereinbarten Kriterien sind Beschwerden (siehe Ziffer 2.2 dieses Berichts), Beratungen (siehe Ziffer 2.3 dieses Berichts), Meldungen von Datenschutzverletzungen (siehe Ziffer 2.4 dieses Berichts), Abhilfemaßnahmen (siehe Ziffer 2.5 dieses Berichts), europäische Verfahren (siehe Ziffer 2.6 dieses Berichts) und förmliche Begleitung von Rechtsetzungsvorhaben (siehe Ziffer 2.7 dieses Berichts). Zusätzlich berichten wir über Meldungen über die Bestellung behördlicher und betrieblicher Datenschutzbeauftragter (siehe Ziffer 2.8 dieses Berichts), die datenschutzrechtliche Zertifizierung (siehe Ziffer 2.9 dieses Berichts) und das europäische Binnenmarkt-Informationssystem (siehe Ziffer 2.10 dieses Berichts).

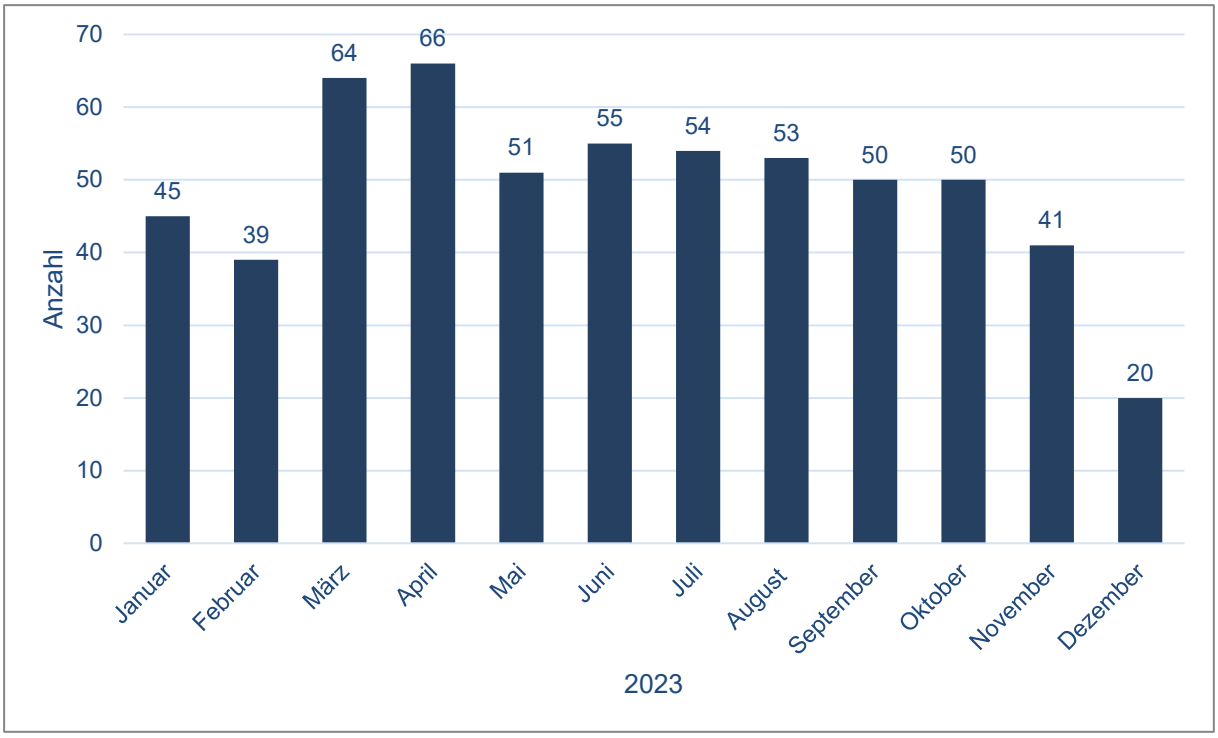
### 2.1 Auswahl datenschutzrelevanter Sachverhalte, die 2023 an die Landesbeauftragte für Datenschutz und Informationsfreiheit herangetragen wurden

| Monat | Beschwerden | Beratungs-anfragen | Meldungen Datenschutz-verletzungen | Meldungen Datenschutz-beauftragte |
|---|---|---|---|---|
| Januar | 45 | 22 | 13 | 46 |
| Februar | 39 | 28 | 13 | 20 |
| März | 64 | 29 | 19 | 28 |
| April | 66 | 32 | 10 | 38 |
| Mai | 51 | 29 | 13 | 15 |
| Juni | 55 | 27 | 22 | 43 |
| Juli | 54 | 27 | 21 | 25 |
| August | 53 | 29 | 6 | 46 |
| September | 50 | 35 | 16 | 17 |
| Oktober | 50 | 22 | 12 | 24 |
| November | 41 | 43 | 22 | 22 |
| Dezember | 20 | 18 | 9 | 24 |
| **Gesamt** | **588** | **341** | **176** | **348** |

Tabelle 1

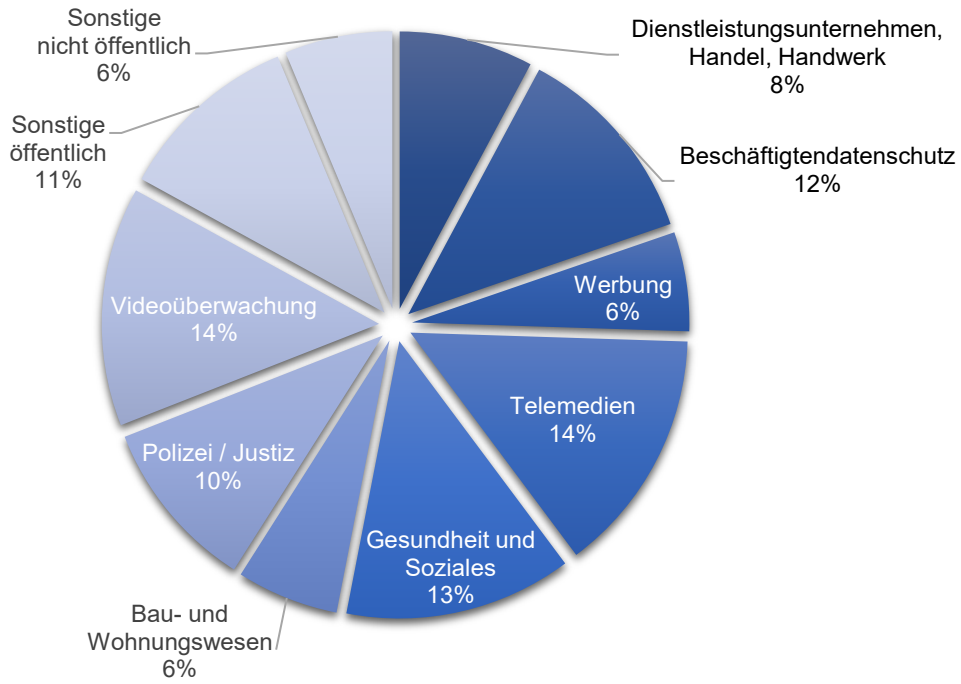
Nähere Angaben hierzu finden sich in den nachfolgenden Ziffern.

## 2.2 Beschwerden




Säulendiagramm 1

In diesem Diagramm sind die monatlichen Beschwerdezahlen des Jahres 2023 dargestellt.




Tortendiagramm 1

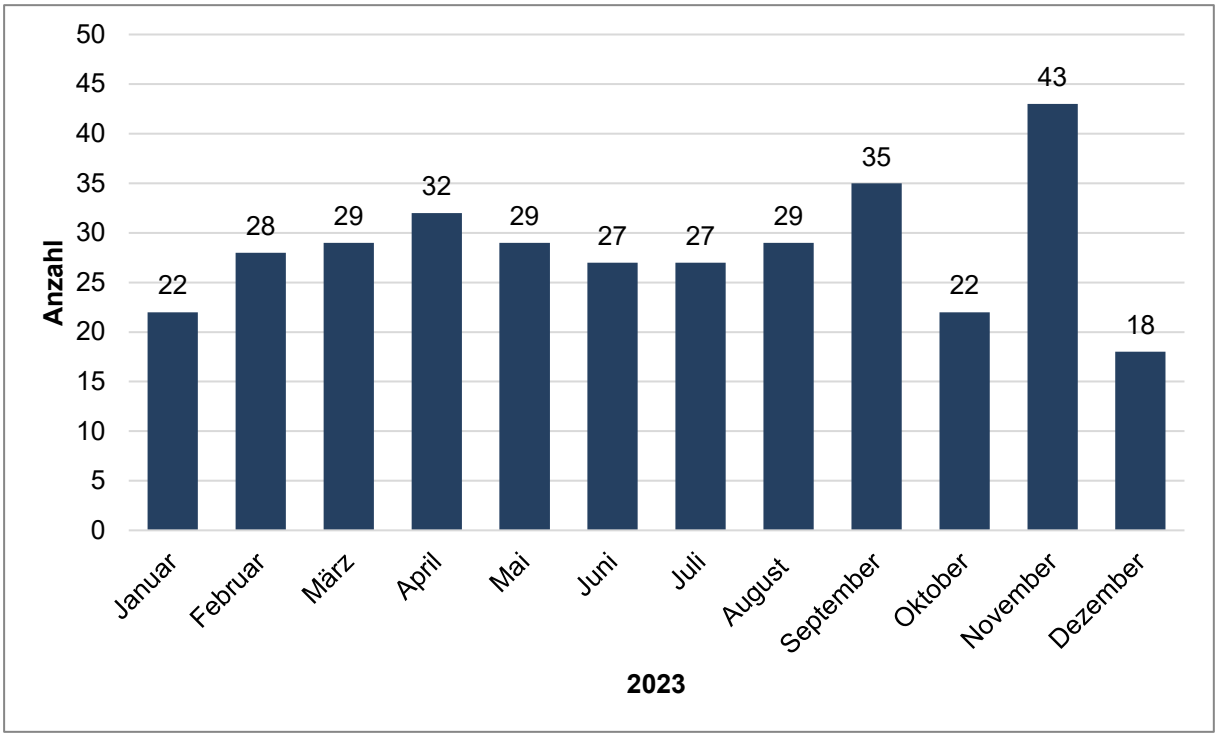
Das Diagramm zeigt die bei der Landesbeauftragten für Datenschutz und Informationsfreiheit eingegangenen Beschwerden im gesamten Jahr 2023 nach Themengebieten aufgeschlüsselt.

| Themengebiet | Absoluter Wert | Relativer Wert |
|---|---|---|
| Dienstleistungsunternehmen, Handel, Handwerk | 46 | 8 % |
| Beschäftigtendatenschutz | 70 | 12 % |
| Werbung | 34 | 6 % |
| Telemedien | 84 | 14 % |
| Gesundheit und Soziales | 78 | 13 % |
| Bau- und Wohnungsunternehmen | 35 | 6 % |
| Polizei / Justiz | 59 | 10 % |
| Videoüberwachung | 82 | 14 % |
| Sonstiges (nicht öffentlich) | 37 | 6 % |
| Sonstiges (öffentlich) | 63 | 11 % |

Tabelle 2

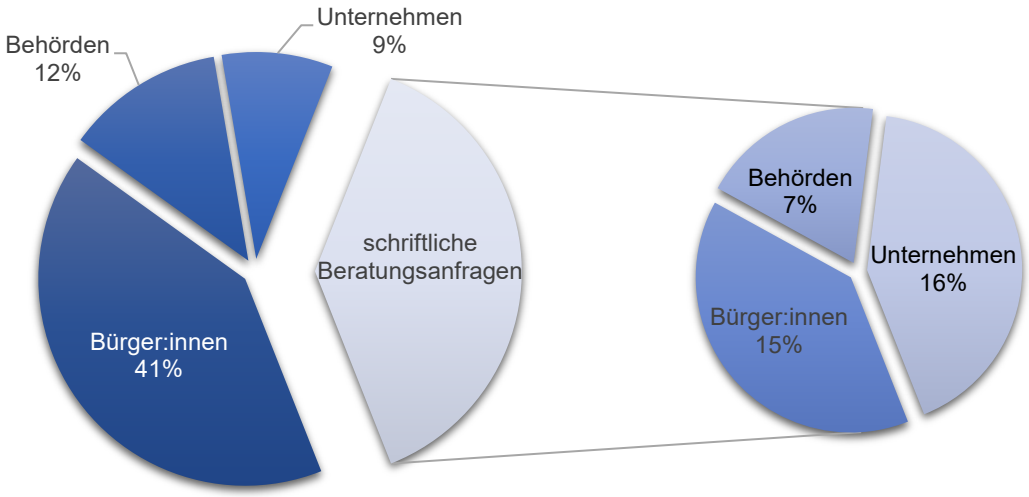
Die Tabelle stellt die absoluten Werte und relativen Werte der unterschiedlichen Themengebiete der Beschwerden dar.

## 2.3 Beratungen




Säulendiagramm 2

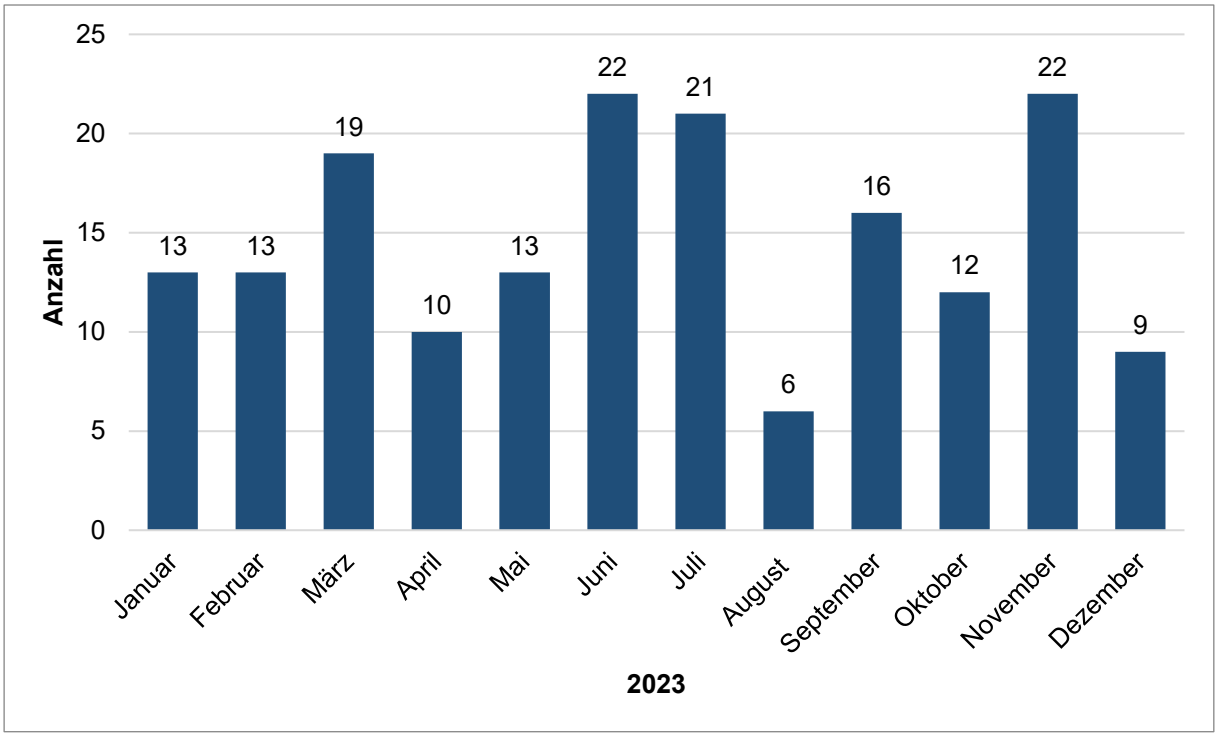
Diese Grafik gibt eine Übersicht über die Anzahl von schriftlichen und telefonischen Beratungen von Verantwortlichen und betroffenen Personen.




Tortendiagramm 2

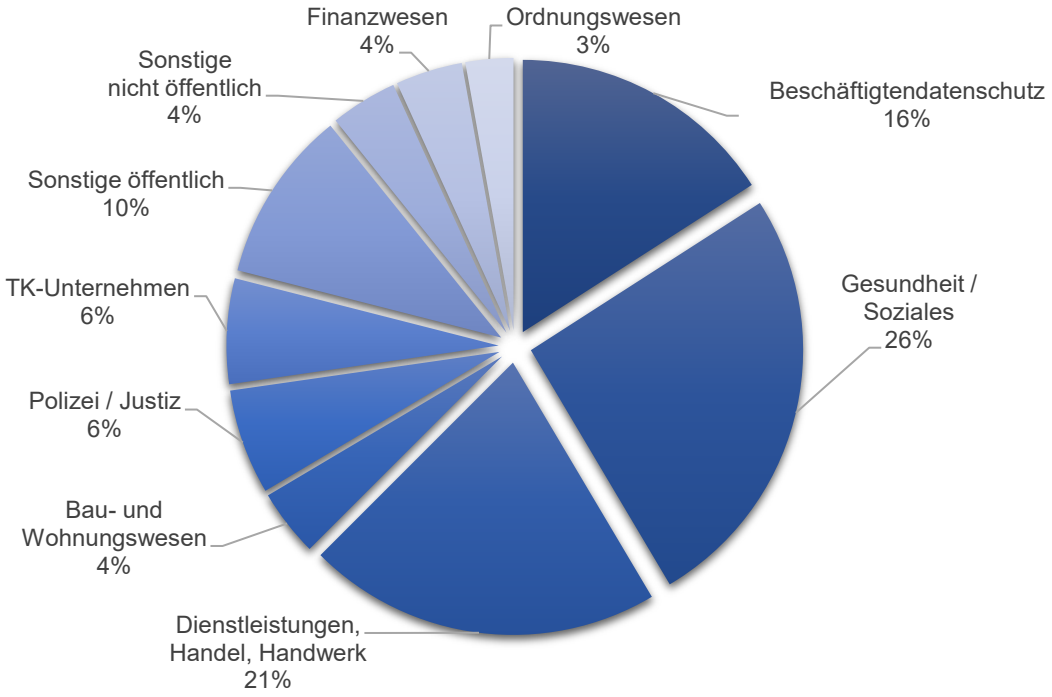
Dieses Tortendiagramm stellt die telefonischen und schriftlichen Beratungen im Jahr 2023 dar. Differenziert wird dabei zwischen telefonischen und schriftlichen Beratungsanfragen. Daneben wird danach unterschieden, wer Beratungsanfragen stellt. Dies sind zum einen die Verantwortlichen (Behörden und Unternehmen) und andererseits die von der Verarbeitung personenbezogener Daten betroffenen Grundrechtsträgerinnen und Grundrechtsträger.

## 2.4 Meldungen von Datenschutzverletzungen




Säulendiagramm 3

In dieser Grafik sind die monatlichen Meldungen von Datenschutzverletzungen nach Artikel 33 Datenschutzgrundverordnung im Jahr 2023 dargestellt.




Tortendiagramm 3

Diese Darstellung schlüsselt die gemeldeten Datenschutzverletzungen für das Jahr 2023 nach Themengebieten auf.

## 2.5 Abhilfemaßnahmen

**Warnungen**

nach Artikel 58 Absatz 2 a DSGVO: Keine

**Verwarnungen**

nach Artikel 58 Absatz 2 b DSGVO: 20

**Anweisungen und Anordnungen**

nach Artikel 58 Absatz 2 c-g DSGVO und § 85 BremPolG: Sechs

**Geldbußen**

nach Artikel 58 Absatz 2 i DSGVO: 30

**Widerruf von Zertifizierungen**

nach Artikel 58 Absatz 2 h DSGVO: Keine

### 2.5.1 Anfrage nach sämtlichen bisher erlassenen Maßnahmen nach Artikel 58 Datenschutzgrundverordnung

Im August des Berichtsjahrs bat uns ein Antragsteller nach den Bestimmungen des Informationsfreiheitsrechts, ihn über sämtliche Maßnahmen, die wir nach Artikel 58 Datenschutzgrundverordnung verfügten, zu informieren. Zu diesem Antrag konnten wir dem Antragsteller Folgendes mitteilen:

**Warnungen (gegen)**

**2019**

- eine politische Partei ausgesprochen, weil von ihr geplante Datenverarbeitungen voraussichtlich gegen die Datenschutzgrundverordnung verstoßen würden

**2020**

- eine Krankenkasse wegen technisch-organisatorischer Mängel bei der Bereitstellung einer elektronischen Patientenakte

**2021**

- ein Mitglied eines Beirats wegen unzulässiger Veröffentlichung von Behördenschreiben und Videomitschnitten

**2023**

- ein Industrieunternehmen wegen unzulässiger Datenverarbeitung

**Verwarnungen (gegen)**
**(spätere Verhängung einer Geldbuße nach Artikel 83 DSGVO ist zusätzlich möglich)**

**2018**

- ein Dienstleistungsunternehmen wegen unzulässiger Übermittlung von Kund:innendaten an eine Datenbank
- ein Dienstleistungsunternehmen wegen unzulässiger Kund:innenkontaktdatenoffenlegung ("offener Mailverteiler")

**2019**

- ein Dienstleistungsunternehmen wegen der Fehladressierung/-Übermittlung von Kund:innedaten
- ein Handelsunternehmen wegen unzulässiger Offenlegung von Kund:innendaten gegenüber Drittem
- ein Dienstleistungsunternehmen wegen unzulässiger Kund:innenkontaktoffenlegung ("offener Mailverteiler")

- ein Dienstleistungsunternehmen wegen des Abdrucks von Kund:innendaten in einem Briefkopf
- eine Arztpraxis wegen unzulässiger Übermittlung von Gesundheitsdaten

**2020**

- ein Dienstleistungsunternehmen wegen unzulässiger Offenlegung von Kund:innendaten
- eine Apotheke wegen technisch-organisatorischer Mängel und Nichteinhaltung der Pflicht zur Meldung einer Datenschutzverletzung
- eine Arztpraxis wegen unzulässiger Verarbeitung von Gesundheitsdaten

**2021**

- einen Verein wegen unbefugter Offenlegung von Mitgliederkontaktdaten
- ein Dienstleistungsunternehmen wegen Fehlversands von Kund:innenunterlagen
- ein Dienstleistungsunternehmen wegen fehlerhafter Mitteilung von Kund:innendaten infolge einer Personenverwechslung
- ein Dienstleistungsunternehmen wegen unbefugter Übermittlung von Kund:innendaten
- ein Dienstleistungsunternehmen wegen Fehlversands von Kund:innenunterlagen
- ein Dienstleistungsunternehmen wegen Fehlversands von Kund:innenunterlagen
- einen Händler wegen unzulässiger Kund:innenkontaktoffenlegung ("offener Mailverteiler")
- ein Dienstleistungsunternehmen wegen Fehlversands von Kund:innenunterlagen
- ein Dienstleistungsunternehmen wegen Fehlversands von Kund:innenunterlagen
- ein Dienstleistungsunternehmen wegen des Mangels an technischen IT-Sicherheitsmaßnahmen
- ein Dienstleistungsunternehmen wegen unzulässiger Zugänglichkeit von Kund:inneninformationen
- einen Händler wegen unzulässiger Kund:innenkontaktoffenlegung ("offener Mailverteiler")
- ein Dienstleistungsunternehmen wegen unzulässigen Umgansg mit Kund:innendaten
- ein Dienstleistungsunternehmen wegen unzulässigen Umgangs mit Kund:innendaten
- ein Unternehmen wegen technisch-organisatorischer Mängel beim Betriebsrat
- einen Pflegedienst wegen mangelnder Dokumentation
- eine Anstalt des öffentlichen Rechts wegen der unzulässigen Speicherung von Gesundheits- und Beschäftigtendaten
- eine Arztpraxis wegen unzulässiger Übermittlung von Patient:innendaten
- eine Arztpraxis wegen unzulässiger Übermittlung von Patient:innendaten
- eine Rechtsanwaltskanzlei wegen des Fehlversands einer E-Mail
- eine Rechtsanwaltskanzlei wegen des Fehversands einer Rechnung

**2022**

- ein Dienstleistungsunternehmen wegen technisch-organisatorischer Mängel
- ein Dienstleistungsunternehmen wegen unzulässiger Übermittlung von Kund:innendaten an Dritten
- einen Händler wegen unzulässiger Weitergabe von Kund:innendaten an Dritten
- ein Dienstleistungsunternehmen wegen unzulässiger Übermittlung von Kund:innendaten
- ein Dienstleistungsunternehmen wegen unzulässiger Übermittlung von Kund:innendaten
- ein Dienstleistungsunternehmen wegen unzulässiger Übermittlung von Kund:innendaten
- ein Dienstleistungsunternehmen wegen unzulässiger Kund:innenkontaktoffenlegung ("offener Mailverteiler")
- ein Dienstleistungsunternehmen wegen technisch-organisatorischer Sicherheitsmängel
- ein Dienstleistungsunternehmen wegen unzulässiger Übermittlung von Kund:innendaten
- ein Dienstleistungsunternehmen wegen unterlassener Löschung von Kund.innendaten
- ein Dienstleistungsunternehmen wegen unzulässiger Übermittlung von Kund:innendaten
- ein Dienstleistungsunternehmen wegen technisch-organisatorischer Sicherheitsmängel
- eine Rechtsanwaltskanzlei wegen des Fehlversands einer E-Mail mit Mitarbeiter:innendaten
- eine Rechtsanwaltskanzlei wegen des Fehlversands einer Rechnung
- eine Rechtsanwaltskanzlei wegen des Fehlversands von Lohnbescheinigungen

**2023**

- eine Pflegeeinrichtung wegen unzulässiger Datenübermittlung von Patient:innendaten)
- eine Rechtsanwaltskanzlei wegen unzulässiger Übersendung von Daten zu einer Forderung
- eine Rechtsanwaltskanzlei wegen technisch-organisatorischer Sicherheitsmängel bei der Übersendung einer E-Mail
- eine Rechtsanwaltskanzlei wegen technisch-organisatorischer Sicherheitsmängel bei der Übersendung einer E-Mail
- eine Rechtsanwaltskanzlei wegen technisch-organisatorischer Sicherheitsmängel bei der Übersendung einer E-Mail

**Anordnungen (gegen)**

**2019**

- eine politische Partei wegen unzulässiger Datenverarbeitung
- einen Bürger zur Unterlassung der Veröffentlichung von Behördenschreiben auf dessen Website

**2020**

- einen Betreiber wegen einer Facebook-Fanpage zur Weiterleitung eines Löschersuchens an Facebook und Bereitstellung von Datenschutzinformationen auf der Fan-Page

**2021**

- eine Privatperson zur Löschung und Unterlassung der Veröffentlichung von Beiratssitzungen auf deren Website

**2022**

- ein Fitnessstudio zur Löschung von Impf- und Genesungsdaten aus der Pandemie
- eine Privatperson zur Löschung und Unterlassung der Veröffentlichung von Beiratssitzungen auf deren Website

**Geldbußen**

Zu den von uns erlassenen Bescheiden, mit denen wir Geldbußen verhängten, teilten wir dem Antragsteller Folgendes mit:

**2020**

- ein Bescheid im Bereich Gesundheit und Soziales

**2021**

- fünf Bescheide gegen Polizist:innen

**2022**

- sechs Bescheide im Bereich Beschäftigtendatenschutz
- sechs Bescheide im Bereich Dienstleistungen/Handel/Handwerk
- fünf Bescheide im Bereich Gesundheit und Soziales
- drei Bescheide im Bereich Telemedien
- ein Bescheid im Bereich Bau- und Wohnungswesen

**2023**

- neun Bescheide gegen Polizist:innen
- fünf Bescheide im Bereich Beschäftigtendatenschutz
- vier Bescheide gegen Rechtsanwälte beziehungsweise Rechtsanwaltskanzleien
- zwei Bescheide im Bereich Gesundheit und Soziales
- zwei Bescheide im Bereich Telemedien
- ein Bescheid im Bereich Kreditwesen
- ein Bescheid im Bereich Werbung
- ein Bescheid im Bereich Bau- und Wohnungswesen

## 2.6 Europäische Verfahren nach der Datenschutzgrundverordnung (DSGVO)

| | |
|---|---|
| Verfahren mit Betroffenheit nach Artikel 56 DSGVO: | Sieben Fälle |
| Verfahren mit Federführung nach Artikel 56 DSGVO: | Kein Fall |
| Verfahren gemäß Kapitel VII nach den Artikeln 60ff. DSGVO: | Vier Fälle (Artikel 61) |

## 2.7 Förmliche Begleitung bei Rechtsetzungsvorhaben

Folgende Beratungen wurden im Berichtsjahr 2023 durchgeführt:

**Soziales**

– Bremische Verordnung zur Durchführung des Studierenden-Energiepreispauschalengesetzes (BremEPPSG-VO)

– Gesetz zur Ausführung des Kinder- und Jugendhilfegesetzes

**Justiz**

– Novellierung des Bremischen Richtergesetzes (BremRiG)

– Neufassung des Gesetzes über das Halten von Hunden (BremHundG)

**Bau, Wohnen, Umwelt, Energie und Verkehr**

- Bremisches Architektengesetz (BremArchG)
- Bremisches Ingenieurgesetz (BremIngG)
- Bremische Landesbauordnung (BremLBO)
- Bremisches Landesraumordnungsgesetz (BremROG)
- Verordnung über abfallrechtliche Zuständigkeiten, über die Zuständigkeit für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach dem Batteriegesetz, dem Verpackungsgesetz, der Einwegkunststoffverbotsverordnung, der Einwegkunststoffkennzeichnungsverordnung und zur Änderung der Verordnungen über die Zuständigkeiten für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach dem Elektro- und Elektronikgerätegesetz und nach der Elektro- und Elektronikgeräte-Stoff-Verordnung

- Verordnung zum Schutz von Bäumen und freiwachsenden Hecken im Land Bremen (BaumSchutzVO)

- Verordnung zur Durchführung des Gebäudeenergiegesetzes (GEGV)

- Entwässerungsgebührenortsgesetz (EGebOG)

- Gebührenordnung für die Abfallentsorgung in der Stadtgemeinde Bremen

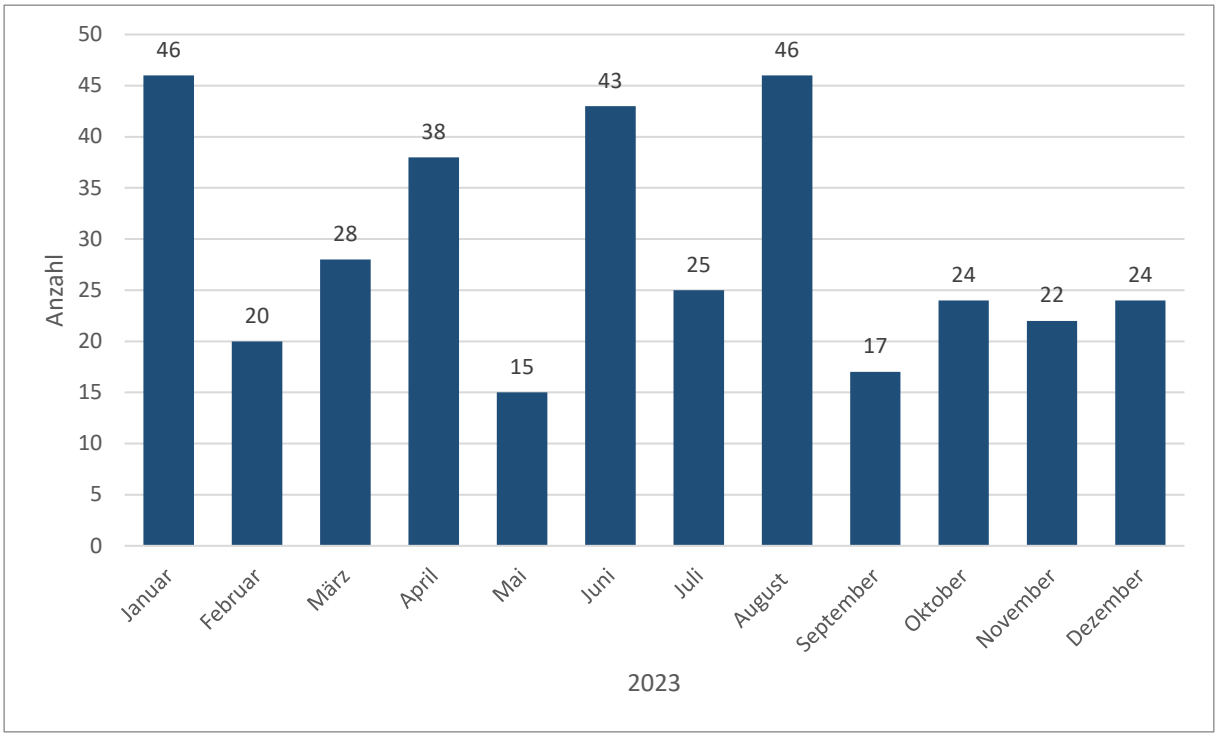
- Verwaltungsvereinbarung zwischen der Freien Hansestadt Bremen und dem Land Niedersachsen zur Durchführung des Staatsvertrages vom 1./15. Februar 2022 (Niedersächsisches Gesetz- und Verordnungsblatt Nummer 18/2022, Seite 350 und Bremisches Gesetzblatt Nummer 45/2022, Seite 230) zwischen der Freien Hansestadt Bremen und dem Land Niedersachsen im Bereich der beiden EU-Fonds Europäischer Garantiefonds für die Landwirtschaft (EGFL) und Europäischer Landwirtschaftsfonds für die Entwicklung des ländlichen Raums (ELER) sowie nationaler Fördermaßnahmen

**Beschäftigtendatenschutz**

- Verordnung zur Änderung der Wahlordnung zum Bremischen Personalvertretungsgesetz (BremPersVGWO)

- Gesetz zur Errichtung eines Ausbildungsunterstützungsfonds im Land Bremen (AusbUFG)

## 2.8 Meldungen über die Bestellung behördlicher und betrieblicher Datenschutzbeauftragter




Säulendiagramm 4

Nach Artikel 37 Datenschutzgrundverordnung müssen die behördlichen und betrieblichen Datenschutzbeauftragten an die zuständige Aufsichtsbehörde gemeldet werden. Diese Grafik zeigt die Zahl der jeweiligen Meldungen pro Monat.

## 2.9 Datenschutzrechtliche Zertifizierung

Die Förderung von datenschutzspezifischen Zertifizierungsverfahren beschäftigt die Datenschutzaufsichtsbehörden in ganz Europa bereits seit mehreren Jahren. Die Akkreditierung von Zertifizierungsstellen ist ein Verfahren, bei dem die Kompetenz und Integrität der Zertifizierungsstellen geprüft wird. Diese Prüfung ist entscheidend, um sicherzustellen, dass die von den Zertifizierungsstellen ausgestellten Zertifikate glaubwürdig sind und den hohen Anforderungen an den Datenschutz gerecht werden. Grundlage dafür sind die Artikel 42 und 43 der Datenschutzgrundverordnung (DSGVO).

Nachdem die Landesbeauftragte für Datenschutz und Informationsfreiheit (LfDI) im vorangegangenen Jahr einen Kriterienkatalog geprüft und für grundsätzlich genehmigungsfähig gehalten hatte, den ein bremisches Unternehmen erarbeitet hatte, das zuvor einen Antrag auf Akkreditierung als Zertifizierungsstelle gestellt hatte (siehe hierzu 5. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 2.9), begann die sogenannte Kooperationsphase auf europäischer Ebene. Hier haben sich die italienische

Datenschutzaufsichtsbehörde Garante per la Protezione dei Dati Personali und die Berliner Beauftragte für Datenschutz und Informationsfreiheit bereit erklärt, als Co-Reviewer tätig zu werden und im Rahmen dessen den Kriterienkatalog ebenfalls geprüft. Im Anschluss daran informierte die LfDI das Sekretariat des Europäischen Datenschutzausschusses (EDSA) über den Verfahrensstand und stellte den Kriterienkatalog allen europäischen Datenschutzaufsichtsbehörden zur Verfügung. Diese hatten daraufhin eine 30-tägige Frist, um Anmerkungen zu formulieren. Eine europäische Datenschutzaufsichtsbehörde hatte Fragen hierzu und gab Hinweise, deren Bearbeitung zum Redaktionsschluss noch andauert.

Zeitgleich wurde von der Deutschen Akkreditierungsstelle (DAkkS) gemeinsam mit einem Fachbegutachter der LfDI eine Vor-Ort-Begutachtung auf Grundlage der in der Norm DIN EN ISO/IEC 17065 definierten Anforderungen sowie der zusätzlichen Konkretisierungen der deutschen Datenschutzaufsichtsbehörden[1] bei dem antragstellenden Unternehmen durchgeführt.

Auf dem Weg zur Akkreditierung einer Zertifizierungsstelle sind zu diesem Verfahrensstand nur noch wenige Hürden zu nehmen. So müssen die eingereichten Unterlagen in der EDSA-Arbeitsgruppe Compliance, e-Government and Health Expert Subgroup diskutiert werden, bevor letztendlich der EDSA eine Stellungnahme nach Artikel 64 DSGVO dazu abgeben wird. Der Antrag auf Zulassung als nationale Zertifizierungsstelle wird im Anschluss von derjenigen datenschutzrechtlichen Aufsichtsbehörde beschieden, bei der das Unternehmen diesen gestellt hat.

## 2.10 Europäisches Binnenmarkt-Informationssystem

Die Anzahl der zu sichtenden und zu bewertenden E-Mails, die durch das europäische Binnenmarkt-Informationssystem (Internal Market Information System, IMI) versandt wurden, blieb 2023 auf dem Niveau des Vorjahres. Ein Großteil der Nachrichten betraf die Prüfung der Zuständigkeit. Es gab allerdings auch diverse Beschlussmitteilungen der europäischen Aufsichtsbehörden.

[1] "Anforderungen zur Akkreditierung gemäß Artikel 43 Absatz 3 DSGVO in Verbindung mit DIN EN ISO/IEC 17065", online abrufbar unter https://www.datenschutzkonferenz-online.de/media/ah/20201008_din17065_Ergaenzungen_deutsch_nach_opinion.pdf

## 3. Bremische Bürgerschaft – Ergebnisse der Beratungen des 5. Jahresberichts nach Inkrafttreten der DSGVO

Der Bericht des Ausschusses für Wissenschaft, Medien, Datenschutz, Informationsfreiheit und Digitalisierung (WMDID-Ausschuss) zum 5. Jahresbericht nach der Europäischen Datenschutzgrundverordnung (DSGVO) der Landesbeauftragten für Datenschutz vom 24. März 2023 (Drucksache 20/1835) und zur Stellungnahme des Senats vom 27. Juni 2023 (Drucksache 21/3) lag zum Redaktionsschluss noch nicht vor.

## 4. Geldbußen

### 4.1 Allgemeines

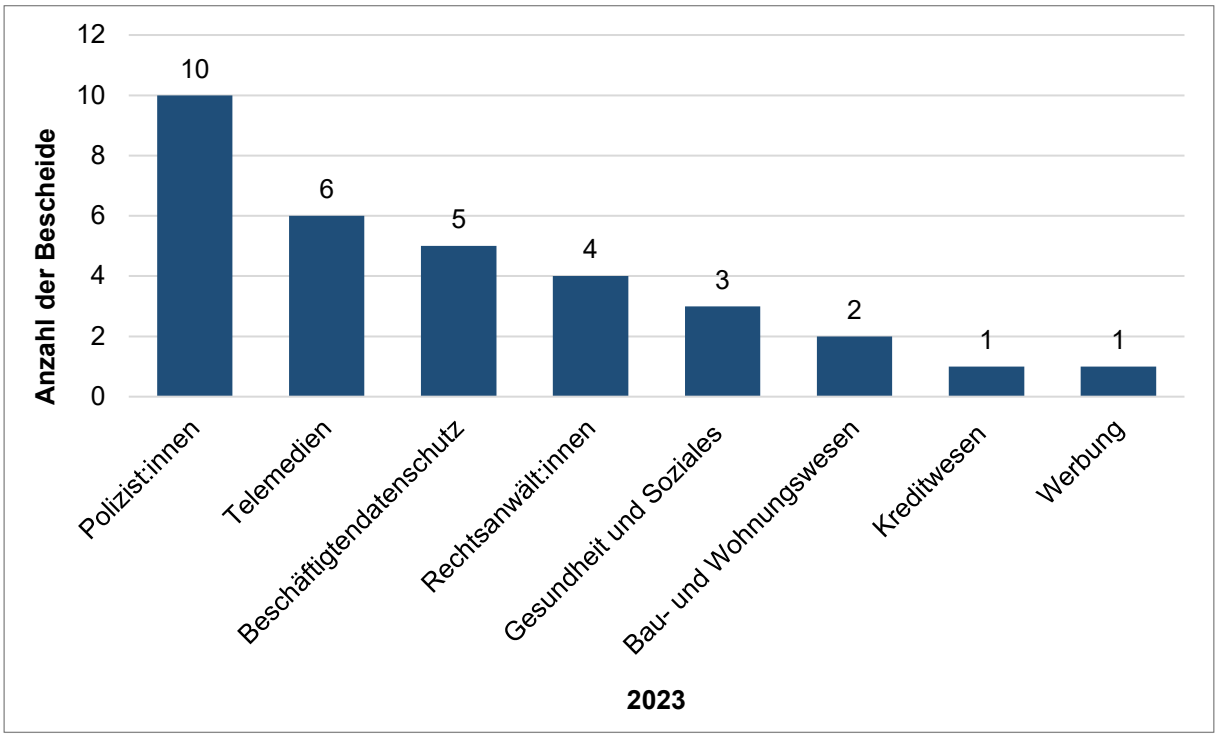
Im Berichtsjahr 2023 lag der Schwerpunkt der aufsichtsbehördlichen Verfahren zur Festsetzung von Geldbußen gemäß Artikel 83 Datenschutzgrundverordnung (DSGVO) auf festgestellten datenschutzrechtlichen Verstößen, die im Jahr 2020 und 2021 stattgefunden hatten.

Europa prägt die deutsche und damit auch die bremische Sanktionspraxis maßgeblich. Auf europäischer Ebene wurden die Leitlinien 04/2022 zur Berechnung von Geldbußen gemäß der Datenschutzgrundverordnung am 25. Mai 2023 endgültig festgelegt, die gemäß Artikel 70 Absatz 1 Buchstabe k DSGVO ausgearbeitet wurden und deren praktische Anwendung gemäß Artikel 71 Absatz 2 DSGVO überprüft wird.

Am 5. Dezember 2023 entschied der Europäische Gerichtshof (EuGH) in der Rechtssache 807/21 "Deutsche Wohnen SE", dass die Verhängung von Geldbußen nach der Europäischen Datenschutzgrundverordnung gegen Unternehmen, die für die Verarbeitung personenbezogener Daten verantwortlich sind, nicht davon abhängt, dass die datenschutzrechtliche Aufsichtsbehörde zuvor festgestellt hat, dass eine oder mehrere identifizierte natürliche Personen gegen die DSGVO verstoßen haben. Vielmehr reicht es aus, dass eine im Namen des Unternehmens handelnde Person einen vorsätzlichen oder fahrlässigen Verstoß gegen die DSGVO begangen hat. Eine datenschutzrechtliche Haftung von Unternehmen besteht dabei schon dann, wenn sich die verantwortlichen Stellen über die Rechtswidrigkeit ihres Verhaltens nicht im Unklaren sein konnten, unabhängig davon, ob ihnen dabei bewusst war, dass sie gegen die Vorschriften der DSGVO verstoßen. Mit dieser Entscheidung bestätigte der EuGH die Sanktionspraxis der bremischen Datenschutzaufsichtsbehörde: Unternehmen haften in datenschutzrechtlicher Hinsicht für alle Beschäftigten.

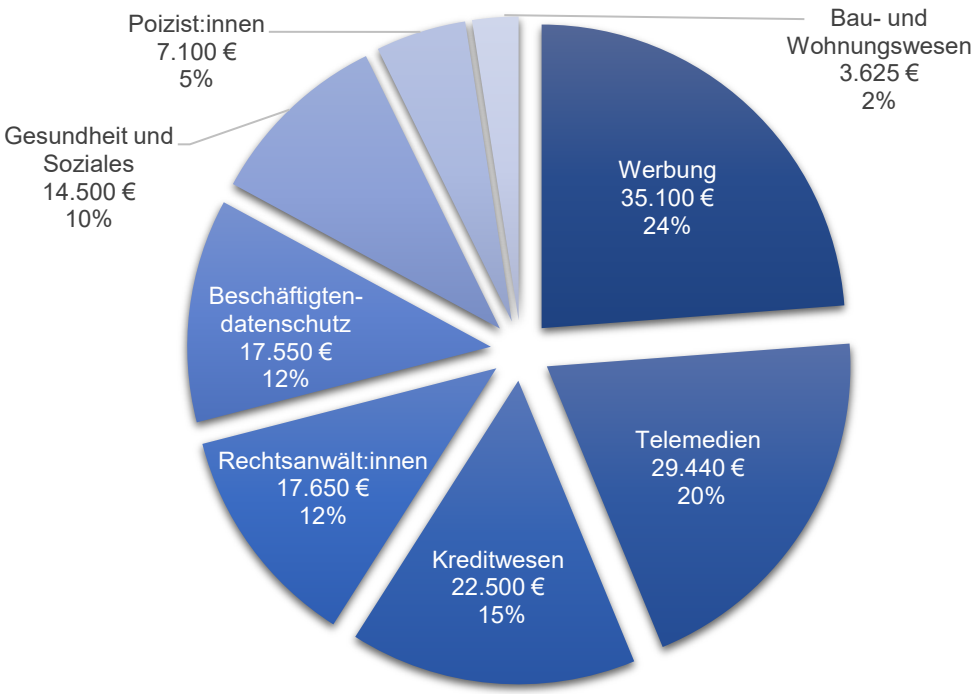
Im Berichtsjahr ergingen gegen Unternehmen und natürliche Personen 32 Bescheide zur Verhängung von Geldbußen, die insgesamt 51 Geldbußen enthielten. Die Anzahl der verhängten Geldbußen divergiert mit der Anzahl der Bescheide, da gegen eine verantwortliche Stelle in einem Bescheid mehrere Geldbußen verhängt werden können.

Insgesamt wurden im Berichtsjahr Geldbußen in Höhe von 147.465 Euro verhängt. Von den 32 erlassenen Bescheiden wurden 20 im Berichtsjahr rechtskräftig. Aus dem Berichtsjahr und vorangegangenen Jahren befinden sich 13 Bescheide zu Redaktionsschluss im Einspruchsverfahren. 14 Verfahren aus dem Berichtsjahr und vorangegangenen Jahren wurden eingestellt.




Säulendiagramm 5

Im Berichtsjahr verteilten sich die Geldbußen nach Artikel 83 DSGVO auf die folgenden Bereiche: zehn Bescheide beziehungsweise 15 Geldbußen gegen Polizist:innen, sechs Bescheide im Bereich Telemedien, fünf Bescheide beziehungsweise neun Geldbußen im Bereich Beschäftigtendatenschutz, vier Bescheide beziehungsweise acht Geldbußen gegen Rechtsanwält:innen, drei im Bereich Gesundheit und Soziales, zwei Bescheide beziehungsweise sechs Geldbußen im Bereich Bau- und Wohnungswesen, jeweils ein Bescheid beziehungsweise vier Geldbußen im Bereich Kreditwesen und Werbung.




Tortendiagramm 4

Die Verteilung der im Jahr 2023 verhängten Geldbußen auf die jeweiligen Bereiche ergibt sich aus dem Tortendiagramm. Die Themengebiete sind in absoluten und relativen Werten dargestellt.

## 4.2 Unzulässige Videoüberwachung von Beschäftigten und Kund:innen

Im Berichtsjahr verhängte die Landesbeauftragte für Datenschutz und Informationsfreiheit eine Geldbuße nach Artikel 83 Datenschutzgrundverordnung gegen ein Unternehmen, welches in den Büroräumen Videokameras installiert hatte und sowohl die Beschäftigten vor, während und nach ihrer Arbeitszeit als auch die Kund:innen während der Öffnungszeiten ohne Befugnis mittels Kameras über einen Zeitraum von zwei Jahren beobachtet hatte und diese Aufnahmen aufgezeichnet hatte (siehe hierzu 5. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 12.6).

## 4.3 Zu lange Speicherung von Daten von Bewerber:innen und ehemaligen Beschäftigten

In zwei Fällen verhängte die Landesbeauftragte für Datenschutz und Informationsfreiheit Geldbußen nach Artikel 83 Datenschutzgrundverordnung (DSGVO) gegen Unternehmen in ihrer Funktion als Arbeitgeberinnen, die personenbezogene Daten ihrer Bewerber:innen und ehemaliger Beschäftigter ohne Rechtsgrundlage speicherten.

In einem Fall speicherte ein Unternehmen die Bewerbungsunterlagen einer Bewerberin über das Bewerbungsverfahren hinaus, ohne von der betroffenen Bewerberin eine Einwilligung

nach Artikel 6 Absatz 1 Satz 1 Buchstabe a DSGVO in die Weiterspeicherung zwecks erneuter Berücksichtigung ihrer Person bei zukünftigen Ausschreibungen eingeholt zu haben. In einem anderen Fall speicherte ein Unternehmen Kontaktdaten ehemaliger geringfügig Beschäftigter ohne ihre vorherigen Einwilligungen, um diese bei Bedarf in der Zukunft zu kontaktieren und ihnen weitere Jobangebote zu unterbreiten.

In diesen Fällen konnte nicht ohne Weiteres ein mutmaßliches Interesse der Betroffenen in die Weiterspeicherung angenommen werden. Bewerber:innen und Beschäftigte haben das Recht, selbst zu entscheiden, was mit ihren personenbezogenen Daten nach dem Ablauf des Bewerbungsverfahrens oder nach dem Ausscheiden aus dem Unternehmen passiert. Ein ausdrücklicher Wunsch einer Bewerberin/Beschäftigten oder eines Bewerbers/Beschäftigten auf Weiterspeicherung ihrer/seiner Bewerbungsunterlagen und Kontaktdaten muss von den Arbeitgeberinnen dokumentiert werden. Letztere unterliegen den Nachweispflichten gemäß Artikel 7 Absatz 1 DSGVO in Bezug auf die von den Beschäftigten erteilten Einwilligungen.

## 4.4 Rechtswidrige Versendung eines psychiatrischen Berichts

Veranlasst durch eine Beschwerde verhängte die Landesbeauftragte für Datenschutz und Informationsfreiheit eine Geldbuße nach Artikel 83 Datenschutzgrundverordnung gegen ein Klinikum, das einen ungeschwärzten Behandlungsbericht über die psychiatrische Behandlung des Betroffenen an eine Unfallkasse übermittelt hatte, ohne dass die Datenübermittlung durch eine Rechtsgrundlage legitimiert war. Entscheidend bei der Sanktionierung dieses Verstoßes war der Umstand, dass der übermittelte Entlassungsbericht umfangreiche Angaben zum Gesundheitszustand, zu strafrechtlichen Vorwürfen und andere Informationen über den Betroffenen enthielt, die in die Intim- und Privatsphäre des Betroffenen fielen. Die Datenübermittlung verletzte in hohem Maße das allgemeine Persönlichkeitsrecht des Betroffenen. Des Weiteren wurde berücksichtigt, dass dem Betroffenen durch die Übermittlung des Entlassungsberichts Nachteile bei der Feststellung der Unfallrente drohten.

## 4.5 Wiederholte Kontaktaufnahmen per Telefon und E-Mail durch Maklerbüro ohne Rechtsgrundlage

Die Landesbeauftragte für Datenschutz und Informationsfreiheit verhängte fünf Geldbußen gegen ein Maklerbüro. Dieses hatte wiederholt per Anruf und E-Mail einen Immobilieninteressenten kontaktiert, der einst bei dem Vorgänger-Maklerbüro ein Exposé zu einer inserierten Immobilie angefragt hatte. Nachdem der Betroffene das Exposé erhalten hatte, teilte er dem Vorgänger-Maklerbüro sofort mit, dass seinerseits kein Interesse bestehe und beantragte die Löschung seiner Daten.

Gleichwohl rief das Nachfolger-Maklerbüro, das den Kund:innenstamm des Vorgängerbüros übernommen hatte, den Betroffenen ein Jahr später an und erkundigte sich nach bestehendem Immobilieninteresse. Obwohl der Betroffene seine Aufforderung nach Löschung seiner Daten wiederholte, versandte das Maklerbüro an den Betroffenen drei Newsletter mit Immobilienangeboten. Außerdem versuchte das verantwortliche Maklerbüro den Betroffenen noch einmal telefonisch zu kontaktieren, nachdem es der Landesbeauftragten für Datenschutz und Informationsfreiheit gegenüber bestätigt hatte, alle Daten über den Betroffenen gelöscht zu haben. Das Maklerbüro hatte zu keinem Zeitpunkt eine Legitimationsgrundlage für die oben genannten Kontaktaufnahmen. Das Maklerbüro hätte den vormaligen Kunden seines Vorgängers nicht ohne dessen ausdrückliche Einwilligung kontaktieren dürfen. Spätestens nachdem der Betroffene die Löschung seiner personenbezogenen Datenvon dem Maklerbüro verlangt hatte, hätte das Maklerbüro alle personenbezogenen Daten aus allen seinen Systemen unwiderruflich löschen müssen.

## 4.6 Fehlende Verifizierung von E-Mail-Adressen im Internetgeschäft

Die Landesbeauftragte für Datenschutz und Informationsfreiheit belegte eine Betreiberin einer Dating-Internetplattform mit einer Geldbuße wegen Verstoßes gegen Artikel 32 Datenschutzgrundverordnung. Der Grund dafür war, dass die verantwortliche Betreiberin der Plattform kein E-Mail-Verifizierungsverfahren bei der Registrierung auf ihrer Dating-Internetplattform vorgesehen hatte. Dies führte dazu, dass sich in einem der Landesbeauftragten für Datenschutz und Informationsfreiheit durch Beschwerde eines Betroffenen bekannt gewordenen Fall ein Dritter mit der E-Mail-Adresse des Betroffenen auf dem Portal registrieren konnte. Der ahnungslose Betroffene erhielt eine Registrierungsbestätigung sowie weitere Nachrichten mit Hinweisen auf eingehende Post und Angebote des Portals. Der von der verantwortlichen Betreiberin praktizierte Registrierungsprozess – keine Angabe von Klarnamen, keine Verifizierung angegebener E-Mail-Adressen – war nicht dazu geeignet, den Schutz personenbezogener Daten ihrer Kund:innen und anderer Personen zu gewährleisten.

## 4.7 Sanktionierung in Sachen Google Analytics

Aufgrund eines bei der Landesbeauftragten für Datenschutz und Informationsfreiheit (LfDI) eingegangenen Hinweises überprüfte die LfDI mehrere Internetseiten von bremischen Unternehmen auf Datenschutzkonformität der Nutzung des Tracking Tools "Google Analytics". Bei der Überprüfung stellte es sich heraus, dass die Betreiber:innen der angezeigten Internetseiten das Tool "Google Analytics" auf datenschutzwidrige Weise einsetzten.

Die "Google Analytics" Cookies wurden bereits zum Zeitpunkt des Öffnens der Internetseiten durch Websitebesucher:innen gesetzt.

Das Einbinden eines "Google Analytics" Cookies auf einer Website bewirkt die Verarbeitung personenbezogener Daten über die Websitebesucher:innen nach Artikel 4 Nummer 1 Datenschutzgrundverordnung. In dem Moment, in dem Besucher:innen die Website öffnen, auf der das Tracking Tool "Google Analytics" eingebunden ist, werden auf dem Endgerät der Websitebesucherin oder des Websitebesuchers "Google Analytics" Cookies gesetzt. Ein Cookie beinhaltet eine eindeutige Kennnummer, anhand derer die Nutzer:innen wiedererkannt werden können, und kann zu unterschiedlichen Zwecken genutzt werden. "Google Analytics" Cookies, deren Kennnummern von Google vergeben werden, dienen der Analyse des Websitebesucher:innen-Verhaltens und werden zu Marketingzwecken eingesetzt. Mittels "Google Analytics" Cookies werden IP-Adressen (hierin enthaltende Daten wie das Herkunftsland der IP-Adresse und Providerangaben), Informationen zum Browser, Betriebssystem, Bildschirmauflösung (daraus lässt sich gegebenenfalls das verwendete Gerät – Smartphone, Tablet, Desktop-PC – ermitteln), Zeitzoneneinstellung, verweisende Website, Websitebesucher:innen-Verhalten auf der aktuellen Website und Datum und Uhrzeit des Websitebesuchs erhoben, an Google-Server übertragen, gespeichert und für die "Google Analytics" Berichte für die verantwortliche Stelle verarbeitet.

Dies stellt eine Verarbeitung der oben genannten personenbezogenen Daten der Websitebesucher:innen dar, die nach Rechtsprechung des Europäischen Gerichtshofes (Urteil vom 1. Oktober 2019 – C-673/17 "Planet49") und anschließend Rechtsprechung des Bundesgerichtshofes (Urteil vom 28. Mai 2020 - I ZR 7/16 "Planet 49") nur aufgrund einer wirksamen Einwilligung der Websitebesuchenden legitimiert werden kann. Die Internetseitenbetreiber:innen müssen also zunächst eine Einwilligung von den Websitebesucher:innen mittels eines Cookie-Banners einholen, bevor die "Google Analytics" Cookies auf ihren Internetseiten gesetzt werden dürfen. Dabei ist besonders auf die datenschutzkonforme Ausgestaltung des Banners zu achten. Die Websitebesucher:innen müssen stets aktiv in das Setzen der "Google Analytics" Cookies einwilligen können, ein voreingestelltes Ankreuzkästchen genügt dagegen nicht.

In fünf Fällen verhängte die Landesbeauftragte für Datenschutz und Informationsfreiheit Geldbußen aufgrund der Verwendung des Tracking Tools "Google Analytics" ohne vorherige Einwilligung der Websitenutzer:innen.

## 4.8 Unbefugte Abfragen von Polizist:innen

Die Landesbeauftragte für Datenschutz und Informationsfreiheit verhängte gegen zehn Polizist:innen Geldbußen nach Artikel 83 Datenschutzgrundverordnung (DSGVO) wegen unbefugter Abfragen. Die Mehrzahl der Fälle ging auf eine von dem polizeilichen Datenschutzbeauftragten durchgeführte Stichprobenkontrolle der polizeilichen Informationssysteme in Zusammenhang mit einer Pressemitteilung der Polizei Bremen zurück.

Gegenstand dieser Pressemitteilung aus dem Jahre 2021 waren Ermittlungen gegen einen Polizeibeamten gewesen. Die Motive der Polizist:innen für die unbefugten Abfragen waren unterschiedlich. Die einzeln verhängten Geldbußen reichten von 100 Euro bis 1.000 Euro je nach Einzelfall. Bei der Zumessung der Höhe der Geldbuße spielten gemäß Artikel 83 Absatz 2 DSGVO verschiedene Faktoren eine Rolle: unter anderem die Häufigkeit der Abfragen, die Qualität der personenbezogenen Daten (insbesondere Artikel 9 DSGVO oder Artikel 10 DSGVO), das Einkommen und etwaige geständige Einlassungen.

## 5. Datenschutzbeauftragte und Allgemeines öffentliche Stellen

### 5.1 Benennung von Datenschutzbeauftragten durch die Parteien

Ein Wahlberechtigter, der im Rahmen der Wahlwerbung vor den Wahlen zur Bremischen Bürgerschaft Post erhalten hatte, beschwerte sich, dass ihm von der Partei beziehungsweise Wählervereinigung, die ihn angeschrieben hatte, weder eine Datenschutzbeauftragte noch ein Datenschutzbeauftragter genannt werden konnte, an die beziehungsweise an den er sich wegen des Wahlwerbeschreibens hätte wenden können. Unsere Prüfung ergab, dass eine den Bestimmungen des Artikels 37 Datenschutzgrundverordnung (DSGVO) und ergänzend hierzu des § 38 Bundesdatenschutzgesetz (BDSG) entsprechende Benennung einer oder eines Beauftragten nicht erfolgt war, obwohl hierzu eine Verpflichtung bestand.

Nach § 38 Absatz 1 BDSG hat der Verantwortliche, also in der Regel die für die Datenverarbeitung verantwortliche Stelle, eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen, soweit er in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt. Nimmt der Verantwortliche Verarbeitungen vor, die einer Datenschutz-Folgenabschätzung nach Artikel 35 DSGVO unterliegen, hat er unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen eine Beauftragte oder einen Beauftragten zu benennen. Eine Datenschutz-Folgenabschätzung ist nach Artikel 35 Absatz 3 Buchstabe b DSGVO insbesondere erforderlich bei einer umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 DSGVO. Zu den besonderen Kategorien von personenbezogenen Daten zählen unter anderem Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen. Unter den Begriff der "politischen Meinungen" fallen dabei auch Daten wie die Zugehörigkeit zu einer Partei oder Wählervereinigung.

Wir baten die Partei beziehungsweise die Wählervereinigung daher, eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen, deren oder dessen Kontaktdaten zu veröffentlichen und uns als Aufsichtsbehörde mitzuteilen. Dies wurde

uns von dort zugesagt. Da uns auch von anderen Parteien beziehungsweise Wählervereinigungen bislang keine Kontaktdaten einer oder eines Datenschutzbeauftragten gemeldet wurden, werden wir den Vorgang zum Anlass nehmen, bei diesen auf die Einhaltung ihrer Bestellpflicht zu dringen.

## 5.2 Anforderungen an die Benennung von internen und externen Datenschutzbeauftragten

Nach den Vorschriften der Datenschutzgrundverordnung (DSGVO) und ergänzend hierzu den Regelungen des Bundesdatenschutzgesetzes (BDSG) sind von Verantwortlichen und Auftragsverarbeiter:innen Datenschutzbeauftragte zu benennen, wenn die dort genannten Sachverhalte vorliegen. Nach Artikel 37 Absatz 6 DSGVO kann die/der Datenschutzbeauftragte Beschäftigte oder Beschäftigter der/des Verantwortlichen oder der Auftragsverarbeiterin beziehungsweise des Auftragsverarbeiters sein oder ihre/seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen. Von Verantwortlichen und Auftragsverarbeiter:innen werden daher sowohl interne als auch externe Datenschutzbeauftragte benannt.

Sowohl bei der Benennung interner als auch externer Datenschutzbeauftragter ist nach Artikel 37 Absatz 5 DSGVO zu beachten, dass diese auf der Grundlage der vorhandenen beruflichen Qualifikation und insbesondere des bestehenden Fachwissens, das die für die Funktion vorgesehene Person auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf derer Fähigkeit zur Erfüllung der in Artikel 39 DSGVO genannten Aufgaben, zu erfolgen hat. Das Fachwissen muss sich auf die beim Verantwortlichen oder der Auftragsverarbeiterin beziehungsweise des Auftragsverarbeiters betriebene Datenverarbeitung beziehen. Insbesondere für externe Beauftragte, die mit der Verarbeitung häufig weniger in Verbindung stehen als interne Beauftragte, ergeben sich hieraus für ihre Benennung und ihr Tätigwerden spezielle Anforderungen, denen sie entsprechen müssen. Zur oder zum betrieblichen Datenschutzbeauftragten kann nur eine natürliche Person, nicht aber ein Unternehmen oder eine andere Einrichtung benannt werden.

Um die Aufgaben der oder des Datenschutzbeauftragten erfüllen zu können, müssen die Beauftragten auch über die dafür benötigte Zuverlässigkeit verfügen. Zu vermeidende Inkompatibilitäten, die sich bei internen Datenschutzbeauftragten insbesondere durch andere ihnen zugewiesene Aufgaben, zum Beispiel bei einer Behörde oder einem Unternehmen ergeben können, lassen eine Benennung zur oder zum Datenschutzbeauftragten nicht zu. Die oder der Beauftragte kann daher nicht gleichzeitig mit einer leitenden Funktion, die die personenbezogene Datenverarbeitung betrifft, wie im Bereich der Geschäftsführung, der Leitung der IT-Abteilung oder der Verwaltungsleitung, betraut sein. Bei externen Datenschutzbeauftragten ergibt sich ein besonderes Problem nicht selten daraus, dass die

oder der Beauftragte für eine Behörde oder ein Unternehmen gleichzeitig als Beraterin oder Berater tätig wird und sich daraus eine wirtschaftliche Abhängigkeit ergibt. Die oder der Beauftragte muss in ihren Positionen und Entscheidungen unabhängig und frei von Weisungen sein.

Sowohl die internen als auch die externen Datenschutzbeauftragten sind ordnungsgemäß und frühzeitig in allen mit dem Schutz personenbezogener Daten zusammenhängenden Fragen einzubinden. Den externen Beauftragten ist in gleichem Maße wie der oder dem internen Beauftragten Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen zu gewähren, damit sie ihre Aufgaben nach Artikel 39 DSGVO erfüllen können.

Die DSGVO sieht die Abberufung der oder des Datenschutzbeauftragten nicht vor. § 38 in Verbindung mit § 6 BDSG lässt die Abberufung der oder des Beauftragten vielmehr nur in entsprechender Anwendung von § 626 Bürgerliches Gesetzbuch, also aus wichtigem Grund, zu. Zumeist erfolgt die Beendigung der Amtsausübung bei internen Beauftragten daher in gegenseitigem Einvernehmen. Externe Datenschutzbeauftragte, deren Benennung auf der Grundlage eines Dienstleistungsvertrags erfolgt, sind jedoch auch an die Laufzeit des Vertrags gebunden, die um die Amtsausübung der DSGVO entsprechend nicht zu gefährden, ausreichend lang, das heißt für mehrere Jahre vereinbart sein muss.

## 5.3 Deutschland online – Datenschutzcockpit

Mit Einführung des Registermodernisierungsgesetzes (RegMoG) wurde die Grundlage für das sogenannte "Once-Only-Prinzip" geschaffen, welches besagt, dass diejenigen Menschen, die sich mit einem Anliegen an Behörden und Verwaltungen wenden, zukünftig ihre Daten nur einmal mitteilen müssen. Unter Einhaltung der Datenschutzbestimmungen sowie nach der expliziten Zustimmung der betroffenen Personen dürfen bestimmte öffentliche Stellen diese Daten wiederverwenden und untereinander austauschen.

Beim Datenschutzcockpit handelt es sich um ein System, welches auf Grundlage des RegMoG entsteht und allen Menschen die Möglichkeit bietet, ihre Informations-, Kontroll- und Mitwirkungsmöglichkeiten wahrzunehmen, indem sie selbstständig überprüfen können, welche Daten wann und aus welchem Grund zwischen öffentlichen Stellen ausgetauscht wurden. Das RegMoG gibt die Einführung einer persönlichen Identifikationsnummer (IDNr) vor, welche als übergreifendes Ordnungsmerkmal in den Registern eingesetzt wird, die für die Bereitstellung von Verwaltungsdienstleitungen nach dem Onlinezugangsgesetz (OZG) wesentlich sind. Die Register dürfen die IDNr in ihren Datenübermittlungen nur verwenden, wenn sie an das Datenschutzcockpit angeschlossen sind.

Die Landesbeauftragte für Datenschutz und Informationsfreiheit begleitet die Einführung des vom Bundesministerium des Innern und für Heimat beauftragten und von der Freien

Hansestadt Bremen umgesetzten Datenschutzcockpits gemeinsam mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Im regelmäßig stattfindenden Steuerungskreis werden Projektfortschritte und offene Fragen beraten, insbesondere zur technischen Ausgestaltung und zu verschiedenen Rechtsfragen. Ein besonderes Augenmerk liegt dabei auf der Umsetzung der Anforderungen des Datenschutzgrundsatzes "Privacy by Design" nach Artikel 25 Absatz 1 Datenschutzgrundverordnung.

# 6. Inneres

## 6.1 Gemeldete Datenschutzverletzungen

Aus dem Bereich der öffentlichen Stellen, insbesondere aus dem Bereich Inneres, erreichten uns im Berichtsjahr insgesamt neun Meldungen von Datenschutzverletzungen. Diese betrafen unterschiedliche Sachverhalte. Nach wie vor ein Klassiker aus diesem Bereich ist die Fehlversendung von Unterlagen.

## 6.2 Videoüberwachung

Wie bereits im vergangenen Berichtsjahr (siehe hierzu 5. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 6.2) waren wir auch im aktuellen Berichtsjahr verstärkt mit der Thematik der Videoüberwachung durch öffentliche Stellen befasst.

### 6.2.1 Maritime Tage 2023

Auch im aktuellen Berichtszeitraum nutzte die Ortspolizeibehörde Bremerhaven wie im letzten Jahr (siehe hierzu 5. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 6.2.1) und im vorletzten Jahr (siehe hierzu 4. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 5.4.1) die Rechtsgrundlage des § 32 Absatz 3 Satz 1 Nummer 2 Bremisches Polizeigesetz (BremPolG) für eine Videoüberwachung der Maritimen Tage in Bremerhaven.

Wir wurden frühzeitig in die Planung einbezogen. Entscheidende Unterschiede zu der Überwachungsmaßnahme im letzten und vorletzten Jahr waren nicht feststellbar. Wir sehen jedoch auch aufgrund dieser erneuten umfassenden Videoüberwachungsmaßnahmen in der Stadt Bremerhaven Anlass, die Verhältnismäßigkeit und die Rechtsgrundlage für die Überwachung von Großveranstaltungen nach dem BremPolG kritisch zu hinterfragen.

### 6.2.2 Bremer Freimarkt und Weihnachtsmarkt 2023

Erstmalig wurden im Berichtsjahr auch der Bremer Freimarkt und der Weihnachtsmarkt (partiell) von der Polizei Bremen videoüberwacht. Damit machte auch die Polizei Bremen von

der Rechtsgrundlage des § 32 Absatz 3 Satz 1 Nummer 2 Bremisches Polizeigesetz (BremPolG) Gebrauch. Die Modalitäten der Überwachung entsprachen weitgehend denen der Überwachung der Maritimen Tage. Dementsprechend erstellte auch die Polizei Bremen jeweils eine Datenschutz-Folgenabschätzung nach § 82 BremPolG, zu der wir eine Stellungnahme verfassten, die auch den Mitgliedern der Innendeputation übermittelt wurde. Wie bei den Maritimen Tagen überprüften wir die Überwachungsmaßnahme vor Ort. Die Überwachung des Weihnachtsmarktes prüften wir ergänzend auch in der Videoleitstelle der Polizei Bremen. Bei diesem Termin stellte sich heraus, dass der Beamte, der Kameras steuerte, über einen Account angemeldet war, bei dem entgegen der Angaben in der Datenschutz-Folgenabschätzung und entgegen der getroffenen Absprachen ein Schwenken der Kameras möglich war. Der Erfassungsbereich der Kameras wurde dadurch in unzulässiger Weise deutlich erweitert. Wir forderten die Polizei Bremen daher nachdrücklich auf, die weitere Nutzung der Schwenkfunktion zu unterbinden und ausschließlich den Account zu nutzen, über den die vereinbarten Begrenzungen vollumfänglich griffen. Zugleich forderten wir Login-Daten an um zu überprüfen, wann welcher Account genutzt wurde. Diese Nichteinhaltung der vereinbarten Beschränkungen der Videoüberwachung bestärkt noch einmal unsere grundsätzliche Kritik an der Überwachung von Volksfesten wie dem Weihnachtsmarkt.

### 6.2.3 Drohneneinsatz durch die Polizei zu repressiven Zwecken

Im letzten Berichtsjahr sprachen wir nach § 86 Absatz 3 Satz 1 Bremisches Polizeigesetz im Rahmen unserer Stellungnahme zur Datenschutz-Folgenabschätzung der Polizei Bremen die Empfehlung aus, im präventiven Aufgabenbereich keine Drohnen einzusetzen, bis der bremische Gesetzgeber eine entsprechende Rechtsgrundlage geschaffen hat. In diesem Jahr übermittelte uns die Polizei Bremen eine Datenschutz-Folgenabschätzung für den Drohneneinsatz im Strafverfolgungsbereich. Für diesen Bereich sieht die Strafprozessordnung (StPO) insbesondere in § 100h StPO Möglichkeiten des Drohneneinsatzes vor. Im Rahmen unserer Stellungnahme sprachen wir eine Reihe von Empfehlungen aus, die von der Polizei umgesetzt wurden. Diese Umsetzung überprüften wir, indem wir uns die Drohnen, ihre Funktionalitäten und die technischen Einstellungen vorführen ließen. Grundsätzlich kritisch bewerten wir, dass Drohnen eines chinesischen Herstellers beschafft wurden, der auf die sogenannten Blacklist des US-Verteidigungsministeriums gesetzt wurde, was zu erhöhten Anforderungen an die technische Sicherheit nach § 64 Bundesdatenschutzgesetz führt, infolgedessen etwa der Betrieb der Drohnen nur im Local-Data-Modus als zulässig zu erachten ist, bei dem die Drohnen keine Verbindungen ins Internet aufbauen.

### 6.2.4 Drohneneinsatz durch die Feuerwehr Bremerhaven

Nachdem wir durch eine entsprechende Berichterstattung der Sendung buten un binnen des Regionalsenders Radio Bremen darauf aufmerksam geworden sind, dass sich auch die

Feuerwehr Bremerhaven Drohnen beschafft hat, wiesen wir die Feuerwehr darauf hin, dass vor dem Einsatz der beschafften Drohnen eine Datenschutz-Folgenabschätzung durchzuführen ist. Die unter unserer Einbeziehung nach Artikel 35 Datenschutzgrundverordnung erstellte Datenschutz-Folgenabschätzung wurde uns zur Prüfung übermittelt. Einzelne Punkte wurden im Rahmen eines Vor-Ort-Termins besprochen. Das Bremische Hilfeleistungsgesetz (BremHilfeG) sieht vor, dass die Feuerwehr Bremerhaven in bestimmten Einsatzszenarien Drohnen zur Aufgabenerfüllung einsetzen kann. Unabhängig davon ist aus unserer Sicht aber auch in diesem Zusammenhang kritisch zu bewerten, dass Geräte eines chinesischen Herstellers beschafft wurden, was eine besondere Beachtung der technischen Sicherheit erfordert, wodurch letztlich auch der Drohneneinsatz verkompliziert wird.

### 6.2.5 Evaluierung Videoüberwachung öffentlicher Plätze

Im Berichtsjahr fand eine öffentliche Debatte über eine mögliche Erweiterung der (polizeilichen) Videoüberwachung statt. Konkret ging es um eine Überwachung von Haltestellen der Bremer Straßenbahn AG (BSAG). Auch im aktuellen Koalitionsvertrag findet sich eine Passage zu einer möglichen Ausweitung der Videoüberwachung.

Eine Überwachung von Bus- und Bahnhaltestellen der BSAG durch die Polizei Bremen kommt nach der bestehenden Rechtslage nur nach § 32 Absatz 3 Satz 1 Nummer 1 Bremisches Polizeigesetz (BremPolG) in Betracht. Die Voraussetzungen des § 32 Absatz 3 Satz 1 Nummer 1 BremPolG liegen an den Haltestellen der BSAG nach unserer Bewertung derzeit nicht vor. Zu berücksichtigen ist insbesondere, dass die Überwachung von Haltestellen als eine polizeiliche Maßnahme zu werten ist, die mit einem schweren Grundrechtseingriff in das informationelle Selbstbestimmungsrecht (Artikel 2 Absatz 1 Grundgesetz in Verbindung mit Artikel 1 Absatz 1 Grundgesetz) und in das Grundrecht auf Datenschutz (Artikel 8 Grundrechte-Charta) der Bürger:innen einhergeht und an die infolgedessen deutlich erhöhte Rechtfertigungsanforderungen zu stellen sind. Die Schwere des Eingriffs resultiert wiederum vor allem aus seiner Streubreite. Haltestellen im Allgemeinen und zentrale Knotenpunkte wie die Domsheide im Besonderen sind Orte des Zusammentreffens ganz unterschiedlicher, nicht näher bestimm- und typisierbarer Gruppen, deren Überwachung eine nahezu unbegrenzte Streuweite aufweist. Insoweit unterscheidet sich eine Überwachung etwa der Domsheide auch von der Überwachung von Polizeirevieren zum Beispiel in Findorff oder in Schwachhausen (siehe hierzu 5. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 6.2.4). Verstärkt wird die Intensität eines solchen Grundrechtseingriffs nochmals dadurch, dass das Aufsuchen von Haltestellen für alle Personen unerlässlich ist, die die Busse und Straßenbahnen nutzen möchten und Videoaufnahmen durch die Polizei daher für sie unausweichlich sind. Ebenso ist zu berücksichtigen, dass die Mehrzahl der Personen, die von der polizeilichen Maßnahme

erfasst und in deren Rechte eingegriffen wird, selbst aufgrund ihres normgetreuen Verhaltens gar keinen Anlass für die Maßnahme bietet.

Aus diesen Gründen hielten wir auch eine Erweiterung der polizeilichen Befugnisse zur Videoüberwachung für problematisch. Da die Ausweitung der Überwachungsbefugnisse in Bremen im Raum steht, halten wir es für erforderlich, nicht nur die Rechtmäßigkeit der aktuellen Überwachung öffentlicher Plätze durch Behörden zu überprüfen, sondern auch – im Sinne einer Gesamtüberwachungsrechnung – deren Intensität und grundrechtsbeschränkende Wirkung zu evaluieren. Hierzu erhoben wir im Berichtsjahr im ersten Schritt den aktuellen Stand der Überwachung.

## 6.3 Einsatz von KI bei Auswertung kryptierter Messenger

Das Thema Künstliche Intelligenz (KI) hat inzwischen auch die Sicherheitsbehörden und damit auch die bremischen Polizeibehörden erreicht. Im Zuge unserer Beratungstätigkeit sowie im Rahmen unserer Konsultation nach der Übermittlung entsprechender Datenschutz-Folgenabschätzungen nach § 82 Bremisches Polizeigesetz beziehungsweise § 67 Bundesdatenschutz wurden daher auch wir mit dieser Thematik konfrontiert. In Bremen ist derzeit das Thema KI vor allem bei der Auswertung kryptierter Messenger im Rahmen der sogenannten EncroChat-Verfahren von Relevanz. Unsere bremischen Prüfungserfahrungen flossen in die Entschließung "Verfassungsrechtliche Anforderungen bei automatisierter Datenanalyse durch Polizei und Nachrichtendienste beachten!" der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder ein (siehe hierzu sowie zu den Rahmenbedingungen für einen KI-Einsatz Ziffer 19.2 dieses Berichts).

Im Berichtsjahr prüften wir drei Anwendungen, die vor allem dazu eingesetzt werden, große Mengen an Bildmaterial aus den genannten Verfahren auszuwerten und Netzwerke zwischen den Chat-Teilnehmer:innen zu entdecken. Entscheidend für die Beurteilung der Grundrechtssensibilität der Thematik ist dabei, dass die Anwendungen derzeit lediglich Materialien für die Ermittler:innen aufbereiten, kein Informationsgehalt aus weiteren Quellen beigezogen wird und die Entscheidung über den Umgang mit der Auswertung und über die Einleitung weiterer Ermittlungsschritte ausschließlich den Ermittler:innen obliegt. Gleichwohl können gerade auch (KI-)Anwendungen zur Bildanalyse nicht zuletzt aufgrund von Diskriminierungspotenzialen hohe Risiken für die betroffenen Personen aufweisen. Der Einsatz weiterer Software, die das KI-Potenzial weitergehend ausschöpft und die insbesondere auch neue, händisch nicht zu gewinnende Informationen generiert, erfordert daher die Schaffung klarer Rechtsgrundlagen im Bremischen Polizeigesetz, mittels derer der Gesetzgeber den Einsatz von analyse- und/oder KI-gestützter Software und deren Grenzen deutlich definiert.

## 6.4 Zuverlässigkeitsüberprüfungen

Bereits im letzten Berichtsjahr thematisierten wir Probleme bei sogenannten Zuverlässigkeitsüberprüfungen von Bewerber:innen, Beschäftigten und anderen für öffentliche Stellen tätige Personen (siehe hierzu 5. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 6.8). In diesem Berichtsjahr erreichte uns eine Beschwerde über Zuverlässigkeitsüberprüfungen bei Einstellungen im Ordnungsdienst. Die für die Durchführung der Überprüfung erforderliche Datenverarbeitung – insbesondere die Datenabfrage bei der Polizei – wurde damit begründet, die Bewerber:innen hätten hierzu ihr Einverständnis gegeben. Eine solche Erklärung kann indes nicht als Einwilligung im datenschutzrechtlichen Sinne angesehen werden und daher die Datenverarbeitung nicht legitimieren. Grund hierfür ist, dass Bewerber:innen, die die vermeintliche Einwilligung verweigerten, vom Bewerbungsverfahren ausgeschlossen werden sollten, und die Erklärung infolgedessen nicht das Wirksamkeitskriterium der Freiwilligkeit erfüllte. Der Ordnungsdienst verzichtet nun auf die genannten Datenverarbeitungen.

Die Durchführung von Zuverlässigkeitsüberprüfungen kann nur auf eine gesetzliche Legitimationsgrundlage gestützt werden. Im Rahmen unserer Aufgabenwahrnehmung regen wir daher erneut an, dass sich der bremische Gesetzgeber dieser Thematik annimmt, indem er bestehende Regelungen überprüft, gegebenenfalls erweitert und zugleich klare Vorgaben zur Durchführung derartiger Prüfungen und damit auch zum Schutz betroffener Personen normiert. Zu beachten ist dabei insbesondere auch das Zusammenspiel mit dem Bremischen Sicherheitsüberprüfungsgesetz, dessen Änderung wir aktuell begleiten.

## 6.5 Einführung eines Alarmierungs- und Verfügbarkeitssystems bei der Feuerwehr Bremen

Bei der Berufsfeuerwehr Bremen und bei den freiwilligen Feuerwehren soll das Alarmierungs- und Verfügbarkeitssystemen DIVERA 24/7® eingeführt werden. Dieses System dient dazu, Kapazitäten für einen Einsatzfall abzufragen und zu steuern. Gleichzeitig beinhaltet die Anwendung auch ein Kommunikationstool, das anstelle bekannter Messenger-Dienste genutzt werden soll. Wir haben den Prozess der Systemeinführung kontinuierlich begleitet und wurden im Rahmen der Datenschutz-Folgenabschätzung nach Artikel 35 Datenschutzgrundverordnung (DSGVO) gemäß den Vorgaben des Artikel 36 DSGVO konsultiert. Da die Bediensteten der Feuerwehren die Anwendung auf ihrem privaten Smartphone installieren sollen, waren neben Fragen des Beschäftigtendatenschutzes, der IT-Sicherheit und des Auftragsverhältnisses mit dem Systemanbieter vor allem solche zum Bring-Your-Own-Device (BYOD) von Relevanz. Grundsätzlich sehen wir es kritisch, wenn auf privaten Smartphones dienstlichen Anwendungen installiert werden und so dienstliche Daten

auf private Endgeräte gelangen. Die Datenübermittlung auf private Endgeräte war daher auch in diesem Fall auf das unbedingt Erforderliche zu beschränken. Eine Art BYOD-Politik darf nicht zum Regelfall in der bremischen Verwaltung werden. Zu groß sind beispielsweise die Risiken, dass private Smartphones nicht hinreichend gegen den Zugriff Dritter – auch aus dem privaten Kreis – gesichert sind, dass sie verloren gehen und dass private und dienstliche Daten in unzulässiger Weise vermischt werden. Bei der Auswahl von Systemanbietern, insbesondere für neue Kommunikationstools, ist des Weiteren kritisch zu überprüfen, ob diese datenschutzrechtlichen Vorgaben genügen, vorzugswürdig sind grundsätzlich Anbieter, derer Server innerhalb der Europäischen Union und daher im Geltungsbereich der DSGVO stehen.

## 6.6 Aufzeichnungen von Anrufen beim Rettungsdienst

Bereits seit längerer Zeit befassen wir uns im Rahmen unserer Beratungstätigkeit mit dem Thema der Aufzeichnung von Anrufen beim Rettungsdienst. Der bremische Gesetzgeber hat mit § 61 Absatz 2a und mit § 61 Absatz 2b Bremisches Hilfeleistungsgesetz (BremHilfeG) Rechtsgrundlagen geschaffen, die die Aufzeichnung insbesondere von Notrufen und weiteren Anrufen ermöglichen und zum Teil sogar zur Aufzeichnung verpflichten. Der Rettungsdienst möchte diese Aufzeichnungen jedoch nicht nur zur Abwicklung des Notrufes nutzen, sondern auch zu Zwecken des Qualitätsmanagements, etwa um zu überprüfen, ob und wie die Vorgaben der standardisierten Notrufabfrage eingehalten werden. Mit § 62 BremHilfeG sieht der bremische Gesetzgeber grundsätzlich eine Rechtsgrundlage vor, die die Verwendung der Aufzeichnungen zu Zwecken des Qualitätsmanagements legitimiert. Jedoch ist die Rechtsgrundlage unvollständig. Sie legitimiert lediglich die Verwendung von Daten über Patient:innen zu Zwecken des Qualitätsmanagements. Werden Aufzeichnungen von Telefonaten zu diesen Zwecken verarbeitet, werden neben den Daten über die Patient:innen hingegen vor allem auch Daten über die Beschäftigten des Rettungsdienstes verarbeitet, die den Notruf entgegennehmen. Da die Verarbeitung von Beschäftigtendaten für das Qualitätsmanagement nicht legitimiert wird, können Anrufaufzeichnungen mithin nicht in rechtlich zulässiger Weise zu diesen Zwecken ausgewertet werden. Da uns gegenüber vorgetragen wird, dass eine Auswertung der Anrufe gewollt ist, sollte der bremische Gesetzgeber hierzu klar Stellung beziehen und – sofern er diese Auffassung teilt –, eine eindeutige Rechtsgrundlage schaffen, aus der sich ergibt, wie und in welchem Umfang Daten über Beschäftigte nach dem BremHilfeG zum Zwecke des Qualitätsmanagements verarbeitet werden dürfen. Die Normierung eine umfassenden (Leistungs-)Kontrolle wäre dabei wegen Verstoßes gegen europarechtliche Vorgaben nicht haltbar.

## 6.7 Rechtsverordnung zu Prüf- und Speicherfristen

Bereits im 4. Jahresbericht nach der Datenschutzgrundverordnung unter Ziffer 5.2 sowie im 5. Jahresbericht nach der Datenschutzgrundverordnung unter Ziffer 6.6 legten wir dar, dass

das Bremische Polizeigesetz (BremPolG) noch den Erlass einer Rechtsverordnung zu Prüf- und Speicherfristen der Polizei erfordert. Gemäß § 58 Absatz 6 Satz 1 BremPolG werden die Aussonderungsprüffristen vom Senator für Inneres und Sport durch Rechtsverordnung festgelegt, wobei nach unserer Rechtsauffassung auch die Normierung von Speicherfristen zulässig ist, insbesondere dann, wenn sich Aussonderungsprüffristen nicht als praktikabel erweisen. Trotz eines fortwährenden Austausches mit dem Senator für Inneres und Sport und wiederholte Betonung der Dringlichkeit des Erlasses einer derartigen Rechtsverordnung wurde eine solche noch nicht fertiggestellt. Zuletzt wurde seitens der Senatorin für Justiz und Verfassung mitgeteilt, dass nach dortiger Auffassung die Normierung von Speicherfristen nicht von § 58 Absatz 6 Satz 1 BremPolG gedeckt sei. Aufgrund des Bestrebens, eine praktikable Rechtsverordnung zu schaffen, werde daher nun eine Erweiterung der Ermächtigungsgrundlage angestrebt. Wir sehen uns noch einmal veranlasst, die Dringlichkeit des Erlasses einer praktikablen Rechtsverordnung zu betonen. Nur mit einer solchen Rechtsverordnung kann zum einen auf der Seite der Rechtsanwender:innen Klarheit über die zulässige Speicherdauer polizeilicher Daten geschaffen und zum anderen uns ein klarer Prüfungsmaßstab an die Hand gegeben werden.

## 6.8 Behördlicher Datenaustausch zwecks Beantwortung parlamentarischer Anfragen

Im Berichtsjahr erreichten uns Anfragen dazu, ob und gegebenenfalls unter welchen Voraussetzungen ein behördlicher Datenaustausch zwecks Beantwortung parlamentarischer Anfragen zulässig ist. So prüften wir, ob die Polizei Bremen und der Senator für Inneres und Sport eine Liste über eine Gruppe von Straftäter:innen an die Senatorin für Arbeit, Soziales, Jugend und Integration übermitteln darf, damit diese zwecks Beantwortung einer parlamentarischen Anfrage mitteilen kann, wie viele der auf der Liste genannten Personen Sozialleistungen beziehen (siehe hierzu Bremische Bürgerschaft, Drucksache 21/130). In einem Fall erlangten wir Kenntnis davon, dass ein derartiger Datenaustausch zwischen den Behörden stattgefunden hat.

Wir antworteten, dass dieser Datenaustausch zwecks Beantwortung der parlamentarischen Anfrage rechtswidrig wäre. Der Datenaustausch zwischen Behörden zwecks Beantwortung parlamentarischer Anfragen fällt unter die Datenschutzgrundverordnung (DSGVO) und gegebenenfalls unter die JI-Richtlinie (Richtlinie [EU] 2016/680 des europäischen Parlamentes und des Rates). § 2 Absatz 4 Bremisches Ausführungsgesetz zur EU-Datenschutz-Grundverordnung (BremDSGVOAG) nimmt nur die Bürgerschaft (Landtag), ihre Mitglieder, ihre Gremien, die von ihnen gewählten Mitglieder der staatlichen Deputationen, sowie die Fraktionen und Gruppen vom Anwendungsbereich des BremDSGVOAG sowie der DSGVO aus. Infolgedessen fällt zwar die parlamentarische Anfrage sowie die parlamentarische

Auswertung der erhaltenen Antwort nicht unter datenschutzrechtliche Bestimmungen, wohl aber die Datenverarbeitung durch die Behörden zwecks Beantwortung der Anfrage. Sofern hierzu auch auf polizeiliche Daten zugegriffen werden soll, sind zudem die Vorgaben des Bremischen Polizeigesetzes als Umsetzung der JI-Richtlinie zu beachten.

Mit diesen gesetzlichen Vorgaben nicht vereinbar wäre der behördliche Datenaustausch zur Beantwortung der parlamentarischen Anfragen. Da die Behörden ursprünglich die Daten nicht zu diesem Zweck erhoben hatten, galt dies insbesondere mit Blick auf den Zweckbindungsgrundsatz. Daneben war unter Verhältnismäßigkeitsgesichtspunkten zu bedenken, dass die beteiligten Behörden infolge des Austausches Daten erhielten, die zu ihrer originären Aufgabenerfüllung nicht erforderlich waren. Es hätte infolgedessen ein unverhältnismäßiger Eingriff in das informationelle Selbstbestimmungsrecht der betroffenen Personen vorgelegen, wenn etwa die Senatorin für Arbeit, Soziales, Jugend und Integration im Zuge eines solchen Datenaustausches Kenntnis davon erlangt hätte, welche der Sozialleistungsempfänger:innen Straftaten begangen haben, obwohl diese Kenntnis für ihre Aufgabenerfüllung irrelevant ist. Im Regelfall dürfen Behörden zur Beantwortung parlamentarischer Anfragen unter Beachtung datenschutzrechtliche Vorgaben auf ihren eigenen Datenbestand zugreifen, nicht aber Daten mit anderen Behörden austauschen um die erfragten Informationen zu generieren.

## 6.9 Überprüfung der Umsetzung der Protokollierungspflicht

Sofern eine Verarbeitung personenbezogener Daten nicht unter die Datenschutzgrundverordnung, sondern unter die sogenannte JI-Richtlinie (Richtlinie [EU] 2016/680 des europäischen Parlamentes und des Rates), unterliegen öffentliche Stellen einer Protokollierungspflicht. Dies betrifft insbesondere Behörden, die auf dem Gebiet Gefahrenabwehr und der Strafverfolgung tätig sind. So hat etwa die Polizei nach § 84 Bremisches Polizeigesetz (BremPolG) eine Reihe von Verarbeitungsvorgängen in automatisierten Verarbeitungssystemen zu protokollieren. Festgehalten werden müssen zum Beispiel bei einer Datenabfrage im Vorgangsbearbeitungssystem @rtus eine Begründung, das Datum und die Uhrzeit der Abfrage und soweit wie möglich die Identität der Person, die die personenbezogenen Daten abgefragt oder offengelegt hat. Die Protokollierungspflicht dient der Disziplinierung und der Erweiterung der Kontrollmöglichkeiten, über die etwa rechtswidrige Abfragen aufgedeckt werden können. Ihre Umsetzung ist daher ein wichtiger Baustein zum Schutz betroffener Personen. Aus diesem Grund begannen wir im Berichtsjahr mit der Überprüfung der Umsetzung der Protokollierungspflicht. Da die Polizei Bremen und die Ortspolizeibehörde Bremerhaven mitteilten, dass die Protokollierungspflicht nicht in allen Systemen vollständig umgesetzt wurde, sprachen wir gegen beide Behörden jeweils eine Beanstandung nach § 85 Absatz 1 BremPolG aus.

## 6.10 Überprüfung von EURODAC, ATD und RED

Im Berichtsjahr haben wir entsprechend unserer gesetzlichen Verpflichtung das System European Dactyloscopy (EURODAC), die Antiterrordatei (ATD) und die Rechtsextremismusdatei (RED) beim Landesamt für Verfassungsschutz und bei der Polizei überprüft. Während bei EURODAC und der RED keine Auffälligkeiten durch uns festgestellt wurden, gelangten wir im Rahmen der Prüfung der ATD zu dem Ergebnis, dass die Polizei Bremen in drei Fällen die Aussonderungsprüffristen nicht beachtet und damit in diesen Fällen gegen die Vorgaben des § 11 Absatz 4 des Gesetzes zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern (Antiterrordateigesetz – ATDG) verstoßen hat. Diesem Verstoß wurde zwischenzeitlich abgeholfen.

## 6.11 Weiterleitung von Daten durch den Rettungsdienst an die Polizei bei einem Verkehrsunfall

Wir erhielten eine Anfrage eines Betroffenen zur Frage der Rechtmäßigkeit der Weitergabe personenbezogener Daten durch den Rettungsdienst an Polizeibehörden im Rahmen eines Verkehrsunfalls. Dabei wurde auch die Frage aufgeworfen, ob die Rettungskräfte im Falle eines Verkehrsunfalls mit verletzten Personen legitimiert oder sogar verpflichtet sind, die Polizei zu verständigen und ob die Weitergabe personenbezogener Daten der versorgten Personen in diesem Zusammenhang erlaubt ist.

Bei dem Verdacht einer Straftat besteht für Rettungskräfte die Möglichkeit, die Polizei zu verständigen, ohne eine Datenschutzverletzung oder einen Verstoß gegen § 203 Strafgesetzbuch (StGB, Verletzung von Berufsgeheimnissen) zu begehen. Wenn die mit der Verarbeitung personenbezogener Daten zu einem anderen Zweck als zur Rettung und medizinischen Versorgung von Menschen verbundene Alarmierung der Polizei durch Mitglieder der Rettungsdienste der Verfolgung möglicher Straftaten oder Ordnungswidrigkeiten dient, stellt dies keinen Datenschutzverstoß dar.

Andererseits ist keine Pflicht der Bediensteten zu erkennen, die Polizei zu alarmieren. Ob eine Person im Rettungsdiensteinsatz die Polizei verständigt, ist die Entscheidung der Bediensteten beziehungsweise der Einsatzleitung.

## 6.12 Datenerhebung im Rahmen waffenrechtlicher Kontrollen

Im Rahmen einer Beschwerde wurde uns geschildert, dass das Ordnungsamt Bremen im Rahmen einer Waffenkontrolle einen registrierten Waffenbesitzer zuhause aufgesucht habe und personenbezogene Daten erhoben habe, zum Beispiel auch die aktuelle Telefonnummer

des Waffenbesitzers. Die Datenschutzkonformität dieser Maßnahme war Gegenstand einer Beschwerde nach Artikel 77 Datenschutzgrundverordnung.

Die Kontrolle der registrierten Signalpistole erfolgte datenschutzkonform. Es wurde eine Kontrolle der sicheren Aufbewahrung im Sinne der beim Ordnungsamt Bremen registrierten Waffe durchgeführt. Dabei hatte das Ordnungsamt Anlass und Zweck der Prüfung erläutert und war anhand eines vorgefertigten standardisierten Prüfprotokolls vorgegangen. Eine derartige Kontrolle beinhaltet eine Datenerhebung im Rahmen der Zuverlässigkeit und Eignung des Waffenbesitzers. Die sichere Aufbewahrung der Waffe ist ein Kriterium der Zuverlässigkeit. Im konkreten Fall hatten in den Vorjahren regelmäßig entsprechende Kontrollen stattgefunden. Bei der Kontrolle im Berichtsjahr wurden die aktuellen Informationen mit den in der Akte vorhandenen Daten abgeglichen, wozu auch die Erhebung der aktuell gültigen Telefonnummer des Waffenbesitzers gehörte.

## 6.13 Datenerhebung im Rahmen der Anzeigenerstattung beim Ordnungsamt

Wir erhielten eine Anfrage einer Person, die eine Anzeige beim Ordnungsamt wegen einer Verkehrsordnungswidrigkeit erhoben hatte. Im Anhörungsschreiben war sie namentlich als Zeugin der Ordnungswidrigkeit benannt worden, und Gegenstand der Anfrage war, ob die Preisgabe ihrer Identität an den Betroffenen im Rahmen des Ordnungswidrigkeitenverfahrens zulässig war.

Im Rahmen der Anhörung erhalten die Angeschriebenen die Gelegenheit, sich zu dem Verdacht zu äußern, sie hätten einer Ordnungswidrigkeit begangen. Damit diese ihre rechtsstaatlich verbürgten Rechte umfassend wahrnehmen können, soll im Rahmen des Anhörungsverfahrens der Tatvorwurf hinreichend konkretisiert werden. Dazu gehört die Schilderung des Tatvorwurfs, die Benennung von Beweismitteln und die namentliche Benennung von Zeug:innen des Vorgangs. Die der Begehung der Ordnungswidrigkeit Beschuldigten sollen alle Informationen erhalten, die sie benötigen, um zu entscheiden, ob und wie sie sich zur Sache äußern, das heißt zum Tatvorwurf Stellung nehmen. Je mehr Informationen ihnen zur Verfügung gestellt werden, desto besser können sie diese Entscheidung treffen. Aus diesem Grund ist es zulässig, Zeug:innen des Ordnungswidrigkeitenverfahrens bereits im Anhörungsverfahren namentlich zu benennen.

# 7. Justiz

## 7.1 Gemeldete Datenschutzverletzungen (inklusive Rechtsanwält:innen, Steuer- und Rechnungswesen)

Im Jahr 2023 wurden bei der Landesbeauftragten für Datenschutz und Informationsfreiheit durch die Staatsanwaltschaft Bremen als verantwortliche Stelle zwei Datenschutzverletzungen gemeldet. Im ersten Fall war auf dem Postweg eine Ermittlungsakte verloren gegangen; im zweiten Fall ging es um den rechtswidrigen Abruf von Daten aus dem internen Informationssystem web.sta.

Von Rechtsanwält:innen und Notar:innen wurden der Landesbeauftragten für Datenschutz und Informationsfreiheit im Berichtsjahr sechs Verletzungen des Schutzes personenbezogener Daten nach Artikel 33 Datenschutzgrundverordnung gemeldet. Vier Fälle davon hatten den Fehlversand anwaltlicher Schreiben an unberechtigte Empfänger:innnen zum Gegenstand (siehe hierzu Ziffer 7.2 dieses Berichts).

Im Berichtsjahr wurden durch Angehörige der steuerberatenden Berufe neun Fälle von Datenschutzverletzungen gemeldet. Außerdem wurde durch die bremische Finanzverwaltung eine Datenschutzverletzung gemeldet. In vier Fällen war Ursache der Datenschutzverletzungen der Fehlversand von Briefpost an falsche Empfänger:innen. In einem weiteren Fall ist ein Datenträger durch eine Beschädigung der Verpackung auf dem Postweg verloren gegangen. In vier weiteren Fällen wurde vorsorglich eine Datenschutzverletzung durch Angehörige der steuerberatenden Berufe gemeldet, weil ein IT-Dienstleister dieser Kanzleien Opfer eines Hacking-Angriffs geworden ist.

## 7.2 Datenschutzrechtliche Anforderungen an den digitalen Versand anwaltlicher Schreiben

Die Landesbeauftragte für Datenschutz und Informationsfreiheit (LfDI) erhielt im Berichtszeitraum erneut eine Beschwerde über eine Rechtsanwaltskanzlei, die anwaltliche Schreiben auf digitalem Wege an falsche Empfänger:innen versendet hatte, und vier entsprechende "Datenpannen"-Meldungen von Seiten der Rechtsanwält:innen selbst. Ursache für die hierin liegenden Verstöße gegen die Datenschutzgrundverordnung (DSGVO) war in den meisten Fällen die fehlerhafte Eingabe von E-Mail-Adressen durch Kanzleimitarbeiter:innen. Neben organisatorischen Maßnahmen, die fehlerhafte Datenübermittlungen verhindern können, wie beispielsweise, der Einführung des Vieraugenprinzips, einer Ausgangskontrolle durch die verantwortlichen Rechtsanwält:innen und dem Verzicht auf die manuelle Eingabe von E-Mail-Adressen liegt der Schlüssel zur Verhinderung dieser Datenschutzverletzungen im informationstechnischen Bereich.

Besondere Brisanz erhielten diese Fälle nämlich, weil die irrtümlich versandten personenbezogenen Daten, bei denen es sich zum Teil sogar um Gesundheitsdaten handelte, zumeist unverschlüsselt oder lediglich transportverschlüsselten (TLS) via E-Mail versandt worden waren und deshalb für die irrtümlich Adressierten im Klartext lesbar waren.

Nachdem wir schon in den Vorjahren wiederholt von Fällen erfahren hatten (siehe hierzu 2. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 7.2; 3. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 6.6) in denen die informationstechnischen Anforderungen der DSGVO an die elektronische Korrespondenz von Rechtsanwälten:innen per E-Mail nicht beachtet worden waren, wandten wir uns im April 2023 an die Hanseatische Rechtsanwaltskammer Bremen (RAK) mit der Bitte, unsere datenschutzrechtliche Einschätzung dieser Problematik an ihre Mitglieder weiter zu leiten.

Auch wenn die RAK und die LfDI bei der juristischen Bewertung dieser Problematik nicht in allen Punkten einig sind, gehen sie gleichermaßen davon aus, dass wohl in jeder Rechtsanwaltskanzlei auch Datenübermittlungen an Mandant:innen erfolgen, die einen besonders hohen Schutzbedarf aufweisen und deshalb – sofern sie auf digitalem Wege erfolgen sollen – ausreichend technisch abgesichert werden müssen. Insofern muss jede Rechtsanwaltskanzlei, die auf digitalem Wege kommunizieren will – wozu im Übrigen nicht allein die Kommunikation per E-Mail zählt – in technischer Hinsicht entsprechende sichere Verfahren nutzen.

Bereits im Berichtsjahr wandten sich bremische Rechtsanwaltskanzleien an uns, die entsprechende Lösungen entwickelt hatten. Wir haben angeboten, bei der Beratung der RAK zu solchen und anderen Lösungen unsere informationstechnische Expertise einzubringen und zur Kenntnis genommen, dass entsprechende Lösungen nicht bis Ende 2023 bei allen Kammermitgliedern vorhanden sein können. Konkreten Beschwerden Betroffener, die diesen Gegenstand betreffen, werden wir unabhängig davon nachgehen.

## 7.3 Umfang der Datenübermittlung der Staatsanwaltschaft an die Polizei

Im Austausch der Datenschutzaufsichtsbehörden der Bundesländer wurde im Berichtsjahr die Fragestellung diskutiert, welche Angaben Staatsanwaltschaften im Zusammenhang mit der Rückmeldung von Verfahrensausgängen nach § 482 Absatz 2 Strafprozessordnung (StPO) in Verbindung mit Nummer 11 Mitteilung in Strafsachen (MiStra) regelmäßig (von Amts wegen) an die jeweilige Polizeibehörde übermittelt werden. Dazu erfragten wir bei der Staatsanwaltschaft Bremen, ob die Staatsanwaltschaft solche Rückmeldungen regelmäßig (auch ohne vorherige Einzelanforderung) durchführt. Die Beantwortung der Anfrage steht noch aus.

## 7.4 Novellierung des Bremischen Richtergesetzes (insbesondere Zuverlässigkeitsüberprüfungen)

Von der Bremischen Bürgerschaft erhielten wir einen Gesetzentwurf zur Novellierung des Bremischen Richtergesetzes (BremRiG) mit der Bitte um Stellungnahme. Der Entwurf enthielt zunächst eine Zuverlässigkeitsüberprüfung für Bewerber:innen für die Einstellung in den richterlichen und staatsanwaltschaftlichen Dienst. Diese Prüfung sollte der Feststellung dienen, ob eine Person jederzeit für die freiheitliche demokratische Grundordnung eintreten wird (Zuverlässigkeit). Die Beurteilung der Zuverlässigkeit sollte der Einstellungsbehörde obliegen. Im Entwurf war vorgesehen, dass die Einstellungsbehörde weitgehende Recherchen zu den Bewerber:innen durchführen können und dazu ermächtigt werden sollte, zu diesem Zweck in größerem Umfang personenbezogene Daten der Personen zu erheben und zu verarbeiten. Es war vorgesehen, diese Verarbeitung durch eine Einwilligung der Bewerber:innen zu legitimieren.

In unserer Stellungnahme äußerten wir uns wie einige andere Befragte kritisch zu diesem gesetzgeberischen Vorhaben. Letztlich beschränkte der Gesetzgeber die Modalitäten für die Überprüfung auf solche von Bewerber:innen, die bereits in die engere Auswahl gelangt waren und schränkte diese auch quantitativ ein. Beispielsweise soll die Mitwirkung des Landesamts für Verfassungsschutz als mögliche Maßnahme nunmehr nur bei großen Zweifeln an der Eignung einer Person genutzt werden können.

Das Gesetz wurde mittlerweile verabschiedet und trat am 28. Februar 2023 in Kraft.

Nach § 11 des Gesetzes besteht die Befugnis, für die Feststellung der Verfassungstreue der Bewerber:innen in der engeren Auswahl Informationen aus öffentlich zugänglichen Quellen einzuholen sowie in Zweifelsfällen das Landesamt für Verfassungsschutz um Mitwirkung zu ersuchen. Absatz 1 enthält eine Ermächtigungsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten wie zum Beispiel ethnische Zugehörigkeit und weltanschauliche Überzeugungen. Hierzu übermittelt die Einstellungsbehörde der Verfassungsschutzbehörde den Namen, den Vornamen, den Geburtsnamen, das Geburtsdatum, den Geburtsort, das Geschlecht und die Staatsangehörigkeit der Bewerberin oder des Bewerbers. Sofern bei der Verfassungsschutzbehörde nach § 3 Absatz 1 Satz 1 Nummer 1 bis 4 des Bremischen Verfassungsschutzgesetzes Erkenntnisse zu der Person vorliegen, übermittelt sie diese im Falle eines Auskunftsersuchens nach Satz 2 an die Einstellungsbehörde. Die Gesetzesnovelle enthält die Möglichkeit, eine entsprechende Überprüfung auch bei ehrenamtlichen Richter:innen durchzuführen.

# 8. Gesundheit

## 8.1 Gemeldete Datenschutzverletzungen

Im Berichtsjahr wurden uns im Bereich Gesundheit insgesamt 27 Datenschutzverletzungen gemeldet. Neben Fehlsendungen und Diebstählen von Datenträgern fiel auf, dass Gesundheitseinrichtungen vermehrt Opfer von Cyberangriffen geworden sind.

### 8.1.1 Einbruch in Außenstelle des Gesundheitsamts Bremen

Das Gesundheitsamt Bremen informierte uns im Berichtsjahr über einen Einbruch in einer seiner Außenstellen. Hierdurch hätten Unbefugte Zugang zu personenbezogenen Daten mehrerer tausend Personen erhalten. Alle Schränke, in denen Akten aufbewahrt werden, seien bei dem Vorfall geöffnet worden. Es stellte sich heraus, dass die Schränke teilweise nicht abschließbar waren. Die abschließbaren Schränke wurden mit Schlüsseln geöffnet, die in den Räumlichkeiten vermeintlich versteckt worden waren.

Wir forderten das Gesundheitsamt auf, zukünftig auf das Verstecken von Schlüsseln zu verzichten und stattdessen die Schlüssel an diejenigen Beschäftigten auszuhändigen, die die verschlossenen Akten für die Erfüllung ihrer Aufgaben benötigen. Die Nutzung von abschließbaren Schränken als organisatorische Maßnahme zur Datensicherheit gemäß Artikel 32 Datenschutzgrundverordnung bleibt anderenfalls nahezu wirkungslos.

### 8.1.2 Cyberangriffe auf Einrichtungen der Gesundheitsversorgung

Auffällig war im laufenden Berichtsjahr, dass uns im Vergleich zu vorherigen Jahren vermehrt Vorfälle von Cyberkriminalität bei Gesundheitseinrichtungen gemeldet wurden. Die Angriffe erfolgten in Form von Phishing-Attacken oder auch gezielten Hackerangriffen. Der Schaden für die betroffenen Personen ist in solchen Fällen häufig nicht unmittelbar spürbar. Wenn der Angriff mit einem Abfluss von sensiblen Gesundheitsdaten einhergeht, führt dies jedoch zu einem Kontrollverlust über Daten, die ursprünglich nur für Kenntnis einer Berufsgeheimnisträgerin beziehungsweise eines Berufsgeheimnisträgers bestimmt waren. Dies kann auf Seiten der betroffenen Personen zu einem erheblichen Vertrauensverlust in die verantwortlichen Stellen führen.

Erfreulicherweise zeigten die bei uns gemeldeten Fälle bereits eine hohe Sensibilisierung für die Gefahren von Cyberangriffen bei den Verantwortlichen. Hierdurch wurden oftmals bereits unmittelbar nach einer Kenntnisnahme Maßnahmen ergriffen, durch die die Folgen des Angriffs abgemildert wurden beziehungsweise ein weiterer Datenabfluss unterbunden werden konnte. Um im Falle eines Angriffs die nötigen Schritte parat zu haben, empfehlen wir, dass

sich Verantwortliche frühzeitig mit der Gefahr von Cyberangriffen auseinandersetzen und Strategien und Konzepte für den Ernstfall entwickeln.

## 8.2 Hackerangriff auf den Klinikverbund Gesundheit Nord

Im Mai des Berichtsjahres meldete der Klinikverbund Gesundheit Nord uns einen Angriff auf ihre IT-Infrastruktur, bei dem personenbezogene Daten von Patient:innen und Beschäftigten abgeflossen waren. Angreifer hatten die Zugangsdaten für die VPN-Verbindung zum Netz der Gesundheit Nord über ein kompromittiertes Notebook eines Dienstleisters erlangt. Mit den erbeuteten Zugangsdaten erhielten die Angreifer die Passwörter für andere Nutzer:innenkonten und gelangten so zu personenbezogenen Daten, die auf einer Dateiablage gespeichert waren. Diese wurde vom Bereich Verwaltung, von diversen klinischen Bereichen und Einzelnutzer:innen verwendet. Die Angreifer kopierten Daten in einem erheblichen Umfang. Laut den durchgeführten Ermittlungen wiesen etwa 600.000 der Datensätze einen Personenbezug auf. Die kopierten Datensätze wurden auf ausländischen Servern entdeckt, konnten dort jedoch mithilfe der Polizei sowie des Bundeskriminalamtes zeitnah gelöscht werden.

Die Aufarbeitung des Vorfalles erfolgte in enger Abstimmung mit uns. Im Verfahren stellte sich heraus, dass bei einigen der betroffenen Datensätze Aufbewahrungsfristen bereits überschritten waren und die Dokumente teilweise doppelt angelegt worden waren. Mit einer konsequenteren Umsetzung bei der Löschung hätte der Schaden geringer ausfallen können. Die Gesundheit Nord hat mit der Bereinigung der Daten begonnen und plant, diese im Jahr 2024 abzuschließen. Zudem wurde durch eine Vielzahl an Maßnahmen die IT-Infrastruktur des Klinikverbundes weiter "gehärtet", sodass Angriffe früher erkannt werden und potenzielle Schäden so gering wie möglich gehalten werden können.

Dieser Fall zeigt anschaulich, dass zügiges Handeln und Einschalten der zuständigen (Ermittlungs-)Behörden dazu beitragen können, das Ausmaß eines Angriffes und dessen Schaden für die betroffenen Personen zu begrenzen. Er legt allerdings auch Schwachstellen bei der verantwortlichen Stelle offen, die es gilt, schnellst möglichst zu beheben.

## 8.3 Versand von Terminerinnerungen durch Arztpraxen

Regelmäßig erreichen uns Beschwerden über den Versand von Terminerinnerungen per E-Mail und/oder SMS durch Arztpraxen oder Krankenhäuser. In vielen Fällen werden Dienstleister mit dieser Aufgabe beauftragt. Patient:innen beklagen häufig, nicht darüber informiert worden zu sein, dass ihre Termindaten zu diesem Zweck an ein Unternehmen übertragen werden.

Das Versenden von Terminerinnerungen stellt eine Zusatzleistung von Praxen dar, welche nicht Teil der ärztlichen Behandlung ist. Die Verarbeitung von Kontaktdaten wie E-Mail-Adressen und Telefonnummern ist daher zu diesem Zweck nur zulässig, wenn der beziehungsweise die Patient:in gegenüber der Praxis in die Datenverarbeitung eingewilligt hat. Die Einwilligung muss informiert erfolgen, was auch eine Information darüber erfordert, dass die Erinnerungen nicht von der Praxis selbst, sondern von einem Dienstleister verschickt werden. Zum Zwecke der Nachweisbarkeit sollten Praxen Einwilligungen schriftlich einholen oder zumindest schriftlich dokumentieren.

Die Praxis oder das Krankenhaus bleibt für die datenschutzkonforme Verarbeitung der Patient:innendaten verantwortlich. Ein besonderes Augenmerk sollte daher auf die Auswahl des Dienstleisters gelegt werden. Es muss unter anderem sichergestellt sein, dass nur diejenigen Daten an den Dienstleister übertragen werden, die dieser für die Erfüllung seiner Aufgabe benötigt. Zudem müssen sich auch die Geheimhaltungspflichten auf den Dienstleister und möglichen Unterauftragnehmern erstrecken. Die konkrete Datenverarbeitung sowie die Rechte und Pflichten der Parteien sind in einer Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 Absatz 3 Datenschutzgrundverordnung festzuhalten.

## 8.4 Keine Erstattung der Anwaltskosten des Verantwortlichen durch den/die Beschwerdeführer:in

In einem Beschwerdeverfahren gegen eine Arztpraxis ließ sich die verantwortliche Ärztin durch einen Rechtsanwalt vertreten. Die Beschwerde betraf einen Antrag auf Auskunft nach Artikel 15 Datenschutzgrundverordnung (DSGVO). Da die Auskunft auch nach Ablauf der gesetzlich zugestandenen Monatsfrist nicht erteilt worden war, bat die betroffene Person um unsere Unterstützung. Die Praxis forderte den Antragsteller auf, eine schriftförmliche Einwilligung zu erteilen, damit die von der vorherigen Praxisinhaberin geführten Behandlungsakte beauskunftet werden könne. Der Antragsteller erteilte seine Einwilligung per E-Mail. In einem anschließenden Schriftwechsel mit dem Rechtsanwalt der Praxis stellte der Rechtsanwalt dem Antragsteller die Kosten für seine anwaltliche Tätigkeit im Wege des Schadensersatzes in Rechnung, da die Vorwürfe einer angeblichen Datenschutzverletzung unbegründet gewesen seien. Das Beschwerdeverfahren war zu diesem Zeitpunkt noch nicht abgeschlossen.

Wir teilten dem beauftragten Rechtsanwalt mit, dass der Antragsteller zwar den Anlass für das von uns geführte aufsichtsbehördliche Verfahren gegeben hatte, jedoch in dem Verfahren kein Verfahrensbeteiligter war. Das Beschwerderecht gemäß Artikel 77 DSGVO ist kostenfrei. Ob sich Verantwortliche in einem dadurch eröffneten Verwaltungsverfahren anwaltlich vertreten lassen, ist ihnen überlassen. Es gibt keine rechtliche Grundlage dafür, etwaige Anwaltskosten auf Beschwerdeführer:innen abzuwälzen. Betroffene Personen würden anderenfalls

abgeschreckt, datenschutzrechtliche Aufsichtsbehörden über mögliche Datenschutzverstöße zu informieren. Es ist gerade nicht notwendig, dass die betroffene Person den Verstoß schlüssig darlegt und rechtlich würdigt (unter anderem Bergt in Kühling/Buchner, DS-GVO BDSG, Artikel 77 DSGVO Randnummer 10). Vielmehr genügt es, den Sachverhalt in einer prüfbaren Weise darzulegen. Selbst wenn das Ergebnis der Prüfung durch die Aufsichtsbehörde ergibt, dass kein Datenschutzverstoß vorliegt, sind hierdurch bei dem Verantwortlichen entstandene Kosten von diesem selbst zu tragen. Möglichkeiten der Kostenerstattung durch die betroffene Person können sich allenfalls im Rahmen von zivilrechtlichen Auseinandersetzungen, etwa bei der Geltendmachung von Schadensersatzansprüchen, ergeben.

## 8.5 Angebot an Bremer Schüler:innen zur Durchführung von HPV-Impfungen durch das Gesundheitsamt Bremen

Durch eine Beschwerde erfuhren wir, dass das Gesundheitsamt Bremen in den Schulen der Stadt Bremen über die Empfehlung der Ständigen Impfkommission für Mädchen und Jungen im Alter von 9 bis 14 Jahren informiert, sich gegen Humane-Papillom-Viren (HPV) impfen zu lassen. Das Gesundheitsamt bietet dabei auch an, die Impfung in den Schulen oder im Gesundheitsamt durchführen zu lassen. Die Eltern werden über einen Fragebogen um Mitteilung gebeten, ob bereits eine Impfung vorgenommen wurde und ob eine Impfung gewünscht ist. Wenn das Kind geimpft werden soll, werden zusätzlich Fragen zum Gesundheits- und Versicherungsstatus abgefragt.

Hinsichtlich der uns vorgelegten Dokumente und der beschriebenen Verfahrensweise äußerten wir datenschutzrechtliche Bedenken. Vor dem Hintergrund, dass die Inanspruchnahme einer HPV-Impfung nicht verpflichtend ist, war beispielsweise unklar, wie bei dem Ausfüllen des Fragebogens die Freiwilligkeit gewährleistet werden kann. Wir forderten diesbezüglich, die Information an die Eltern klar und transparent zu formulieren und Lehrer:innen dahingehend zu sensibilisieren, dass der Rücklauf des Fragebogens freiwillig ist und nicht mit einer Klassenliste nachverfolgt werden darf. Zudem tauschten wir uns mit dem Gesundheitsamt Bremen über die Rechtsgrundlagen der Datenverarbeitung sowie die Datenschutzinformation aus und baten um Anpassungen.

Wir sind optimistisch, dass unsere Anmerkungen bald umgesetzt werden und auf diese Weise dazu beigetragen werden kann, dass personenbezogene Daten von Schüler:innen im Zusammenhang mit der HPV-Impfung nur dann verarbeitet werden, wenn sich ihre Erziehungsberechtigten für eine Impfung entscheiden oder die Daten ihrer Kinder freiwillig bereitstellen.

## 8.6 Erstellung von Gutachten durch den Amtsärztlichen Dienst

Im Berichtsjahr erhielten wir mehrere Beschwerden von betroffenen Personen zu der Verarbeitung ihrer Daten in Zusammenhang mit Einstellungsuntersuchungen durch den Amtsärztlichen Dienst im Gesundheitsamt Bremen. In Bezug auf das Verfahren bei angehenden Tarifbeschäftigten und angehenden Beamt:innen gibt es unterschiedliche Regelungen. Während das Bremische Beamtengesetz sowie auch das Bundesbeamtengesetz ausdrücklich vorschreiben, dass den betroffenen Personen eine Kopie des Gesundheitszeugnisses übermittelt wird, gibt es eine solche Vorschrift für angehende Tarifbeschäftigte nicht. Zwar erhalten diese in Bremen auf Wunsch eine Kopie, hierzu müssen Sie sich jedoch aktiv an das Gesundheitsamt wenden. Um diese unterschiedliche Behandlung zukünftig auszugleichen empfahlen wir dem Gesundheitsamt, bereits zum Zeitpunkt der Datenerhebung über den Gesundheitsfragebogen abzufragen, ob die betroffene Person eine Kopie des Gesundheitszeugnisses erhalten möchte. Auf diese Weise wird die Transparenz des Verfahrens befördert und es kann vermieden werden, dass die betroffene Person erst mit der Entscheidung des potenziellen Dienstherrn von dem Ergebnis der Untersuchung erfährt. In Bezug auf die Ausgangfälle stellte sich heraus, dass betroffene Personen offenbar in zwei Fällen unzureichend informiert worden waren.

## 8.7 Einsichtnahme in Patient:innenakten durch Nationale Stelle zur Verhütung von Folter

Seitens der Senatorin für Gesundheit, Frauen und Verbraucherschutz wurde die Frage an uns herangetragen, ob die Mitglieder der Nationalen Stelle zur Verhütung von Folter bei dem Besuch in einer öffentlichen-rechtlichen Unterbringungseinrichtung eine Einwilligung der betroffenen Person einholen müssen, um Einsicht in deren Patient:innenakte zu erhalten.

Die Nationale Stelle zur Verhütung von Folter ist eine unabhängige nationale Einrichtung zur Prävention von Folter und Misshandlung in Deutschland. Im Rahmen Ihrer Tätigkeit besucht sie regelmäßig Orte der Freiheitsentziehung. Ihre Einrichtung beruht auf dem Zusatzprotokoll zu dem Übereinkommen der Vereinten Nationen gegen Folter und andere grausame, unmenschliche oder erniedrigende Behandlung oder Strafe. Danach soll ihren Mitgliedern Zugang zu allen Informationen gewährt werden, welche die Behandlung der betroffenen Personen und die Bedingungen der Freiheitsentziehung betreffen. Hierfür hat der bremische Gesetzgeber in § 89 Bremisches Gesetz über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten (BremPsychKG) ein Einsichtsrecht in die Akten der untergebrachten Personen statuiert. Nach unserer Einschätzung hat der Gesetzgeber damit den durch die Datenschutzgrundverordnung (DSGVO) vorgegebenen Rahmen für die Verarbeitung von Gesundheitsdaten eingehalten. Artikel 9 Absatz 2 Buchstabe g DSGVO gestattet es dem

Gesetzgeber, die Verarbeitung von Gesundheitsdaten auf gesetzlicher Basis zu erlauben, wenn dies aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist. Eine zusätzliche Einwilligung der betroffenen Person muss dann nicht mehr eingeholt werden. Das Einsichtsrecht soll dazu beitragen, eine menschenwürdige Unterbringung zu gewährleisten und die Rechtsgüter der in besonderem Maße schutzbedürftigen Betroffenen zu wahren.

Nach unserer Auffassung hat der Gesetzgeber in der geschaffenen Regelung geeignete Maßnahmen getroffen, um das Grundrecht auf Datenschutz und die Menschenwürde sowie das Recht auf körperliche Unversehrtheit in Einklang zu bringen.

# 9. Soziales

## 9.1 Gemeldete Datenschutzverletzungen

Im Berichtsjahr wurden uns im Bereich Soziales insgesamt 16 Datenschutzverletzungen gemeldet hat. Der Großteil der Meldungen betraf Einbrüche in Kindertageseinrichtungen und den Verlust von Akten beziehungsweise Dokumenten.

## 9.2 Umgang mit Fotos von Kindern in Kindertageseinrichtungen

Im Laufe des Jahres wurden uns mehrere Einbrüche in Kindertageseinrichtungen gemeldet. Bei diesen wurden elektronische Geräte und Speichermedien entwendet, auf denen sich Fotos aus den jeweiligen Einrichtungen befanden. Neben Fotos von Beschäftigten befanden sich vor allem Fotos von Kindern aus den Einrichtungen auf den entwendeten Geräten. Die betroffenen Geräte waren in allen Fällen nicht durch ausreichende technische Maßnahmen, wie beispielsweise eine Festplattenverschlüsselung, geschützt.

Der öffentliche Träger KiTa Bremen hat nach unserem Tätigwerden durch den Erlass einer neuen Dienstanweisung zur Speicherung von digitalen Daten innerhalb der Einrichtungen auf die Vorfälle reagiert. Diese sieht insbesondere vor, dass personenbezogene Daten nur noch auf zentral verwalteten PCs mit Festplattenverschlüsselung verarbeitete werden dürfen. Auch der Umgang mit in den Einrichtungen erstellten Fotos wird in der neuen Dienstanweisung konkretisiert. So werden die auf den zentral beschafften PCs gespeicherten Fotos gelöscht, sobald ihre Speicherung nicht mehr erforderlich ist. Auch bei Speicherkarten werden in regelmäßigen Abständen Löschungen vorgenommen.

## 9.3 Unzureichender Datenschutz bei freiem Träger der Kinder- und Jugendhilfe

Auf der Grundlage eines anonymen Hinweises prüften wir im Berichtsjahr die Umsetzung datenschutzrechtlicher Vorgaben bei einem freien Träger der Kinder- und Jugendhilfe. Der

Schwerpunkt unserer Prüfung lag auf der Umsetzung technischer und organisatorischer Maßnahmen der Datensicherheit. Dabei stellten wir fest, dass der Träger zur Kommunikation mit Klient:innen unter anderem den Messengerdienst WhatsApp einsetzte. Die Nutzung dieses Messengers führt zu einer Übermittlung von Daten auf Server außerhalb der Europäischen Union, für die es im Regelfall keine Rechtsgrundlage gibt. Dies ist gerade bei der Verarbeitung von Sozialdaten hochproblematisch. Wir forderten den Träger daher auf, nach einer alternativen Lösung zu suchen.

Im Rahmen unserer Prüfung stellten wir darüber hinaus Mängel bei der Sicherheit von Endgeräten fest, die nicht über Festplattenverschlüsselungen verfügten. Zudem bestanden Mängel bei der Dokumentation, da weder Löschkonzept noch Verfahrensverzeichnisse vorhanden waren. In einem persönlichen Termin erörterten wir die festgestellten Mängel und forderten eine umgehende Behebung.

Der Träger kam unserer Aufforderung zügig nach und besserte nach. Er teilte mit, dass alle Festplatten nun verschlüsselt seien und ein Löschverfahren entwickelt worden sei. Ebenso wurde für die Kommunikation mit Klient:innen eine sicherere Alternative gefunden. Zum Redaktionsschluss stehen noch einige letzte Nachbesserungen bei den Dokumentationspflichten aus, die auf Seiten des Trägers noch nicht fertig gestellt werden konnten.

## 9.4 Unzulässige Veröffentlichung von Prüfungsergebnissen durch Aus- und Weiterbildungsträger

Wir erhielten eine Beschwerde einer betroffenen Person, die bei einem Aus- und Weiterbildungsträger an einer Umschulungsmaßnahme teilgenommen hatte. Nachdem sie die Abschlussprüfung abgelegt hatte, sei sie darauf aufmerksam geworden, dass ein Foto ihres Zeugnisses durch den Geschäftsführer des Trägers veröffentlicht worden war. Hierbei sei zwar nicht der Name, jedoch die genaue erreichte Punktzahl lesbar gewesen. Zudem sei das Foto so kommentiert worden, dass Rückschlüsse auf die betroffene Person möglich gewesen seien. Die uns vorgelegten Screenshots konnten dies bestätigen.

Der Fall macht deutlich, dass die Datenschutzgrundverordnung aus gutem Grund nicht nur eindeutig identifizierte Personen schützt, sondern auch die Verarbeitung von Daten reguliert, die personenbeziehbar sind. Gemeinsam mit der vorliegend recht negativen Kommentierung des Fotos ist der Rückschluss nicht nur für den Ersteller des Fotos, sondern auch für weitere Personen wie etwa Mitschüler:innen möglich. Es bedarf somit auch für eine derartige Veröffentlichung einer rechtlichen Grundlage. Fehlt diese, liegt ein Datenschutzverstoß vor.

## 9.5 Akteneinsichtsrecht von Abgeordneten der Bremischen Bürgerschaft bei Sozialbehörden

Uns erreichten zwei Beratungsanfragen des Amts für Jugend, Familie und Frauen zum Einsichtsrecht von Abgeordneten der Bremischen Bürgerschaft beziehungsweise Mitgliedern der Stadtverordnetenversammlung Bremerhaven in Akten eines durch das Amt untergebrachten Minderjährigen.

Nach Artikel 99 der Bremische Landesverfassung hat jedes Mitglied der Bremischen Bürgerschaft das Recht, Einsicht in Akten der Verwaltung zu nehmen. Da die Gewährung einer Akteneinsicht zwangsläufig mit einer Offenlegung personenbezogener Daten einhergeht, kamen wir auch hinsichtlich der Akteneinsicht im Rahmen der parlamentarischen Kontrollrechte zu dem Ergebnis, dass sich diese an den Regelungen der Datenschutzgrundverordnung messen lassen muss. Vorliegend kam nur eine Verarbeitung nach Artikel 6 Absatz 1 Buchstabe e Datenschutzgrundverordnung in Betracht. Danach ist eine Verarbeitung dann rechtmäßig, wenn sie für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt. Die Verarbeitung von personenbezogenen Daten durch Sozialbehörden ist durch das Sozialgeheimnis geschützt und wird nach § 35 Absatz 2 Erstes Buch Sozialgesetzbuch (SGB I) grundsätzlich abschließend in den Sozialgesetzbüchern geregelt. Die Rechtmäßigkeit der Offenlegung der Daten im Rahmen der Akteneinsicht müsste sich also aus einer Regelung der Sozialgesetzbücher ergeben. Eine Regelung zur Akteneinsicht durch Abgeordnete gibt es indes in den Sozialgesetzbüchern nicht.

Vor dem Hintergrund, dass sich eine Zulässigkeit der Offenlegung von Sozialdaten an Abgeordnete nicht aus den Sozialgesetzbüchern ergibt, war zu prüfen, ob aus dem parlamentarischen Kontrollrecht selbst eine solche Offenlegungsbefugnis entnommen werden kann. Dies bejahten wir grundsätzlich. Allerdings gilt auch dieses Recht nicht schrankenlos. Nach Artikel 99 Absatz 3 Bremische Landesverfassung darf die Akteneinsicht ausnahmsweise abgelehnt werden, wenn überwiegende Belange des Betroffenen entgegenstehen. In diese Interessensabwägung floss im vorliegenden Fall nicht nur der besondere Schutz von Sozialdaten, sondern auch die Schutzbedürftigkeit von Kindern ein. Es sprach daher vieles dafür, dass die Interessen des betroffenen Minderjährigen das Auskunfts- und Kontrollinteresse überwogen.

Das Recht auf Akteneinsicht für Mitglieder der Stadtverordnetenversammlung ist in § 23 Absatz 4 Satz 4 der Verfassung für die Stadt Bremerhaven (VerfBrhv) geregelt. Wir gelangten diesbezüglich zu dem Ergebnis, dass im vorliegenden Fall eine Akteneinsicht abzulehnen war.

## 9.6 Datenbank Haaranalyse

Seit 2012 stehen wir mit dem Sozialressort hinsichtlich einer durch das Amt für Soziale Dienste betriebenen Datenbank zur Verwaltung von Daten aus Gutachten zu Haaranalysen zum Drogenkonsum drogenabhängiger und/oder substituierter Eltern und deren Kinder in Kontakt (siehe hierzu 38. Jahresbericht, Ziffer 8.1; 40. Jahresbericht, Ziffer 8.2; 2. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 9.6). Frühzeitig äußerten wir datenschutzrechtliche Bedenken und forderten den Verantwortlichen auf, durch geeignete Maßnahmen die datenschutzrechtlichen Anforderungen zu erfüllen. Obgleich zwischenzeitlich Anpassungen der Dokumentation erfolgt sind, liegen uns weiterhin keine Informationen vor, denen eine datenschutzkonforme Umsetzung zu entnehmen ist. Im August 2022 nahmen wir zuletzt zu den überarbeiteten Dokumentation Stellung und baten um Klarstellungen beziehungsweise Anpassungen in den Bereichen Auswertung, Datenlöschung, Anonymisierung sowie hinsichtlich der technischen und organisatorischen Maßnahmen zur Datensicherheit. Eine Beantwortung unseres Schreibens erfolgte bis zum Redaktionsschluss trotz mehrfacher Erinnerung im Laufe des Berichtsjahres nicht. Uns wurde lediglich mitgeteilt, dass derzeit eine Überführung der Datenbank in ein Fachverfahren geprüft werde. Obwohl es sich hierbei offenbar um einen längeren Prüfprozess handelt, findet seitens des Sozialressorts bedauerlicherweise keine erkennbare Bemühung statt, die Datenbank zwischenzeitlich datenschutzkonform zu betreiben.

# 10. Bildung

## 10.1 Gemeldete Datenschutzverletzungen

Im Bereich Schulen und Bildung gab es im Berichtsjahr acht Meldungen verantwortlicher Stellen nach Artikel 33 Datenschutzgrundverordnung. Hierbei betrafen zwei Meldungen die Schulen, drei weitere die Hochschulen im Land Bremen. Eine weitere Meldung erfolgte seitens der Senatorin für Kinder und Bildung hinsichtlich eines unbefugten Zugriffs im Rahmen der Nutzung der iCloud. Auch erreichten uns erneut diverse telefonische Beratungsanfragen. Zentrales Thema waren hierbei zumeist Fragen zur Zulässigkeit der Übermittlung personenbezogener Daten von Schüler:innen.

## 10.2 Sprachstandsfeststellung – Institut für Qualitätsentwicklung im Land Bremen (IQHB)

Uns erreichte eine Eingabe hinsichtlich des Verfahrens zur Sprachstandsfeststellung, welches durch das Institut für Qualitätsentwicklung im Land Bremen (IQHB) durchgeführt wird. Der sogenannte PRIMO-Sprachtest wird ein Jahr vor der Einschulung durchgeführt, mit dem Ziel, einen möglichen Sprachförderbedarf zu ermitteln und gegebenenfalls bei der Sprachförderung

unterstützen zu können. Von unserer Seite bestanden aufgrund der übermittelten Unterlagen zunächst erhebliche datenschutzrechtliche Bedenken, die jedoch im Laufe der Prüfung durch vorgenommene Anpassungen teilweise beseitigt wurden. Wir bemängelten unter anderem die fehlenden Datenschutzinformationen für die Erziehungsberechtigten vor Durchführung der Sprachstandsfeststellung. Hier erfolgte zeitnah eine Nachbesserung, sodass die Anschreiben nunmehr einen Hinweis auf die Datenschutzinformationen enthalten und diese auch online zugänglich sind. Aus der uns vorgelegten Verfahrensbeschreibung ergaben sich auch Unklarheiten hinsichtlich der datenschutzrechtlichen Verantwortlichkeit. So war hieraus nicht ersichtlich, ob das IQHB die Sprachstandsfeststellung als Verantwortlicher im Sinne der Datenschutzgrundverordnung (DSGVO) durchführt oder ob es sich um eine Verarbeitung im Auftrag der Senatorin für Kinder und Bildung handelt. Im Rahmen der Prüfung konnte hier jedoch eine Klärung herbeigeführt werden. Aufgrund der Weisungsgebundenheit liegt eine Auftragsverarbeitung vor. Das IQHB sagte in diesem Zusammenhang zu, unsere Anregung, den Auftragsverarbeitungsvertrag sowie die Verfahrensbeschreibung zu konkretisieren, umzusetzen. Auch eine zeitnahe Umsetzung von erforderlichen Änderungen im Verfahren zur Erteilung von Auskünften nach Artikel 15 DSGVO wurde zugesagt. Hinsichtlich weiterer offener Punkte sind wir mit dem IQHB weiterhin im Gespräch. Dies betrifft unter anderem die datenschutzrechtlichen Bedenken bezüglich der Rechtsgrundlage für die Übermittlung der Ergebnisse der Sprachstandsfeststellungen an die Kindergärten.

## 10.3 Nutzung der iCloud an bremischen Schulen

Die Senatorin für Kinder und Bildung hat in einer Mitteilung (Mitteilung Nummer 296/2021) die Nutzung der iCloud für schulische Endgeräte für zulässig erachtet. Aus der Mitteilung ergibt sich, dass vom behördlichen Datenschutzbeauftragten die Risiken und Möglichkeiten zur Ausweitung der Datenspeicherung in der iCloud geprüft worden seien und dass auf Grundlage der von Apple in einem Prüfgespräch gelieferten Informationen und der Dokumentation der technischen und organisatorischen Maßnahmen, sowie den vertraglichen Rahmenbedingungen die Nutzung der iCloud im schulischen Kontext auch für die Verarbeitung personenbezogener Daten mit normalem Schutzbedarf als vertretbar eingestuft werde. Eine vorherige Unterrichtung der Landesbeauftragten für Datenschutz und Informationsfreiheit war nicht erfolgt.

Wir forderten die Senatorin für Kinder und Bildung daher zunächst auf, uns die Datenschutz-Folgenabschätzung gemäß Artikel 35 Datenschutzgrundverordnung (DSGVO) vorzulegen. Eine solche war aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung vorliegend erforderlich. Die übermittelten Unterlagen konnten unsere datenschutzrechtlichen Bedenken nicht ausräumen.

Nach § 2 Absatz 1 Bremisches Schuldatenschutzgesetz (BremSchulDSG) dürfen personenbezogene Daten über Schüler:innen und deren Erziehungsberechtigte verarbeitet werden, soweit es zur Erfüllung ihres Unterrichts- und Erziehungsauftrages, zum Übergang vom Elementarbereich in den schulischen Bereich, zur Wahrnehmung der Aufgaben zur Betreuung von Schulkindern, zur besonderen Förderung, zur Durchführung sonstiger schulischer Aktivitäten oder zur Wahrnehmung gesetzlicher Mitwirkungsrechte erforderlich ist. Diese Voraussetzungen sind jedoch nach aktuellem Stand nicht erfüllt. Aus den übermittelten Unterlagen ergab sich unter anderem, dass für die Dateiablage die etablierten Systeme wie itslearning genutzt werden. Dementsprechend bestehen bereits Zweifel hinsichtlich der Erforderlichkeit der Nutzung der iCloud.

Auch die Freiwilligkeit der Nutzung ist in diesem Zusammenhang höchst problematisch. Zweifel an einer Freiwilligkeit der Nutzung ergaben sich insbesondere aus den Angaben in der Datenschutzinformation für die Schüler:innen, wonach die verarbeiteten personenbezogenen Daten für die Erfüllung des Unterrichts- und Erziehungsauftrages erforderlich sind. Dies steht im klaren Widerspruch zu einer freiwilligen Nutzung. Ein konkretes Konzept, das sicherstellt, dass auch die Daten der Schüler:innen, die die iCloud nicht nutzen wollen, gesichert werden, wurde nicht vorgelegt.

Weitere Bedenken ergaben sich, da in der iCloud nach den vorgelegten Unterlagen unter anderem auch Unterrichtsdaten, Kalenderdaten, Kontaktdaten, der Verlauf in Safari, Lesezeichen, Fotos und Sprachmemos verarbeitet werden. Hier kann unseres Erachtens, entgegen der Einschätzung der Senatorin für Kinder und Bildung nicht lediglich von einem normalen Schutzbedarf ausgegangen werden.

Problematisch ist darüber hinaus, dass nach Angaben der Senatorin für Kinder und Bildung bezüglich des Speicherortes der personenbezogenen Daten in der iCloud nicht sichergestellt werden kann, dass ausschließlich Rechenzentren in der Europäischen Union genutzt werden. Wir wiesen daher darauf hin, dass personenbezogene Daten nur aus einem Auftragsverarbeitungsverhältnis in die Vereinigten Staaten von Amerika übermittelt werden dürfen, soweit der Auftragsverarbeiter zusätzliche Maßnahmen in erforderlichem Umfang im Sinne der Rechtsprechung des Europäischen Gerichtshofes (Schrems II) trifft sowie der Empfehlung des Europäischen Datenschutzausschusses 1/2020 gegen Zugriffe von US-Behörden nachkommt.

Auf unsere Nachfragen, wie sichergestellt wird, dass personenbezogene Daten der Schüler:innen, Eltern und Beschäftigten nicht nach gesetzlichen US-Normen offengelegt werden, erhielten wir bisher keine Rückmeldung. Dies gilt ebenso für die Frage, wie sichergestellt wird, dass sämtliche personenbezogenen Daten von Apple nach Ende des Datenverarbeitungsvertrages im Sinne von Artikel 28 Absatz 3 Buchstabe g DSGVO gelöscht

oder an die Schulen zurückgegeben und dann gelöscht werden. Aufgrund der bestehenden Bedenken, wiesen wir die Senatorin für Kinder und Bildung darauf hin, dass die Nutzung der iCloud rechtswidrig und einzustellen ist, sofern kein ausreichender Nachweis erfolgt, dass die Anforderungen des europäischen Datenschutzrechtes eingehalten werden.

## 10.4 Aushang einer Notenliste im Klassenraum

Die Landesbeauftragte für Datenschutz und Informationsfreiheit erreichte ein Hinweis, dass in einer Schule eine Notenliste im Klassenraum ausgehängt worden sei. Nach Angaben der Schule habe dies dazu gedient nach einer Gruppenarbeit eine Vergleichbarkeit der einzelnen Noten herzustellen und den Schüler:innen zu zeigen, wer mit welchen Leistungen welche Note erlangt hat. Bei den Noten für ausgeführte schulische Aufgaben oder Klassenarbeiten handelt es sich um personenbezogene Daten. Die Bekanntgabe dieser Noten vor der ganzen Klasse, zum Beispiel durch Vorlesen oder durch einen Aushang, stellt eine Übermittlung von personenbezogenen Daten dar, welche einer Rechtsgrundlage bedarf. Eine solche war hier nicht gegeben, insbesondere ist der Aushang einer mit Namen versehenen Notenliste nicht zur Erfüllung des Unterrichts- und Erziehungsauftrages im Sinne des § 2 Absatz 1 Bremisches Schuldatenschutzgesetz erforderlich. Die Bekanntgabe der Noten kann ebenso unter vier Augen stattfinden. Die Verkündung der Noten gegenüber der ganzen Klasse greift insbesondere hinsichtlich der Schüler:innen, die eine schlechte Note erhalten haben, unverhältnismäßig in deren Persönlichkeitsrechte ein. Wir haben die Schule daher unter Verweis auf die datenschutzrechtliche Unzulässigkeit des Aushanges von Notenlisten aufgefordert, derartige Aushänge zukünftig zu unterlassen.

## 10.5 IT-Sicherheitslücke bei der Universität Bremen

Einem Pressebericht im Februar des Berichtsjahres konnten wir entnehmen, dass das Computer-Netzwerk der Universität Bremen zeitweise eine Sicherheitslücke aufwies und auch Spuren eines bereits vollzogenen Hackerangriffs gefunden worden waren. Wir forderten die Universität daher umgehend zur Stellungnahme auf und erhielten die Rückmeldung, dass die Universität unmittelbar nach Bekanntwerden der Sicherheitslücke sowie des Hackerangriffs tätig geworden sei. Die Sicherheitslücke sei noch am selben Tag geschlossen worden und ein Verlust personenbezogener Daten habe ausgeschlossen werden können.

# 11. Bau, Wohnen, Umwelt, Energie und Verkehr

## 11.1 Gemeldete Datenschutzverletzungen

Im Bereich Wohnen, Bau, Verkehr, Energie und Umwelt erreichten uns im Jahr 2023 insgesamt 21 Meldungen von Datenschutzverletzungen nach Artikel 33 Absatz 1

Datenschutzgrundverordnung. In einem Vorgang hatte sich ein Mitarbeiter eines Dienstleisters mit seinem dienstlichen Account Zugang zu den Daten einer Mitbewohnerin seines Hauses verschafft. Weitere Varianten waren unter anderem vielfach "Klassiker" wie fehlgeleitete Kund:innen- oder Mieter:innenschreiben. Inhalt einer dieser Meldungen war, dass ein Kundenschreiben aufgrund von Namensgleichheit an die falsche Person versendet wurde. In einigen weiteren Datenpannenmeldungen waren fehlerhafte Datenzusammenführungen im internen Kund:innenführungssystemen eines Unternehmens Auslöser für die entstandene Datenschutzverletzung, woraufhin wir das Unternehmen auf eine Ausbesserung seiner technisch-organisatorischen Maßnahmen hinwiesen und ankündigten, diesen Prozess mit zu beobachten. Bei einer weiteren Datenschutzverletzung handelte es sich um einen Cyber-Angriff, bei dem der Server eines Unternehmens mit Schadsoftware kompromittiert worden war.

## 11.2 Datenweitergabe an eine Arbeitgeberin durch eine Wohnungsgenossenschaft

Uns erreichte eine Beschwerde, in der die Konsequenz der unrechtmäßigen Bearbeitung der personenbezogenen Daten den Verlust ihres Arbeitsplatzes zur Folge hatte. Hintergrund war, dass der Ehemann der Beschwerdeführerin bei einer Wohnungsgenossenschaft angestellt war. Während ihrer Arbeitszeit tauschten sich die Beschwerdeführerin und ihr Ehemann über ihre jeweiligen dienstlichen E-Mail-Adressen unter anderem auch über berufliche Inhalte aus und stellten sich diese teilweise gegenseitig zur Verfügung. Die arbeitsrechtliche Bewertung eines solchen Verhaltens obliegt nicht der datenschutzrechtlichen Aufsichtsbehörde. Als die Wohnungsgenossenschaft von der E-Mail-Korrespondenz zwischen dem Ehepaar erfuhr, informierte sie die Arbeitgeberin der Beschwerdeführerin darüber und stellte dieser partiell den Schriftverkehr des Ehepaares zur Verfügung. Für die darin liegende Datenverarbeitung konnte sie keine datenschutzrechtliche Rechtfertigung anführen. Diese Weitergabe der personenbezogenen Daten der Beschwerdeführerin war damit rechtswidrig.

## 11.3 Überarbeitung der Orientierungshilfe für Mietinteressent:innen

Im 5. Jahresbericht nach der Datenschutzgrundverordnung berichteten wir unter der Ziffer 11.7 darüber, dass die Orientierungshilfe für Mietinteressent:innen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) herangezogen werden kann, wenn es darum geht, unter welchen Voraussetzungen Vermieter:innen nach Vermögensverhältnissen der Immobilieninteressent:innen fragen dürfen.

Im Berichtsjahr beteiligten wir uns an der Überarbeitung dieser Orientierungshilfe, die nicht nur ein Leitfaden für Mietinteressent:innen sein soll, die vorab eine Übersicht darüber erhalten

wollen, welche Fragen potenzieller Vermieter:innen, Makler:innen oder Hausverwaltungen sie beantworten müssen, sondern soll auch eine Hilfestellung für Kleinvermieter:innen sein, die im Gegensatz zu großen Wohnungsbauunternehmen nicht über die nötigen Mittel verfügen, eine ausführliche rechtliche Beratung in diesem Gebiet einzuholen.

Jede unzulässige, indiskrete und diskriminierende Datenverarbeitung durch potenzielle Vermieter:innen verletzt den Schutz der personenbezogenen Daten von Mietinteressent:innen. In der Orientierungshilfe ist aber genauso das Interesse der Vermieter:innen berücksichtigt, sich vor Abschluss eines Mietvertrages hinsichtlich der Bonität potenzieller Mieter:innen abzusichern. Daher sind vereinzelte Fragen in diesem Bereich zulässig, die aber zum jeweiligen Stadium der Vertragsanbahnung erforderlich sein müssen.

Solange Mietinteressent:innen zunächst lediglich eine Besichtigung der Räumlichkeiten anstreben (Phase A), ist es in der Regel nicht erforderlich, bereits in diesem Stadium Angaben zu ihren wirtschaftlichen Verhältnissen zu erfragen. Hier sind im Regelfall die Informationen zur Identifikation der Person (Name, Vorname und Anschrift) ausreichend.

Erst wenn die Mietinteressent:innen erklären, eine Wohnung anmieten zu wollen (Phase B), können bestimmte Fragen zu Einkommens- und Vermögensverhältnissen sowie zu noch nicht abgeschlossenen Verbraucherinsolvenzverfahren gestellt werden. Fragen nach Räumungstiteln wegen Mietzinsrückständen sind nur zulässig, wenn sie aufgrund der zeitlichen Nähe noch Auskunft zu etwaigen Gefährdungen künftiger Mietansprüche geben können. Dies kann unter anderem der Fall sein, wenn im aktuellen Mietverhältnis Mietinteressent:innen eine Zwangsräumung wegen Mietrückständen droht.

Fragen zum Beruf und zu Arbeitgeber:innen sowie die Erfragung des Nettoeinkommens sind in diesem Stadium regelmäßig zulässig.

Nachdem künftige Vermieter:innen sich für eine bestimmte Mietinteressentin beziehungsweise einen bestimmten Mietinteressenten entschieden haben (Phase C), können weitere Informationen von den Erstplatzierten erforderlich werden.

Begrenzt zulässig sind Fragen nach erheblichen Pflichtverletzungen aus vorherigen Mietverhältnissen. Erheblich sind diese jedenfalls dann, wenn sie auch noch in Zukunft zu erwarten sind. Hier sollte den Betroffenen jedoch die Möglichkeit eingeräumt werden, vorzutragen, weshalb eine gleichartige Verletzung im neuen Verhältnis nicht mehr zu erwarten ist. Nach höchstrichterlicher Rechtsprechung gilt die Erheblichkeitsschwelle auch hinsichtlich der Zahlungswilligkeit und -fähigkeit der Erstplatzierten. Es liege keine zur Kündigung ausreichende Pflichtverletzung vor, wenn der Mietrückstand eine Monatsmiete des bestehenden Mietverhältnisses nicht übersteige und die Verzugsdauer weniger als einen Monat betrage. Dies ändert sich jedoch, wenn Mieter:innen für zwei aufeinanderfolgende

Termine mit der Entrichtung der Miete oder eines nicht unerheblichen Teils der Miete in Verzug sind oder dies in einem Zeitraum er Fall ist, der sich über mehr als zwei Termine erstreckt und der die Miete für zwei Monate erreicht.

Fragen nach besonderen Kategorien personenbezogenen Daten nach Artikel 9 Datenschutzgrundverordnung, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung sind grundsätzlich untersagt. Auch Fragen nach Vorstrafen, strafrechtlichen Ermittlungsverfahren, der Zugehörigkeit zu Mieter:innenvereinen sind unzulässig, da diese Merkmale hinsichtlich der Beurteilung der Bonität keine Rolle spielen. Heiratsabsichten, Schwangerschaften und Kinderwünsche gehören zum Kernbereich der privaten Lebensgestaltung, daher sind Fragen hierzu ebenfalls in jedem Stadium unzulässig.

Daten von Personen, mit denen kein Vertrag abgeschlossen wurde, sind nach Artikel 17 Absatz 1 Buchstabe a Datenschutzgrundverordnung zu löschen. Das Führen einer "schwarzen Liste", in der Daten von "auffälligen" Mietinteressent:innen gespeichert werden, ist unzulässig.

## 11.4 Hinreichende Transparenz bei Datenschutzinformationen

Anlässlich einer bei uns eingegangenen Beschwerde im Zusammenhang mit einem Vertragsabschluss mit einem Energieversorgungsunternehmen weisen wir auf die Transparenzanforderungen aus Artikel 12 Datenschutzgrundverordnung (DGSVO) hin. Danach haben verantwortliche Stellen den Betroffenen alle Informationen und Maßnahmen in präziser, transparenter, verständlicher und leicht zugänglicher Form zu übermitteln. Inbegriffen sind hier auch Informationspflichten bei der Erhebung von personenbezogenen Daten bei der betroffenen Person selbst und bei Dritten.

Ein Konzern genügt den Anforderungen aus Artikel 12 DSGVO nicht, wenn von Verbraucher:innen erwartet wird, dass diese die Konzernstrukturen und sämtliche Konzerntöchter kennen, unterscheiden und die jeweils dazu gehörigen Datenschutzinformationen richtig zuordnen. Insbesondere im Hinblick darauf, dass nach der DSGVO Konzerne als wirtschaftliche Einheit angesehen werden, ist eine zwischen dem Konzern und den Konzerntöchtern differenzierende Argumentation ohnehin fragwürdig. Bei Datenschutzinformationen im Rahmen des Abschlusses eines Energieversorgungsvertrages muss es daher für die Verbraucher:innen eindeutig sein, auf welchen Teil des Konzernes sich die Datenschutzinformationen konkret beziehen, ob also auf den Energieversorgungsvertrag

mit einer der Konzerntöchter oder auf die Datenschutzinformationen im Zusammenhang mit Nutzung der Homepage des Konzernes Bezug genommen wird. Wir haben dem Energieversorgungsunternehmen gegenüber deutlich gemacht, dass die Anforderungen der DSGVO verletzt werden, wenn Verbraucher:innen hier vor einem Rätsel stehen.

## 11.5 Weitergabe von Kontaktdaten im Dreiecksverhältnis

Im Berichtsjahr erreichte uns die Beschwerde eines Mieters eines Mietshauses mit mehreren Mietparteien. Aufgrund eines Wasserschadens hatte die Vermieterin eine Handwerksfirma mit der Reparatur beauftragt. Die Firma meldete sich zwecks Terminabsprache telefonisch bei dem Beschwerdeführer. Da die genaue Ursache des Wasserschadens nicht ermittelt werden konnte, gaben die Handwerker:innen zur weiteren Erforschung der Schadensquelle die Telefonnummer des Beschwerdeführers noch am selben Tag an eine weitere Firma weiter. Der Mieter meldete sich bei uns mit einer Beschwerde über die Weitergabe seiner Telefonnummer.

Grundsätzlich gilt, dass Vermieter:innen, um Reparaturen oder Inspektionen vornehmen zu lassen, berechtigt sind, Handwerker zu beauftragen. Termine zwischen diesen und den Mietparteien müssen sie in der Regel in Eigenregie durch Absprache mit beiden Seiten koordinieren, eine Weitergabe der Telefonnummer und ein Kontakt im Dreiecksverhältnis zwischen Mietpartei und Handwerker:innen sollte in der Regel nicht erfolgen, da externe Fachbetriebe aus Sicht der Mieter:innen Dritte sind und die Verarbeitung der personenbezogenen Daten daher nicht allein mit dem Bestehen eines Mietsverhältnisses gerechtfertigt werden kann.

Etwas Anderes kann bei einer Einwilligung der Mietpartei zur Weitergabe der Telefonnummer oder einer entsprechenden Passage dazu im Mietvertrag gelten. Beides lag im konkreten Fall jedoch nicht vor.

Ungeachtet dessen war die Weitergabe der Telefonnummer des Beschwerdeführers hier nicht rechtswidrig, da die Vermieterin ein berechtigtes Interesse an der Datenverarbeitung hatte. Aufgrund des Wasserschadens und der noch unklaren Ursache dafür, bestand Gefahr im Verzug. Da nicht eingeschätzt werden konnte, ob der Schaden sich noch ausweiten würde, machte die Vermieterin daneben ihr Erhaltungsinteresse an ihrem Eigentum geltend. Hinzu kam, dass das Warmwasser im gesamten Gebäude abgeschaltet war und den Mieter:innen so schnell wie möglich wieder ermöglicht werden sollte, dieses zu nutzen. Dass der Beschwerdeführer den Wasserschaden nicht als sehr groß einstufte, spielte in diesem Zusammenhang keine Rolle, da die Schadensursache zum Zeitpunkt der Weitergabe der Telefonnummer an die Handwerksfirmen noch nicht feststand. Die Interessen der Vermieterin

und die der anderen Mietparteien überwogen damit im Ergebnis das Interesse des Beschwerdeführers an der Nichtweitergabe seiner Telefonnummer.

Im Regelfall, in dem keine Gefahr im Verzug liegt, müssen Vermieter:innen jedoch eine Einwilligung ihrer Mieter:innen einholen, bevor sie deren Telefonnummer an Handwerker:innen weitergeben. Dafür muss der konkrete Grund für eine solche Weiterleitung und die Firma, an die die Telefonnummer weitergegeben wird, genannt werden.

## 11.6 Sichere Datenübermittlung bei Beantragung einer Bauakte

Eine Beschwerdeführerin war anlässlich der Beantragung einer Bauakte unter anderem aufgefordert worden, eine Personalausweiskopie per E-Mail einzureichen.

Im Zusammenhang mit einem Baugenehmigungsverfahren sind Grundstückseigentümer:innen und Erbbauberechtigte als Beteiligte im Verwaltungsverfahren zur Einsicht in die jeweilige Bauakte berechtigt. Zur Überprüfung der Übereinstimmung der antragstellenden Person mit dem Eigentumsnachweis benötigt die Baubehörde einige, nicht jedoch alle personenbezogenen Daten antragstellender Personen, die aus Ausweisdokumenten hervorgehen. Betroffene können deshalb nicht erforderliche Daten auf Kopien der Ausweisdokumente schwärzen.

Nach dem Gesetz zur Förderung der elektronischen Verwaltung in Bremen müssen alle unter den Anwendungsbereich dieses Gesetzes fallenden Behörden einen elektronischen Behördenzugang im Verschlüsselungsverfahren anbieten. Wenn Behörden über ein Kontaktformular auf ihrer Website kontaktiert werden, ist dieser Teil transportverschlüsselt. Sollten darüber hinausgehende Informationen per E-Mail ausgetauscht werden, muss auch der E-Mail-Verkehr verschlüsselt sein. Nach dem Gesetz zur Förderung der elektronischen Verwaltung ist jede Behörde verpflichtet, den elektronischen Zugang auch durch eine De-Mail-Adresse im Sinne des De-Mail-Gesetzes zu eröffnen. Die Homepage der Senatorin für Bau, Mobilität und Stadtentwicklung wies zwar auf die Möglichkeit der Kontaktaufnahme per De-Mail hin, die Website, auf der die Petentin den Bauantrag direkt beantragt hatte, bot diese Möglichkeit jedoch nicht. Der in der Datenschutzgrundverordnung (DSGVO) formulierte Grundsatz der Integrität und Vertraulichkeit erfordert es, dass bei der Verarbeitung personenbezogener Daten eine angemessene Sicherheit durch geeignete technische und organisatorische Maßnahmen zu gewährleisten ist. Der Hinweis auf die Nutzungsmöglichkeit von De-Mail ist daher nicht nur auf der Homepage des Ressorts, sondern auch auf jeglicher Website, auf der eine Behörde Kontaktmöglichkeiten anbietet, erforderlich. Es kann von denjenigen, die mit Behörden Kontakt aufnehmen wollen, nicht erwartet werden, dass sie die in ihrer Angelegenheit zuständige Behörde in jedem Fall zutreffend ermitteln, dann – obwohl für die von ihnen angestrebte Kontaktaufnahme mit der Behörde ein anderer digitaler Weg

vorgesehen ist – die jeweilige Homepage der Behörde besuchen, um erst dort die Information über eine mögliche Kontaktaufnahme per De-Mail zu erhalten.

Wir konfrontierten das zuständige Ressort mit dem von der Beschwerdeführerin geschilderten Sachverhalt und hinterfragten insbesondere, weshalb diese aufgefordert worden war, wichtige Dokumente per nicht hinreichend verschlüsselter E-Mail zu versenden. Auch wiesen wir darauf hin, dass die Website, auf der der Antrag gestellt werden konnte, weder ein Kontaktformular, noch den Hinweis auf die Nutzungsmöglichkeit von De-Mail enthielt. Nach Eingang unseres Schreibens bei der Verantwortlichen konnten wir feststellen, dass Wartungsarbeiten auf der Homepage vorgenommen wurden. Nach Beendigung dieser war die Website gänzlich neugestaltet und verfügte nun über Kontaktformulare.

Wegen weiterer datenschutzrechtlicher Aspekte im Zusammenhang mit der digitalen Beantragung von Bauakten dauert der Austausch mit der Senatorin für Bau, Mobilität und Stadtentwicklung zu Redaktionsschluss noch an. Zum einen stellten wir fest, dass mehrere parallele Kontaktmöglichkeiten wie Adresse, E-Mail und Telefonnummer gleichzeitig als Pflichtfelder im Rahmen der Antragstellung für eine Bauakte markiert waren. Im Sinne des Datenminimierungsgrundsatzes der DSGVO muss die Erhebung personenbezogener Daten auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt werden. Für die Beantragung eines Bauaktenantrages ist es grundsätzlich ausreichend, wenn entweder Post- oder E-Mail-Adresse der beantragenden Person vorliegen. Die Abfrage einer Telefonnummer ist entbehrlich. Entsprechende Angaben können allenfalls freiwillig erfolgen.

Nach der jetzigen Konstellation besteht für die Antragsteller:innen nicht die Möglichkeit der Behörde die Ausweisdokumente persönlich zur Kenntnis zu geben. Auch müssen einzelne Aspekte der Hochladefunktion für Ausweisdokumente aus datenschutzrechtlicher Sicht verbessert werden.

## 11.7 Google Street View

Im Sommer des Berichtsjahres führte Google für seinen Dienst Google Street View auch in Bremen und Bremerhaven Aufnahmefahrten durch. In diesem Zusammenhang erreichten uns zahlreiche Beschwerden und Anfragen.

Laut Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) zu Vorabwidersprüchen bei Street View vom 12. Mai 2020 müssen Anbieter von Straßenansichten wie Google Street View vor Beginn der geplanten Aufnahmen die Öffentlichkeit in geeigneter Weise informieren. Für die Veröffentlichung der Aufnahmen durch Street View oder ähnliche Dienste kann Artikel 6 Absatz 1 Buchstabe f Datenschutzgrundverordnung (DSGVO) als Rechtsgrundlage in Betracht kommen. Zu beachten ist, dass nur die personenbezogenen Daten veröffentlicht werden dürfen, die zur

Zweckerreichung zwingend erforderlich sind. Merkmale, die die Identifizierung einer Person ermöglichen (zum Beispiel Gesichter und Kfz-Kennzeichen), müssen unkenntlich gemacht werden. Betroffene müssen sowohl online als auch postalisch deutlich den Hinweis auf die Möglichkeit der Unkenntlichmachung und des Widerspruchs gegen die Veröffentlichung bekommen.

Bei den Aufnahmen in den Jahren 2022 und 2023 verwendete Google zwei unterschiedliche Aufnahmesysteme: Zum einen waren auf den Dächern der als Aufnahmefahrzeuge erkennbaren Kraftfahrzeuge Kameras angebracht.

Andererseits wurden sogenannte Trekker verwendet, die per "Rucksack-System" die Aufnahmen durchführten. Diese Methode ermöglichte es Google-Beschäftigten, die Kameras auf dem Rücken zu tragen oder an einem Pick-up, Motorrad oder Schneemobil anzubringen. Die Aufnahmen im Land Bremen waren im Jahr 2022 und im Berichtsjahr erfolgt.

Im Jahr 2022 hatte Google Informationen über die Durchführung geplanter Aufnahmen zwar auf einer Website veröffentlicht, es jedoch zunächst versäumt, die Öffentlichkeit auf anderen Kanälen über die geplante Veröffentlichung der Aufnahmen zu informieren. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hatte als federführende Aufsichtsbehörde gefordert, dass Google die Öffentlichkeit ausdrücklich darüber informiert, dass die im Jahr 2022 entstandenen Aufnahmen erst später veröffentlicht werden sollten. Auch sollte es den betroffenen Personen rechtzeitig (ungefähr 6 Wochen vor der geplanten Veröffentlichung) ermöglicht werden Vorabwidersprüche gegen die Abbildung ihrer Häuser einzulegen. Google stellte daraufhin nachträglich die Informationen darüber, an welchen Orten die Aufnahmen stattgefunden hatten, auf der Website von Google Street View zur Verfügung. Widersprüche konnten per E-Mail, per Formular auf der Supportwebsite oder per Brief eingelegt werden.

Eine weitere datenschutzrechtliche Problematik ergab sich daraus, dass die Aufnahmen nicht nur von Google selbst, sondern teilweise auch von Nutzenden stammen. Bei Street View-Inhalten von Nutzenden, die auf 360 Grad-Videoaufnahmen basieren, sorgen die Algorithmen von Google dafür, dass Gesichter und Nummernschilder automatisch unkenntlich gemacht werden. Bei anderen Inhalten geschieht dies jedoch nicht automatisch. In diesem Zusammenhang hatte Google in der Datenschutz-Richtlinie für von Maps-Nutzer:innen diejenigen, die Inhalte veröffentlichten wollten, aufgefordert durch die Veröffentlichung nicht die Privatsphäre anderer Personen zu verletzten und "behielt sich vor", entsprechende Inhalte zu entfernen.

Mit einem solchen "Vorbehalt" kann sich Google nicht der datenschutzrechtlichen Verantwortlichkeit für sämtliche im Dienst Google Street View veröffentlichten Inhalte entziehen. Das Hochladen der Aufnahmen, die in Zusammenhang mit Bildern und/oder Karten in Google Maps oder Google Street View angezeigt werden, wird erst durch Google

ermöglicht. Daher stellen die Aufnahmen ergänzende Informationen zu den von Google angezeigten Orten dar. Insofern sind an Google als verantwortliche Stelle grundsätzlich dieselben datenschutzrechtlichen Anforderungen zu stellen, wie an die Nutzenden, die die Aufnahmen hochgeladen haben.

Bei der Abwägung zwischen den Interessen der betroffenen Personen, nicht identifizierbar dargestellt zu werden, und dem wirtschaftlichen Veröffentlichungsinteresse von Google überwiegen die Interessen der Abgebildeten. Daher muss Google auf Löschungsgesuchen betroffener Personen nachkommen und Gesichter und Kfz-Kennzeichen verpixeln. Sollten bei von Nutzenden hochgeladenen Fotos Datenschutzverstöße festgestellt werden, können diese über das von Google zu dem jeweiligen Bild angebotene Tool gemeldet werden. In diesem Zusammenhang ist anzumerken, dass sich hochladende Personen unter Umständen nach dem Kunsturhebergesetz strafbar machen, wenn sie Bilder ohne Einwilligung der Abgebildeten hochladen.

## 11.8 Neue Aufnahmen durch Apple Look Around

Ebenfalls im Sommer des Berichtsjahres fanden in Bremen und Bremerhaven neue Bilderfassungen von Apple für Apple Maps und für die Funktion Look Around statt. Dabei wurde ein ähnliches System wie bei Google angewendet (weltweite Vermessungsfahrten und "Rucksacktechnologie"). Die für die Erfassungsfahrten geplanten Termine waren entsprechend den Forderungen des Beschlusses der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu Vorabwidersprüchen bei Street View vom 12. Mai 2020 (siehe hierzu Ziffer 11.7 dieses Berichts) zuvor auf der Website von Apple Maps angekündigt worden. Apple kündigte an, Gesichter und Nummernschilder auf Bildern unkenntlich zu machen. Der Vorabwiderspruch gegen die Veröffentlichung und Anträge auf Löschung und Verpixelung bereits veröffentlichter Bilder wurden ermöglicht.

## 11.9 Weitergabe einer ungeschwärzten Unterschrift durch eine Wohnungsverwaltung

Eine weitere Beschwerde im Wohnbereich bezog sich darauf, dass eine Wohnungsverwaltung nach dem Wohnungseigentumsgesetz (WEG) die Kopie eines Schreibens eines Ehepaares samt ungeschwärzter Unterschriften als Anlage im Protokoll einer Versammlung der Wohnungsverwaltung an sämtliche Wohnungseigentümer:innen versendet hatte.

Eine über Namen und Wohnadressen hinausgehende Weitergabe von Kontaktdaten an eine Wohnungseigentümergemeinschaft kann zulässig sein, wenn sie im Rahmen der Einberufung einer Versammlung nach dem WEG und der Aufstellung der Tagesordnung erfolgt (siehe hierzu Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 16.2). Der geschilderte Fall

zeigt jedoch, dass die jeweilige Einzelfallbetrachtung auch dazu führen kann, dass eine Weitergabe im Kontext von Wohnungseigentümerversammlungen unzulässig ist. Zunächst einmal ging es hier nicht um eine Datenübermittlung im Zusammenhang mit der Einberufung einer Versammlung, sondern um eine Datenübermittlung nach Ablauf der Versammlung. Auch muss eine klare Differenzierung zwischen Daten wie Namen und Anschriften der Eigentümer:innen und den darüber hinausgehenden Daten vorgenommen werden (siehe hierzu 4. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 15.).

Die ungeschwärzte Weiterleitung von Unterschriften als Anhang zu einem Protokoll einer Versammlung nach dem WEG ist in der Regel nicht erforderlich und daher unzulässig.

Was die datenschutzrechtliche Verantwortlichkeit anbelangt, ist nicht per se jede Weitergabe von personenbezogenen Daten in vergleichbaren Kontexten der Wohnungseigentümergemeinschaft zuzurechnen, sondern kann durchaus auch der Wohnungsverwaltung zuzurechnen sein. Erneut nehmen wir diesbezüglich Bezug auf das Urteil des Amtsgerichts Mannheim vom 11. September 2019, welches besagt, dass Verwalter:innen Verantwortliche im Sinne des Artikel 4 Nummer 7 Datenschutzgrundverordnung (DSGVO) oder gegebenenfalls gemeinsam verantwortlich mit der Wohnungseigentümergemeinschaft im Sinne des Artikel 26 DSGVO sein können.

Aus der gesetzlichen Aufgabe von Verwalter:innen, unter anderem auch Zustellungen für die Versammlungen entgegenzunehmen, ergibt sich keine Legitimation, von sich aus Schreiben an die gesamte Wohnungseigentümergemeinschaft weiterzuleiten, wenn diese nicht ausdrücklich an die Gemeinschaft der Eigentümer:innen gerichtet sind. Selbst in diesem Fall ist es in der Regel nicht erforderlich, Unterschriften zu übermitteln. Mit dem geschilderten Verhalten verstieß die Wohnungsverwaltung damit gegen die DSGVO.

## 12. Beschäftigtendatenschutz

### 12.1 Gemeldete Datenschutzverletzungen

Im Bereich Beschäftigtendatenschutz wurden im Berichtsjahr 27 Datenschutzverletzungen nach Artikel 33 Datenschutzgrundverordnung gemeldet. 24 der Meldungen stammten aus dem nicht öffentlichen Bereich, lediglich drei Meldungen hingegen aus dem öffentlichen Bereich. Im Vergleich hierzu nahm die Anzahl der Beschwerden und Beratungsanfragen weiter zu, so betrafen insgesamt 52 Beschwerden den Umgang der Verantwortlichen mit Beschäftigtendaten. Auch bei telefonischen Anfragen ist ein hoher Beratungsbedarf im Bereich des Beschäftigtendatenschutzes zu verzeichnen. Besonders häufig betrafen diese Anfragen die Überwachung der Beschäftigten sowie die Zulässigkeit unterschiedlicher Möglichkeiten der Arbeitszeiterfassung.

## 12.2 Doppelte Personalaktenführung

Durch eine Beschwerde wurden wir auf das Vorhandensein von Nebenakten zu einigen Beschäftigten bei der Gewerbeaufsicht des Landes Bremen aufmerksam gemacht. Das Anlegen dieser Akten erfolgte, ohne dass die Gewerbeaufsicht die personalaktenführende Stelle war.

Gemäß § 12 Bremisches Ausführungsgesetz zur EU-Datenschutz-Grundverordnung (BremDSGVOAG) in Verbindung mit § 85 Absatz 1 Bremisches Beamtengesetz (BremBG) darf der Dienstherr personenbezogene Daten über Bedienstete nur verarbeiten, soweit dies im Rahmen der Personalverwaltung oder Personalwirtschaft, insbesondere zur Begründung, Durchführung, Beendigung oder Abwicklung des Dienstverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, einschließlich zu Zwecken der Personalplanung und des Personaleinsatzes erforderlich ist und dadurch schutzwürdige Belange der betroffenen Person nicht beeinträchtigt werden oder eine Rechtsvorschrift dies erlaubt. Weitere Konkretisierungen hinsichtlich der Verarbeitung und des Schutzes von Personalaktendaten ergeben sich aus der Verwaltungsvorschrift über die Verarbeitung von Personalaktendaten und die Führung von Personalakten (PAVwV). So ist hiernach die Führung von Sonderakten oder doppelten Personalakten sowie die Sammlung von Durchschriften durch nichtpersonalaktenführende Dienststellen oder Behörden nicht gestattet. Auch sofern Nebenakten in Einzelfällen nach der PAVwV zulässig sind, dürfen diese nur solche Unterlagen enthalten, deren Kenntnis zur rechtmäßigen Aufgabenerledigung der betroffenen Behörde erforderlich ist. Die Erforderlichkeit der aufgefundenen Akten und der darin enthaltenen personenbezogenen Daten konnte durch die Gewerbeaufsicht des Landes Bremen nicht dargelegt werden.

Aufgrund unseres Tätigwerdens informierte die verantwortliche Stelle die betroffenen Beschäftigten über das Vorhandensein der Akte und bot diesen an, die betreffenden Inhalte an sie herauszugeben. Sofern die Betroffenen eine Herausgabe oder eine Einsicht ablehnten, erfolgte eine Löschung der Akte, da diese für die Aufgabenerfüllung nicht erforderlich war.

## 12.3 Weitergabe von Personaldaten durch den Personalratsvorsitzenden bei einer Anstalt öffentlichen Rechts

Gleich zwei Beschwerden erreichten uns im Zusammenhang mit einer Mitteilung eines Personalratsvorsitzenden einer Anstalt öffentlichen Rechts, welche an alle Beschäftigten versandt worden war. In dem betreffenden Schreiben wurden mehrere Beschäftigte namentlich genannt und es wurde in diesem Zusammenhang auch darauf hingewiesen, dass die Polizei die Personalien einiger anwesender Personen aufgenommen habe, da ein Hausfriedensbruch in Betracht komme.

Das Schreiben des Personalratsvorsitzenden an die Beschäftigten erfolgte im Nachgang einer Presseberichtserstattung. Selbst für den Fall, dass eine solche Information der Beschäftigten über Vorfälle im Rahmen einer Personalversammlung für zulässig erachtet werden würde, konnte die Erforderlichkeit der Namensnennung einzelner Beschäftigter im konkreten Fall nicht dargelegt werden. Auch nach Einschätzung der verantwortlichen Stelle war diese betriebsinterne Information an alle Beschäftigten nicht zur Durchführung des Beschäftigungsverhältnisses erforderlich. Insbesondere ließ sich eine Erforderlichkeit des Vorgehens auch nicht aus den allgemeinen Aufgaben des Personalrates nach dem Bremischen Personalvertretungsgesetz herleiten.

Hinsichtlich der datenschutzrechtlichen Verantwortlichkeit gilt, dass der Personalrat keine eigene, nach außen hin verselbstständigte Stelle ist, sondern unselbstständiger Teil der jeweiligen Behörde oder sonstigen öffentlichen Stelle. Letztere ist damit auch für Datenverarbeitungen des Personalrates verantwortliche Stelle im Sinn der Datenschutzgrundverordnung und muss sicherstellen, dass der Personalrat die einschlägigen datenschutzrechtlichen Vorgaben einhält. Nichtsdestotrotz trifft den Personalrat als unabhängige Institution des Personalvertretungsrechtes innerhalb der Dienststelle eine Verantwortung für eine rechtmäßige Verarbeitung der bei ihm aufkommenden personenbezogenen Daten.

## 12.4 Veröffentlichung von Beschäftigtendaten auf der Homepage der Universität Bremen

Veröffentlichungen im Internet haben zur Folge, dass diese Daten weltweit einem unbeschränkten Personenkreis zur Verfügung stehen. Die Veröffentlichung von Daten der Beschäftigten ist daher nur zulässig, wenn die betroffenen Personen eingewilligt haben oder die Veröffentlichung zur ordnungsgemäßen Aufgabenerfüllung der verantwortlichen Stelle erforderlich ist. Eine Erforderlichkeit kann gegeben sein bei Personen, deren Tätigkeit nach außen wirkt. Hierunter fallen regelmäßig Behördenleitungen, Pressesprecher:innen oder Ansprechpartner:innen für Projekte mit Bürger:innenbeteiligung. Ob eine Bekanntgabe, insbesondere des Namens von Beschäftigten für das Beschäftigungsverhältnis erforderlich ist, bedarf der Abwägung im Einzelfall und muss von der verantwortlichen Stelle nachvollziehbar dargelegt werden. Hierbei ist unter anderem zu beachten, dass es Dritten durch die Angabe von Namen und Vornamen erleichtert wird, unter Nutzung weiterer frei zugänglicher Datenbestände Beschäftigte zu identifizieren und diese eventuell zu belästigen oder zu bedrohen. Es ist zwischen den Interessen der Öffentlichkeit an der namentlichen Nennung der einzelnen Bediensteten und im öffentlichen Bereich der Fürsorgepflicht des Dienstherrn im Hinblick auf die Sicherheit der Bediensteten abzuwägen. Grundsätzlich wird daher bei Beschäftigten, die in Aufgabenbereichen ohne Außenwirkung tätig sind, die Angabe der

allgemeinen Funktionsbezeichnung und der telefonischen Durchwahl für ausreichend erachtet.

Die Veröffentlichung des Namens und der Kontaktdaten auf der Homepage der Universität Bremen war Anlass für die Beschwerde einer betroffenen Person. Die Universität Bremen trug daraufhin vor, dass sie von einer Erforderlichkeit der Veröffentlichung der beruflichen Kontaktdaten ausgehe, da eine Universität für eine Vielzahl unterschiedlicher Personengruppen erreichbar sein müsse. Eine Veröffentlichung der Kontaktdaten lediglich im Intranet würde eine Vielzahl von externen Personen ausschließen, die die Universität und für sie zuständige Bearbeiter:innen regelmäßig erreichen müssten. Da es dezentral keine flächendeckenden Sekretariate für die einzelnen Bereiche gebe, die eine Weiterleitung von Anliegen oder Besucher:innen ermöglichen könnten, scheide eine Veröffentlichung lediglich der Kontaktdaten solcher Anlaufstellen aus. Nur die Veröffentlichung der Kontaktdaten der Beschäftigten gewährleiste daher eine ausreichende Erreichbarkeit der Universität.

Die betroffene Person übte jedoch keine Tätigkeit mit Außenwirkung aus und der betreffende Bereich war außerdem über ein Funktionspostfach erreichbar. Die Universität Bremen konnte in diesem Zusammenhang nicht darlegen, inwiefern darüber hinaus noch die Veröffentlichung der Kontaktdaten der betroffenen Person, inklusive der Nennung des Namens erforderlich war, sodass wir die Universität Bremen zur Entfernung der betreffenden personenbezogenen Daten von der Homepage aufforderten. Dies wurde uns zeitnah bestätigt. Darüber hinaus erfolgte die Rückmeldung, dass einzelne Beschäftigte jederzeit eine Entfernung der Kontaktdaten aus dem Mitarbeiter:innenverzeichnis beantragen könnten, sofern ein berechtigtes Interesse daran bestehe, im Rahmen der Internetsuche nicht mit den beruflichen Kontakten auffindbar zu sein.

## 12.5 "Multiperspektivisches Führungskräfte Feedback"

Der Senator für Inneres und Sport plante die Einführung eines sogenannten multiperspektivischen Führungskräfte Feedbacks. Hierbei sollen ergänzend zu der Einschätzung durch Vorgesetzte eine Selbsteinschätzung der Führungskraft sowie Beurteilungen seitens der Mitarbeiter:innen und Kolleg:innen eingeholt werden. Wir wiesen im Rahmen der Beratung darauf hin, dass für Mitarbeiter:innenbefragungen grundsätzlich gilt, dass diese nicht zur Durchführung des Arbeits- beziehungsweise Dienstverhältnisses erforderlich sind und auch eine wirksame Einwilligung aufgrund des im Beschäftigtenverhältnis bestehenden Über- beziehungsweise Unterordnungsverhältnisses regelmäßig nicht in Betracht kommt. Daher sind derartige Befragungen in einer Form durchzuführen, bei der die Vertraulichkeit der erhobenen Daten sichergestellt ist. Es müssen dementsprechend Anonymität, Freiwilligkeit und Transparenz gewährleistet sein. Weil bei der geplanten Feedbackmethode eine Bewertung auch durch die Vorgesetzten zwingend erfolgen sollte und sie insofern tief in Grundrechte eingreifen würde, teilten wir der verantwortlichen Stelle mit,

dass nicht zuletzt aufgrund der fehlenden Freiwilligkeit und Anonymität erhebliche datenschutzrechtliche Bedenken gegen die Einführung des geplanten "multiperspektivischen Führungskräfte Feedbacks" bestehen.

## 12.6 Weiterführung des personalisierten E-Mail-Kontos eines Beschäftigten nach Ausscheiden aus dem Unternehmen

Bereits in unserem vorherigen Jahresbericht informierten wir darüber, dass sich bei längerer Abwesenheit von Beschäftigten oder auch bei Beendigung des Arbeitsverhältnisses regelmäßig die Frage stellt, wie mit dem personalisierten E-Mail-Konto der oder des Beschäftigten zu verfahren ist (siehe hierzu 5. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 12.3). Nun war diese Fragestellung erneut Anlass für eine Beschwerde. Nach Beendigung des Arbeitsverhältnisses löschte der Arbeitgeber nicht das personalisierte E-Mail-Konto der betroffenen Person, sondern richtete lediglich eine betriebsinterne Weiterleitung aller eingehenden E-Mails ein. Nach Artikel 17 Absatz 1 Buchstabe a Datenschutzgrundverordnung (DSGVO) sind personenbezogene Daten unverzüglich zu löschen, sofern sie für die Zwecke, für die sie gespeichert, erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr benötigt werden. Wir wiesen den Verantwortlichen daher darauf hin, dass die Einrichtung der Weiterleitung von E-Mails, die nach dem Ausscheiden aus dem Betrieb auf dem personalisierten E-Mail-Postfach von Beschäftigten eingehen, datenschutzrechtlich unzulässig ist. Nach dem Ausscheiden von Beschäftigten aus dem Unternehmen ist deren E-Mail-Adresse vielmehr entsprechend Artikel 17 DSGVO unverzüglich zu löschen, sodass keine weiteren E-Mails mehr unter dieser Adresse eingehen können. Auf unsere Aufforderung hin bestätigte uns der Verantwortliche die Löschung des personalisierten E-Mail-Kontos der betroffenen Person und erarbeitete darüber hinaus einen Off-Boarding-Prozess, um derartige Vorfälle zukünftig zu vermeiden.

## 12.7 GPS-gestützte Arbeitszeiterfassung per App bei einem Gebäudereinigungsdienstleister

Uns erreichte eine Beschwerde hinsichtlich der Arbeitszeiterfassung durch einen Gebäudereinigungsdienstleister. Personenbezogene Daten von Beschäftigten dürfen grundsätzlich für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses verarbeitet werden. Die Aufzeichnung der Arbeitszeit ist dabei regelmäßig für die Durchführung des Beschäftigungsverhältnisses erforderlich. Die konkrete Datenverarbeitung muss jedoch auch verhältnismäßig im engeren Sinne sein, das heißt die Maßnahme muss zur Erreichung des Zwecks nicht nur geeignet und erforderlich, sondern auch angemessen sein. Vorliegend nutzte das Unternehmen eine App auf den privaten Mobiltelefonen der Beschäftigten, die per GPS-Signal den genauen Standort übermittelte oder auswies. Die Software glich dabei die GPS-Signale ab und kennzeichnete die Einsätze der

Beschäftigten als ausgeführt, wenn der vorgegebene Einsatzort und das GPS-Signal sowie die vorgegebene Dauer übereinstimmten. Wir wiesen die Verantwortliche darauf hin, dass erhebliche datenschutzrechtliche Bedenken hinsichtlich der Verhältnismäßigkeit der Maßnahme bestehen, da insbesondere die Erforderlichkeit der GPS-Ortung der Beschäftigten nicht nachgewiesen werden konnte. Das Unternehmen bestätigte uns daraufhin, dass die GPS-Funktion unverzüglich deaktiviert worden sei. Darüber hinaus war jedoch auch die Installation der App für die Zeiterfassung auf den privaten Mobiltelefonen der Beschäftigten problematisch. Auch hier konnte die Erforderlichkeit der Nutzung der App nicht dargelegt werden. Diese ist nur dann gegeben, wenn kein anderes gleich geeignetes und wirksames Mittel zur Verfügung steht, welches das allgemeine Persönlichkeitsrecht der Beschäftigten weniger belastet. Aus den uns vorgelegten Unterlagen ergaben sich jedoch Regelungen, die aus datenschutzrechtlicher Sicht hoch problematisch waren. So sollten die Beschäftigten unter anderem die Verpflichtung treffen, den Arbeitgeber rechtzeitig von jeder Verbringung eines Endgeräts zu einem Ort außerhalb des Europäischen Wirtschaftsraums und Großbritannien zu informieren. Eine Informationspflicht traf die Beschäftigten auch für den Fall der Pfändung des Endgerätes oder die Eröffnung eines Insolvenzverfahrens über das Vermögen der Beschäftigten oder ihrer Ehe- beziehungsweise Lebenspartner. Auch war der Arbeitgeber nach der vorgelegten "Bring your own device-Richtlinie" berechtigt, betriebliche Inhalte vom Endgerät der Arbeitnehmerin beziehungsweise des Arbeitnehmers zu löschen. Hierbei handelte es sich um erhebliche Eingriffe in die Lebens-, Privat- und Sozialsphäre der Beschäftigten, die nicht durch das Interesse des Arbeitgebers zur Nutzung einer App zur Zeiterfassung gerechtfertigt werden können. Wir forderten das Unternehmen daher auf, die entsprechende Nutzung auf den privaten Mobiltelefonen umgehend einzustellen. Dies bestätigte uns das Unternehmen und stattete die Beschäftigten mit dienstlichen Mobiltelefonen aus.

## 13. Medien, Telemedien, Digitalisierung

### 13.1 Gemeldete Datenschutzverletzungen

Im Bereich Medien und Telemedien wurden uns im Berichtszeitraum zehn Datenschutzverletzungen gemeldet.

### 13.2 Datenverarbeitung auf Websites der Gastronomie Branche

Uns erreichte im Berichtszeitraum eine Vielzahl von Beschwerden gegen Websites aus dem Bereich der Gastronomie. Hier war auffällig, dass besonders Dienste für die Reservierung von Tischen über die jeweiligen Websites häufig nicht den Anforderungen der Datenschutzgrundverordnung entsprachen oder fehlerhaft in die Funktion der Website eingebunden waren.

## 13.3 Fehlende oder fehlerhafte Datenschutzerklärungen von Websites

Innerhalb des Berichtszeitraums erreichte uns eine Vielzahl von Beschwerden gegen Websites, die gar keine oder unzureichende Informationen nach Artikel 13 Datenschutzgrundverordnung (DSGVO) zur Verfügung stellen. Fünf Jahre nach Inkrafttreten der DSGVO ist dies bemerkenswert.

## 13.4 Veröffentlichung von Gesundheitsdaten in Google Rezensionen

Durch einen Hinweis wurden wir darauf aufmerksam gemacht, dass in den Google Rezensionen zu einer Arztpraxis mehrfach personenbezogene Daten, insbesondere auch Gesundheitsdaten von Patient:innen der Praxis offengelegt wurden. Die Offenlegungen erfolgten hierbei im Rahmen der Antwort des bewerteten Arztes auf seiner Ansicht nach negative beziehungsweise falsche Rezensionen. Dabei offenbarte er mehrfach genaueste Angaben zur Behandlung und zum Gesundheitszustand der jeweiligen Patient:innen.

Als für die Offenlegung der personenbezogenen Daten der Patient:innen verantwortliche Stelle oblag es dem Medizinischen Versorgungszentrum, welches diese Praxis betreibt, die Löschung der beanstandeten Beiträge zu veranlassen. Dem Medizinischen Versorgungszentrum waren die Google Rezensionen bis zu unserem Tätigwerden nicht bekannt gewesen. Die Löschung der beanstandeten Beiträge gestaltete sich problematisch, da der zur Praxis gehörende Google Account nicht dem Medizinischem Versorgungszentrum gehörte, sondern dem sich mittlerweile in Ruhestand befindlichen Arzt. Schlussendlich gelang es dennoch alle Beiträge in den Google Rezensionen zu löschen, die personenbezogene Daten von Patient.innen enthielten.

## 13.5 Fotografieren einer Kindergartengruppe durch eine Privatperson

Uns erreichte eine Beschwerde, dass eine Privatperson Bildaufnahmen von einer sich auf einem Ausflug befindlichen Kindergartengruppe gemacht haben sollte und diese auf der Plattform Instagram hochladen wolle. Unsere Ermittlungen ergaben, dass die fotografierende Privatperson Landschaftsaufnahmen für ein privates Instagram-Fotoprojekt erstellt hatte. Direkt nach Erstellung einer dieser Aufnahmen fiel ihm auf, dass die Kindergartengruppe im Hintergrund des Bildes zu erkennen war. Der Fotograf versuchte sodann eine Einwilligung zum Hochladen der betroffenen Aufnahme auf Instagram von den anwesenden Erzieher:innen der Kindergartengruppe zu erhalten. Nachdem diese deutlich gemacht hatten, dass es eine solche Einwilligung nicht geben werde und den Fotografen aufgefordert hatten, die Aufnahme zu löschen war der Fotograf noch vor Ort dieser Aufforderung nachgekommen, hatte dies aber augenscheinlich nicht ausreichend kommuniziert.

## 13.6 Veröffentlichung von Aufnahmen von Kund:innen einer Tankstelle auf TikTok

Durch einen Hinweis wurden wir darauf aufmerksam gemacht, dass ein Angestellter einer Tankstelle regelmäßig Video- und Tonaufnahmen von Kund:innen in den Verkaufsräumen der Tankstelle erstellte. Bei diesen Aufnahmen handelte es sich größtenteils um sogenannte "Prankvideos", in denen der Angestellte den gefilmten Kund:innen unzutreffende Situationen vorspielte, die geeignet waren, sich über die Betroffenen lustig zu machen, oder sie mit demselben Ziel mit Hilfe von Wortwitzen verwirrte. Diese Videos wurden sodann auf dem TikTok-Account des Angestellten hochgeladen. Auch wurden auf diesem TikTok-Account regelmäßig Livestreams gesendet.

Nachdem die bremische Landesmedienanstalt die Kontaktdaten des Angestellten ermittelt hatte, wandten wir uns an ihn. In Folge unseres Tätigwerdens holt der Angestellte von den gefilmten Personen nunmehr Einwilligungen für die Aufnahmen sowie das Hochladen der Videos auf seinem TikTok-Account ein. Die regelmäßigen Livestreams wurden eingestellt.

# 14. Werbung

## 14.1 Gemeldete Datenschutzverletzungen

Von Unternehmen aus dem Bereich Werbung erhielten wir im Berichtsjahr keine Meldungen über Verletzungen des Schutzes personenbezogener Daten. Dagegen erreichten uns 36 Beschwerden über Unternehmen, die aus Sicht der Beschwerdeführenden im Zusammenhang mit Werbemaßnahmen gegen die Datenschutzgrundverordnung verstoßen hatten. Diese Diskrepanz verdeutlicht, dass es bei den Meldungen über Verletzungen des Schutzes personenbezogener Daten im Werbebereich eine hohe Dunkelziffer gibt.

## 14.2 Werbung per E-Mail

Der wesentliche Teil der Beschwerden über Unternehmen im Werbebereich betraf erneut die Kontaktierung zu Werbezwecken per E-Mail, obwohl die Betroffenen hierfür keine Einwilligung erteilt hatten.

Bereits jeweils unter Ziffer 14.3 des 4. und des 5. Jahresbericht nach der Datenschutzgrundverordnung hatten wir darauf hingewiesen, dass Werbung per E-Mail ohne die vorherige Einwilligung der Betroffenen nur ausnahmsweise möglich ist, wenn ein Unternehmer im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von der Kundin oder dem Kunden deren oder dessen E-Mail-Adresse erhalten hat. der Unternehmer die E-Mail-Adresse zur Werbung für eigene ähnliche Waren oder Dienstleistungen verwendet,

der Kunde der Verwendung seiner E-Mail-Adresse nicht widersprochen hat und der Kunde bei Erhebung der E-Mail-Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen wird, dass er der Verwendung seiner jederzeit widersprechen kann. Vor diesem Hintergrund der engen Ausnahmeregelung, raten wir dazu, dass Werbende die vorherige Einwilligung der jeweiligen betroffenen Kunden zwingende einholen sollten.

# 15. Videoüberwachung im nicht öffentlichen Bereich

## 15.1 Gemeldete Datenschutzverletzungen

Im Bereich Videoüberwachung gab es im Berichtsjahr keine Meldungen der Verletzung des Schutzes personenbezogener Daten nach Artikel 33 der Datenschutzgrundverordnung. Hingegen erhielten wir im Berichtszeitraum 87 Beschwerden, die sich auf Videoüberwachungen durch private Stellen bezogen.

## 15.2 Weiterverarbeitung von übersandten Berichten des Ordnungsamtes

In diesem Berichtsjahr führte das Ordnungsamt gemeinsam mit dem Zoll im Rahmen einer Sondermaßnahme umfangreiche Kioskkontrollen im Land Bremen durch. Im Zuge dieser Maßnahme wurden auch vorhandene Videoüberwachungsanlagen in Augenschein genommen und die ermittelten Feststellungen in den erstellten Berichten dokumentiert sowie teilweise Bilddokumentationen erstellt. Diese Berichte wurden an uns weitergeleitet, damit wir gegebenenfalls erforderliche Maßnahmen einleiten können.

Wir prüften diese Berichte und schrieben dort, wo sich Indizien für Verstöße ergaben, die Kioskbetreiber an. Aufgrund der Stellungnahmen der für die Videoüberwachung verantwortlichen Stellen konnten wir feststellen, dass häufig weder Hinweisschilder noch einsehbare Verzeichnisse über Verarbeitungstätigkeiten oder Aufzeichnungen über durchgeführte Datenschutz-Folgenabschätzungen vorhanden waren und die Erfassungsbereiche der Kameras öffentliche Bereiche erfassen.

Sofern zulässigerweise Videokameras installiert werden, ist durch Hinweisschilder auf die Videobeobachtung sowie auf die dafür verantwortliche Stelle, die Rechtsgrundlage, der verfolgte Zweck, die Speicherdauer, etwaige Empfänger:innen der Daten und die Betroffenenrechte hinzuweisen. Die Informationen sollten bei Betreten des überwachten Bereichs erkennbar sein. Des Weiteren muss unter Berücksichtigung der Grundsätze der Datenminimierung und Speicherbegrenzung eine Aufzeichnung grundsätzlich nach 72 Stunden gelöscht werden. Etliche Kioske führten kein Verzeichnis von Verarbeitungstätigkeiten, obwohl eine entsprechende Verpflichtung auch für Unternehmen, die weniger als 250 Mitarbeiter:innen beschäftigen, gilt, wenn die Verarbeitung personenbezogener Daten nicht nur gelegentlich erfolgt. In der Regel führt daher jede

Videoüberwachung zu der Pflicht, die Verarbeitungstätigkeiten zu beschreiben. Der häufigste Mangel bei den vorgelegten Beschreibungen der Verarbeitungstätigkeiten war die fehlende oder nur unzureichende Beschreibung der getroffenen technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten.

Des Weiteren wurden häufig Bereiche vor den Kiosken sowie Hausfassaden in die Überwachung einbezogen. Eine Überwachung der Hausfassaden ist grundsätzlich nur zulässig, wenn dabei nicht auch öffentlich zugängliche Bereiche erfasst werden. Sollte dies nicht vermieden werden können, weil etwa die Hausfassade direkt an einen Fußweg angrenzt, darf die Überwachung nur auf das zwingend notwendige Ausmaß beschränkt werden und einen maximal einen Meter breiten Streifen entlang der Fassade erfassen. Voraussetzung ist allerdings, dass es sich nachweislich um einen besonders einbruchsgefährdeten oder beschädigungsgefährdeten Bereich handelt.

Letztlich zeigten sich die Kioskbetreibenden überwiegend einsichtig und setzten die von uns aufgegebenen Maßnahmen um, um eine datenschutzkonforme Videoüberwachung zu gewährleisten. In allen Fällen erreichten wir, dass die Kameras entweder entsprechend neu ausgerichtet wurden und nur noch der unmittelbare Fassadenbereich erfasst wird oder mit irreversiblen Schwärzungen bei der Bildspeicherung gearbeitet wird, sodass öffentliche Bereiche nicht mehr erfasst werden. Außerdem wurden an den Fassaden deutlich sichtbare Hinweisschilder angebracht, die auf eine Videoüberwachung hinweisen.

## 16. Kredit-, Versicherungs- und allgemeine Wirtschaft

### 16.1 Gemeldete Datenschutzverletzungen

Mit stetig zunehmender Digitalisierung personenbezogener Datenverarbeitung und Anbindung der IT-Infrastrukturen an das Internet wächst die Gefahr der Angriffe Dritter weltweit aus den Tiefen des Internets. Wie auch schon im vorigen Berichtszeitraum gehörten dementsprechend die uns gemeldeten Angriffe auf die IT-Infrastruktur von Verantwortlichen mit Hilfe von Verschlüsselungs-Schadware, mittels Phishing-Mails, et cetera zu den schwerwiegendsten Schadensereignis-Meldungen. Zugenommen, wenngleich absolut betrachtet auf niedrigem Niveau, haben Meldungen über den im Zuge von Pkw-Aufbrüchen erfolgten Diebstahl mobiler IT und den damit einhergehenden Verlust oder vorübergehenden Wegfall der Verfügbarkeit personenbezogener Daten. Die versehentliche Offenbarung personenbezogener Daten aufgrund falscher Adressierung von Nachrichten oder auch durch Personenverwechslungen gehört zu den immer wiederkehrenden Meldegegenständen.

Es dürfte sich vermutlich bei den gemeldeten Fällen aber nur um einen kleinen Anteil der tatsächlichen Vorfälle handeln; die Meldepflicht gilt eben nicht uneingeschränkt, sondern lässt

Raum für ein Absehen von einer Vorfalls-Meldung, sofern der Verantwortliche begründet kein Risiko für Rechte und Freiheiten der betroffenen Personen prognostiziert. Im Zweifelsfalle empfiehlt sich für Verantwortliche aber eine Meldung. Denn das Unterlassen einer Meldung bei einem nach den Rechtsvorgaben meldepflichtigen Vorfall kann eine Geldbuße nach Artikel 83 Datenschutzgrundverordnung nach sich ziehen.

Im Bereich der Versicherungswirtschaft erreichten die Landesbeauftragte für Datenschutz und Informationsfreiheit im Berichtszeitraum zwei Meldungen. In beiden Fällen waren im Land Bremen ansässige Versicherungsmaklerunternehmen beziehungsweise ihre Auftragsverarbeiter Opfer von "Hacker-Angriffen" geworden. In einem Fall konnten keine Datenabflüsse festgestellt werden. Im anderen Fall laufen zu Redaktionsschluss noch die Sachverhaltsaufklärungen.

## 16.2 Umfang des Betroffenenauskunftsrechts – Präzisierungen durch den Europäischen Gerichtshof

Im Berichtsjahr erfolgten durch den zur letztverbindlichen Auslegung der Datenschutzgrundverordnung (DSGVO) berufenen Europäischen Gerichtshof (EuGH) wichtige Klarstellungen zu Inhalt und Reichweite des zentralen Betroffenenrechts auf Auskunft aus Artikel 15 DSGVO.

In der Rechtssache mit Aktenzeichen C-154/21 stellte der EuGH mit Urteil vom 12. Januar 2023 fest, dass in Artikel 15 Absatz 1 Buchstabe c DSGVO grundsätzlich das Recht für Betroffene verbrieft ist, von der datenverarbeitenden Stelle oder Person bei bereits erfolgten oder sicher feststehenden künftigen Übermittlungen ihrer personenbezogenen Betroffenen-Daten nicht nur abstrakte Empfänger:innenkategorien (zum Beispiel Branchen), sondern vielmehr konkret die Identität der einzelnen Empfänger:innen mitgeteilt zu bekommen. Der EuGH bestätigte hiermit erfreulicherweise zugleich unsere bisherige ständige Auslegungspraxis.

Die Datenschutzgrundverordnung schreibt als Bestandteil des Betroffenen-Auskunftsrechts in Artikel 15 Absatz 3 DSGVO auch das Recht auf Erhalt einer "Kopie" der (verarbeiteten) personenbezogenen Daten fest. In der Rechtssache mit Aktenzeichen C-487/21 stellte der EuGH mit Urteil vom 4. Mai 2023 fest, dass mit dem Begriff der Kopie grundsätzlich eine originalgetreue und verständliche Reproduktion aller dieser Daten gemeint ist. Dies bedeutet jedoch nicht von vornherein stets ein Recht auf eine Ablichtung eines gesamten Dokuments oder Dokumentenauszugs oder Datenbankauszugs. Derartiges kann nur dann verlangt werden, wenn dies "unerlässlich" ist, um der betroffenen Person die wirksame Ausübung ihrer Datenschutzrechte zu ermöglichen; die Rechte und Freiheiten anderer Personen oder Stellen sind hierbei jedoch zu berücksichtigen beziehungsweise in Ausgleich zu bringen.

## 16.3 Tücken der schnellen elektronischen Kommunikation

Bekanntlich ist die Einfachheit und Schnelligkeit der elektronischen Kommunikation via E-Mail nicht nur ein Vorzug, sondern mitunter auch tückisch, was etliche an uns herangetragene Beschwerden im Berichtsjahr wieder einmal veranschaulichten. So führte beispielsweise in einem Beschwerdefall eine kleine Unachtsamkeit bei der Schreibweise der E-Mail-Adresse der eigentlichen Adressatin dazu, dass ein Finanzdienstleister detailreiche Finanzierungsunterlagen an eine namensgleiche aber sonst unbekannte Empfängerin sandte. Ein Fehler, der in seinen Folgen nicht mehr wirksam und vollständig zu beseitigen war. In einem weiteren Beschwerdefall versandte ein Dienstleistungsunternehmen eine Werbe-E-Mail nebst Anhang an mehrere Kund:innen. Anstelle des vorgesehenen Anhangs war jedoch irrtümlich eine Datei angefügt, die eine umfangreichen tabellarischen Kund:innenliste enthielt. Gegenstand von Meldungen Verantwortlicher beziehungsweise Beschwerden Betroffener waren sodann auch wie in jedem Berichtsjahr E-Mail-Versendungen mit "offenem" Adressverteilerkreis.

## 16.4 Keine Beschränkung der Verwendungszwecke einer erteilten Selbstauskunft

In einem Fall erreichte uns eine Beschwerde darüber, dass eine Verantwortliche Auskünfte nach Artikel 15 Datenschutzgrundverordnung (DSGVO) mit dem Hinweis versah:

"Dieses Dokument ist eine Auskunft im Sinne des Artikel 15 DSGVO. Sie ist nicht zu wirtschaftlichen Zwecken gegenüber Dritten zu nutzen."

Grundsätzlich sehen wir keine rechtliche Befugnis von Verantwortlichen Zwecke festzulegen, zu denen die betroffene Person eine erhaltene Auskunft nach Artikel 15 DSGVO verwenden darf. Auch die Verantwortliche konnte uns auf unsere Nachfrage hin keine rechtliche Begründung hierfür geben. Aufgrund unseres Tätigwerdens passte die Verantwortliche im konkreten Fall ihr Auskunftsmuster an und verwendet die oben genannte Formulierung mittlerweile nicht mehr.

## 16.5 Unterlassene Auskunft nach Artikel 15 Datenschutzgrundverordnung

Wie auch schon in den Vorjahren (siehe hierzu 5. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 16.7) erreichten uns im Berichtsjahr erneut zahlreiche Beschwerden über nicht oder nicht rechtzeitig erteilte Auskünfte nach Artikel 15 Datenschutzgrundverordnung. Wir weisen in diesem Zusammenhang nochmals drauf hin, dass eingehende Auskunftsersuchen von allen Verantwortlichen zwingend zu beantworten sind, selbst wenn die Verantwortlichen keine personenbezogenen Daten der oder des

anfragenden Betroffenen verarbeitet haben. Ausnahmen kennt das Gesetz nur für nachweisbar "offenkundig unbegründete" oder "exzessive" Auskunftsersuchen. Für die Auskunft haben die jeweiligen Verantwortlichen grundsätzlich höchstens einen Monat Zeit. Die Verantwortlichen haben darüber hinaus geeignete technisch-organisatorische Maßnahmen zu treffen, um sicherzustellen, dass eingehende Auskunftsersuchen richtig erfasst und innerhalb der vorgenannten Frist bearbeitet werden.

## 16.6 Kund:innendaten im Verkaufsraum öffentlich zugänglich

Nicht selten sind uns gemeldete oder bekannt gewordene Verstöße gegen Datenschutzrecht wohl schlicht auf Unachtsamkeit zurückzuführen. Beispielhaft hierfür scheint folgender Fall: Im öffentlich zugänglichen Geschäftsraum eines Händlers waren Waren, die für Kund:innen reserviert oder bereits an sie verkauft aber noch nicht abgeholt waren, jeweils mit einem Schild versehen. Aus diesen Schildern gingen Name, Adresse und Telefonnummer der jeweiligen Käufer:innen hervor. Alle, die diesen Geschäftsraum betraten, konnten diese Informationen zur Kenntnis nehmen. Dass es für eine solche Bekanntgabe der Käufer:innendaten an eine Vielzahl zufällig Vorbeikommender keine rechtliche Begründung wie auch keine praktische Notwendigkeit geben kann, liegt auf der Hand. Nachdem wir mit dem Datenschutzbeauftragten des betroffenen Unternehmens gesprochen hatten, sorgte dieser für sofortige Abhilfe.

## 16.7 Inkasso – Datenweitergabe

Im Berichtszeitraum erhielten wir eine Beschwerde über die Datenverarbeitung durch ein Inkasso-Unternehmen. Zugrunde lag ein Sachverhalt, wie er häufiger an uns herangetragen wird. Das Inkasso-Unternehmen hatte die personenbezogenen Daten eines Kunden seines Auftragsgebers zum Zwecke der Forderungseinziehung verarbeitet. Der Kunde war der Ansicht, dass der geltend gemachte Anspruch gegen ihn nicht bestehe, da er nicht der richtige Schuldner sei. Ob er hiermit Recht hatte, war nicht Gegenstand unserer Prüfung als datenschutzrechtlichen Aufsichtsbehörde. Eine solche Prüfung, ob geltend gemachte Ansprüche bestehen und gegen die richtigen Schuldner:innen gerichtet sind, obliegt zuständigkeitshalber den Zivilgerichten.

Aus datenschutzrechtlicher Sicht gilt, dass Inkasso-Unternehmen als Rechtsdienstleister grundsätzlich berechtigt sein können, personenbezogene Daten zur Wahrung der berechtigten Interessen ihrer Auftraggeber:innen zu verarbeiten, weil Gläubig:innen mutmaßliche Ansprüche gegen Kund:innen durch eine andere Stelle überprüfen und einziehen lassen dürfen. Im vorliegenden Fall konnten wir aus datenschutzrechtlicher Sicht keinen Verstoß des Inkasso-Unternehmens feststellen.

## 16.8 Begrenzung der Speicherdauer des Merkmals Restschuldbefreiung bei Auskunfteien

Bestimmte Entscheidungen in Verbraucherinsolvenzverfahren, wie etwa die Erteilung einer Restschuldbefreiung, werden aufgrund gesetzlicher Vorgabe durch eine Veröffentlichung in einem hierfür vorgesehenen Online-Portal bekannt gemacht. Aufgrund der massiven Auswirkungen für die Betroffenen erfolgt die Online-Veröffentlichung von Gesetzes wegen allerdings nur für einen begrenzten Zeitraum, die Entscheidung über die Erteilung der Restschuldbefreiung wird beispielsweise für sechs Monate ab Rechtskraft veröffentlicht. Auskunfteien übernehmen diese amtlich veröffentlichten Daten schon vorsorglich für den Fall einer künftigen Bonitätsabfrage zu den Betroffenen in ihren eigenen Datenbestand. Sie sahen sich aber an diese Löschfrist im öffentlichen Register nicht gebunden, sondern hatten sich für eine dreijährige Speicherung entschieden und in dies einer Verbands-Verhaltensrichtlinie zu Prüf- und Löschfristen niedergelegt. Dies konnte in der Praxis beispielsweise dazu führen, dass betroffene Personen mit Restschuldbefreiung aufgrund einer Weiterspeicherung für weitere drei Jahre trotz Restschuldbefreiung massive Schwierigkeiten bei der Teilnahme am Wirtschaftsleben hatten.

Schon vor Geltung der Datenschutzgrundverordnung hatten wir diese Speicherpraxis als rechtlich zweifelhaft kritisiert.

Da auch das Verwaltungsgericht Wiesbaden im Klageverfahren massive Zweifel an der Vereinbarkeit dieser Speicherpraxis mit der Datenschutzgrundverordnung hatte, legte es diese Fragestellung dem Europäischen Gerichtshof zur Entscheidung vor. Mit Urteil vom 7. Dezember 2023 entschied der Europäische Gerichtshof in den verbundenen Rechtssachen C-26/22 und 64/22 unter anderem, dass diese Praxis, aus öffentlich Registern stammende Informationen zur Restschuldbefreiung in privaten Datenbanken länger als nach der für die Veröffentlichung vorgesehene Frist zu speichern, datenschutzrechtswidrig ist. Auch klangen deutliche datenschutzrechtliche Zweifel an der Notwendigkeit der parallelen Speicherung in privaten Auskunfteien-Datenbanken neben dem öffentlichen Register an, zudem an der Speicherung in diversen privaten Datenbanken unterschiedlicher Auskunfteien; die Prüfung dieser Fragen obliege aber dem Verwaltungsgericht Wiesbaden.

# 17. Internationales und Europa

## 17.1 Angemessenheitsbeschluss zum EU-U.S. Data Privacy Framework

Die Europäische Kommission erließ am 10. Juli 2023 einen neuen Angemessenheitsbeschluss für die Vereinigten Staaten von Amerika (USA). Auf Basis dieses Angemessenheitsbeschlusses können Verantwortliche sowie Auftragsverarbeiter

personenbezogene Daten an zertifizierte Unternehmen in die USA übermitteln, ohne geeignete Garantien vorweisen und zusätzliche Maßnahmen ergreifen zu müssen.

Seinen Ursprung hat der nun erlassene Angemessenheitsbeschluss in dem neuen Datenschutzrahmenabkommen zwischen der Europäischen Union (EU) und den USA: dem EU-U.S. Data Privacy Framework, das abgeschlossen werden musste, weil der Europäische Gerichtshof (EuGH) mit seinem Schrems II-Urteil am 16. Juli 2020 entschieden hatte, dass der auf dem vorherigen Abkommen "EU-U.S. Privacy Shield" gestützte Angemessenheitsbeschluss unwirksam ist.

Beim neuen Abkommen haben sich im Vergleich zum Privacy Shield zwei grundlegende Dinge verändert. Zum einen soll der Zugang der US-Nachrichtendienste zu Daten auf das "notwendigste und verhältnismäßigste" Maß beschränkt werden. Zum anderen wurde ein zweistufiges Beschwerdeverfahren gegen US-Überwachungsmaßnahmen eingeführt, welches beinhaltet, dass dieses vom Data Protection Review Court überprüft werden kann. Auf den Angemessenheitsbeschluss stützen können sich nur US-Unternehmen, die auf der Liste vom US-Handelsministerium als zertifizierte Unternehmen verzeichnet sind.

Die Übermittlungen personenbezogener Daten durch nicht zertifizierte Unternehmen erfordern weiterhin geeignete Garantien nach Artikel 46 Datenschutzgrundverordnung (DSGVO), den Rückgriff auf verbindliche interne Datenschutzvorschriften nach Artikel 47 DSGVO oder das Vorliegen eines Ausnahmetatbestands nach Artikel 49 DSGVO im Einzelfall.

Die Landesbeauftragte für Datenschutz und Informationsfreiheit wird weiterhin mit den anderen europäischen Aufsichtsbehörden die Geschehnisse in Europa bezüglich des neuen Angemessenheitsbeschlusses kritisch beobachten. Es ist zu erwarten, dass der neue Datenschutzrahmen aus dem Abkommen aufgrund von erneuten Klagen vom EuGH überprüft werden wird. Darüber hinaus hat die EU-Kommission selbst eine fortlaufende Überprüfung der Funktionsweise des Angemessenheitsbeschlusses angekündigt.

Es ist unklar, ob das neue Abkommen aus datenschutzrechtlicher Sicht eine wirkliche Verbesserung im Vergleich zum EU-U.S. Privacy Shield darstellt und dieses bei einer Klage vor dem EuGH standhalten würde. Kritisch wird dabei der neu erschaffene Data Protection Review Court betrachtet, weil es diesem an Transparenz mangelt. Außerdem haben sich die USA nicht dazu verpflichtet, ihre Geheimdienstüberwachung zu reduzieren. Das grundsätzliche Problem des Zugriffs auf Daten der Menschen in der EU durch US-Geheimdiensten bleibt also weiterhin bestehen. Auch ist zu erwarten, dass die Frage, was zu den "notwendigsten" und "verhältnismäßigsten" Zugängen der US-Geheimdienste zu den personenbezogenen Daten der Menschen in der EU zählt, von den USA anders ausgelegt werden wird als vom EuGH.

Noch kann es deshalb aus unserer Sicht keine langfristige Sicherheit für Unternehmen geben, die Datenübermittlung in die USA auf den neuen Angemessenheitsbeschluss zu stützen. Wir empfehlen bereits vorhandene geeignete Garantien und zusätzliche Maßnahmen beizubehalten und fortzuführen.

## 17.2 IMI als Tor für europäische Zusammenarbeit

Uns erreichten einige Beschwerden, die sich auf Verantwortliche bezogen, die ihren Sitz in anderen europäischen Ländern haben. Dies bedeutet für uns gemäß Artikel 56 fortfolgende der Datenschutzgrundverordnung (DSGVO), dass wir mit den jeweils für diese verantwortlichen Stellen federführenden europäischen Aufsichtsbehörden zusammenarbeiten. Diese Zusammenarbeit wird durch das Binnenmarkt-Informationssystem (Internal Market Information System, IMI), welches von der Europäischen Kommission entwickelt wurde, ermöglicht und vereinfacht. IMI ist auf die Verfahren nach Artikel 56 fortfolgende der DSGVO ausgelegt, bietet verschiedene Herangehensweisen an diese Art von Kommunikation und sorgt für eine präzise Zuständigkeits- und Untersuchungsverteilung zwischen den jeweiligen betroffenen europäischen Behörden.

Für die Betroffenen und für uns bedeutet diese europäische Zusammenarbeit, dass die Kommunikation mit dem Verantwortlichen erleichtert wird und grundrechtssichernde Maßnahmen effizient und erfolgversprechend durchgeführt werden können. Außerdem stärkt die Zusammenarbeit der europäischen Datenschutzaufsichtsbehörden aller Mitgliedstaaten das Ziel, den Datenschutz in Europa einheitlich voranzutreiben und für gleiche datenschutzrechtliche Werte einzustehen. Die behördliche Zusammenarbeit der europäischen Datenschutzaufsichtsbehörden bewirkt, dass die Betroffenen nicht selbst herausfinden müssen, welche europäische Behörde für ihre Beschwerde zuständig ist. Sie können sich direkt an eine beliebige Aufsichtsbehörde wenden, etwa die ihres Wohnorts. Dies ist Ausdruck des sogenannten One-Stop-Shop Prinzips aus Artikel 56 Absatz 1 DSGVO.

Im Jahr 2023 haben uns insgesamt 16 Fälle erreicht, die wir in das System IMI einpflegten, sodass uns beispielsweise eine Kommunikation mit den datenschutzrechtlichen Aufsichtsbehörden der Ländern Frankreich, Irland, Spanien und den Niederlanden ermöglicht wurde.

# 18. Die Beschlüsse des Europäischen Datenschutzausschusses

Der Europäische Datenschutzausschuss (EDSA) ist die Organisationsform, in der die datenschutzrechtlichen Aufsichtsbehörden in Europa gemeinsam handeln. Hierzu beschließt

der EDSA unter anderem Leitlinien, Empfehlungen und bewährte Verfahren zur Datenschutzgrundverordnung[2] und trifft verbindliche Beschlüsse in Einzelfällen.

## 19. Die Entschließungen der Datenschutzkonferenzen im Jahr 2023

### 19.1 Notwendigkeit spezifischer Regelungen zum Beschäftigtendatenschutz!

**Rechtsprechung des Europäischen Gerichtshofs hat Auswirkungen auf zahlreiche deutsche Vorschriften im Beschäftigungskontext**

(Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 11. Mai 2023)

Der Europäische Gerichtshof (EuGH) hat am 30. März 2023 in der Rechtssache C-34/21 über die Anforderungen an eine europarechtskonforme Umsetzung des Beschäftigtendatenschutzrechts in Hessen entschieden. In seinem Urteil formuliert der EuGH hohe Anforderungen an nationale Vorschriften, die auf der Grundlage der Öffnungsklausel des Artikels 88 der Verordnung (EU) 2016/679 (Datenschutzgrundverordnung – DSGVO) erlassen werden. Die Entscheidungsgründe legen nahe, dass die Vorschrift des § 23 Absatz 1 Satz 1 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes und § 86 Absatz 4 des Hessischen Beamtengesetzes diese Anforderungen nicht erfüllen.

Die Entscheidung des EuGH ist bundesweit von großer Bedeutung, weil Gesetzgeber aufgrund der Feststellungen des EuGH, soweit noch nicht geschehen, prüfen müssen, ob bestehende Regelungen zum Beschäftigtendatenschutz in Deutschland den Vorgaben von Artikel 88 DSGVO entsprechen.

Zum einen dürfen diese Regelungen nicht nur die Bestimmungen der DSGVO wiederholen, sondern es muss sich bei ihnen um spezifischere Vorschriften der Mitgliedstaaten handeln (siehe Artikel 88 Absatz 1 DSGVO). Zum anderen müssen diese inhaltlich den Vorgaben des Artikels 88 Absatz 2 DSGVO entsprechen. Danach müssen die mitgliedstaatlichen Vorschriften selbst Maßgaben zum Schutz der Rechte und Freiheiten der Beschäftigten sowie geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person enthalten.

Nationale Regelungen im Beschäftigtenkontext, die nicht den Vorgaben der DSGVO entsprechen, müssen unangewendet bleiben – so der EuGH. In diesen Fällen gelten aufgrund des Anwendungsvorrangs des Unionrechts unmittelbar die Bestimmungen der DSGVO.

[2] https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_de

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hatte bereits in ihrer Entschließung vom 29. April 2022, **"Die Zeit für ein Beschäftigtendatenschutzgesetz ist ‚Jetzt'!"**, festgestellt, dass die bestehende bundesrechtliche Regelung im Beschäftigtenkontext nicht hinreichend praktikabel, normenklar und sachgerecht ist und als Generalklausel weite Interpretationsspielräume eröffnet. Auch der vom Bundesministerium für Arbeit und Soziales (BMAS) eingesetzte unabhängige, interdisziplinäre Beirat zum Beschäftigtendatenschutz ist in seinem Bericht aus Januar 2022 zu dem Schluss gelangt, dass neben weiteren Maßnahmen ein eigenständiges Beschäftigtendatenschutzgesetz notwendig ist.

Anlässlich der EuGH-Entscheidung hält es die DSK für notwendig, über die vorgenannte Entschließung hinaus, den Gesetzgeber auf die daraus resultierenden inhaltlichen Anforderungen an datenschutzrechtliche Regelungen ausdrücklich hinzuweisen.

Die DSK fordert daher den Gesetzgeber erneut auf, ein Beschäftigtendatenschutzgesetz zu schaffen. Sie begrüßt, dass das Bundesministerium für Arbeit und Soziales (BMAS) und das Bundesministerium des Innern und für Heimat (BMI) mit den Arbeiten für ein Beschäftigtendatenschutzgesetz begonnen haben.

Das Urteil des EuGH vom 30. März 2023 in der Rechtssache C-34/21 ist abrufbar unter:

https://curia.europa.eu/juris/document/document.jsf?text=&docid=272066&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=3515175

Die Entschließung der DSK vom 29. April 2022 "Die Zeit für ein Beschäftigten-datenschutzgesetz ist ‚Jetzt'!" ist abrufbar unter:

https://www.datenschutzkonferenz-online.de/entschliessungen.html

Der Bericht des unabhängigen, interdisziplinären Beirats zum Beschäftigtendatenschutz ist abrufbar unter:

https://www.bmas.de/SharedDocs/Downloads/DE/Arbeitsrecht/ergebnisse-beirat-beschaeftigtendatenschutz.pdf?__blob=publicationFile&v=6

## 19.2 Verfassungsrechtliche Anforderungen bei automatisierter Datenanalyse durch Polizei und Nachrichtendienste beachten!

(Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 11. Mai 2023)

Mit Urteil vom 16. Februar 2023 hat das Bundesverfassungsgericht verfassungsrechtliche Weichen für den behördlichen Einsatz von automatisierten Datenanalysen / -auswertungen gestellt (- 1 BvR 1547/19 - und - 1 BvR 2634/20 -). Das Bundesverfassungsgericht hat entschieden, dass das Gewicht des mit der Datenanalyse verbundenen Grundrechtseingriffs insbesondere durch Art und Umfang der zu verarbeitenden Daten und die zugelassene Methode der Datenanalyse bestimmt wird. Ein besonderes Eingriffsgewicht aufgrund von Art und Umfang der Daten ist regelmäßig gegeben, wenn viele Daten zu Personen in die Datenanalyse eingehen, die selbst keinen Anlass für polizeiliche Maßnahmen gegeben haben. Das trifft beispielsweise auf Datenbestände aus Funkzellenabfragen und aus der Vorgangsbearbeitung zu. Funkzellenabfragen betreffen alle Personen, die in der Funkzelle mit ihrem Mobilgerät eingebucht sind. Datenbestände insbesondere aus Vorgängen der Strafverfolgung enthalten regelmäßig auch Daten von Opfern und Zeugen. Besonderes Eingriffsgewicht aufgrund der Methode der Datenanalyse können insbesondere die Verwendung lernfähiger Systeme – Künstliche Intelligenz ("KI") –, aber auch komplexe Formen des Datenabgleichs mit nicht lernfähigen Systemen haben. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) sieht ihre Forderungen aus ihrer Entschließung vom 3. April 2019 "Hambacher Erklärung zur Künstlichen Intelligenz" in dem Urteil bestätigt.

Die DSK, deren Mitglieder in dem Verfahren angehört wurden, betont, dass die im Bereich der Polizei und Nachrichtendienste vorhandenen allgemeinen Vorschriften den Besonderheiten komplexer Analysemethoden nicht ausreichend Rechnung tragen. Dies gilt jedenfalls für solche Analysemethoden, die mit intensiven Eingriffen in die Grundrechte der betroffenen Personen verbunden sein können. Hierfür bedürfte es eigener verhältnismäßig ausgestalteter Rechtsgrundlagen. Der Gesetzgeber wäre dann in der Pflicht, die wesentlichen Grundlagen selbst durch spezifische gesetzliche Vorschriften vorzugeben, um insbesondere Art und Umfang der Daten und die Verarbeitungsmethoden zu begrenzen.

Aufsichtsbehördlichen Erfahrungen entsprechend werden im Bereich der Strafverfolgung und der Gefahrenabwehr auch komplexe Formen der Datenanalyse eingesetzt, mitunter Systeme und Komponenten, die auf maschinellem Lernen basieren. Gerade polizeiliche Ermittlungen und nachrichtendienstliche Beobachtung können mit intensiven Grundrechtseingriffen verbunden sein. Daher ist die Beachtung verfassungsrechtlicher Anforderungen an das Handeln von Polizei und Nachrichtendiensten besonders dringlich.

Die Konferenz appelliert an die in Bund und Ländern politisch Verantwortlichen, den sich aus dem Urteil ergebenden gesetzgeberischen Handlungsbedarf zu prüfen. Erachten sie den Einsatz komplexer Datenanalysemethoden für erforderlich, müssen hierfür klare Rechtsgrundlagen und geeignete Rahmenbedingungen geschaffen werden, mittels derer der

Grundrechtsschutz betroffener Personen sichergestellt wird. Die vorhandenen gesetzlichen Bestimmungen sind in der Praxis in verfassungskonformer Weise anzuwenden.

## 19.3 Geplante Chatkontrolle führt zu einer unverhältnismäßigen, anlasslosen Massenüberwachung!

(Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 17. Oktober 2023)

Die EU-Kommission beabsichtigt, technische Verfahren zur Überwachung der elektronischen Kommunikation zu ermöglichen, deren erklärtes Ziel es ist, Darstellungen von Kindesmissbrauch im Internet vorzubeugen beziehungsweise aufzudecken. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden (Datenschutzkonferenz) weist darauf hin, dass die von der EU-Kommission vorgesehene Wahl der Mittel äußerst zweifelhaft ist, denn hierdurch wären massenweise zum Teil sehr sensible Informationen sämtlicher Nutzender, die E-Mails oder andere Nachrichten in Online-Diensten austauschen, unterschiedslos und verdachtsunabhängig von einer Überwachung betroffen.

Im Mai 2022 hat die Kommission einen Vorschlag für eine Verordnung zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern vorgelegt. Der Vorschlag sieht unter anderem vor, dass Anbieter von E-Mail oder Online-Diensten zur Nachrichtenübermittlung dazu verpflichtet werden, sexuellen Kindesmissbrauch im Internet aufzudecken. Dazu müssen die Anbieter Maßnahmen ergreifen, um die Verbreitung von bekannten oder neuen Darstellungen sexuellen Kindesmissbrauchs oder die Kontaktaufnahme zu Kindern anhand bestimmter Indikatoren zu erkennen.

Ohne Zweifel besteht die Notwendigkeit, Kinder vor sexuellem Missbrauch zu schützen und entsprechende Straftaten aufzudecken. Die Ziele der geplanten Verordnung an sich stehen also nicht infrage. Gleichwohl sind die staatlich angeordnete Kontrolle und Überwachung von Kommunikation in der umfassenden Form, die in dem Verordnungsentwurf vorgesehen ist, von unverhältnismäßigem Ausmaß. Es wird eine Vielzahl von Nutzenden mit einer erheblichen Menge sehr persönlicher Informationen aus sämtlichen Lebensbereichen von den Überwachungsmaßnahmen betroffen sein – und zwar unabhängig davon, ob überhaupt der Verdacht einer Straftat besteht. Der gewählte Ansatz bedeutet, dass die Anbieter sämtliche über beziehungsweise mit ihren Diensten verarbeiteten Daten auf die genannten Inhalte hin überprüfen müssen. Je nachdem, um welche Art von Diensten es sich handelt, werden dabei Verkehrs-, Inhalts- und Standortdaten sowie sämtliche Inhalte der über einen Dienst abgewickelten zwischenmenschlichen Kommunikation überwacht – auch komplette Inhalte von E-Mails und Chats.

Die Verpflichtung soll auch dann gelten, wenn die Dienste eine Ende-zu-Ende verschlüsselte Kommunikation anbieten. De facto bedeutet dies eine Abkehr von der Ende-zu-Ende-Verschlüsselung, die sich in den letzten Jahren als notwendige Vorbedingung privater Kommunikation weitgehend etabliert hat. Damit die Maßnahmen gemäß dem Verordnungsentwurf umgesetzt werden können, müsste nämlich die Ende-zu-Ende-Verschlüsselung aufgebrochen werden.

Daraus folgt, dass Technologien wie Ende-zu-Ende-Verschlüsselung nicht mehr zuverlässig zur Verfügung stehen werden, sondern nur noch unter dem Vorbehalt, dass der anbietende Dienst die Verschlüsselung umgehen kann. Das läuft dem Ziel der Verschlüsselung zuwider, die ausdrücklich die Sicherheit und die Vertraulichkeit der Kommunikation von Nutzenden, einschließlich Kindern, wie der Verordnungsentwurf selbst feststellt, gewährleisten soll. Es ist ein Bruch der Vertraulichkeit elektronischer Kommunikation mit nicht absehbaren Folgen für die Kommunikationsfreiheit als eines der demokratiesichernden Grundrechte schlechthin. Damit wird diese Vertraulichkeitsmaßnahme nicht nur gegenüber den Anbietern nutzlos, sondern es erhöht sich auch generell das Risiko von Schwachstellen, die missbräuchlichen Zugriffen Tür und Tor öffnen. In einer Zeit, in der Sicherheitslücken in IT-Systemen vermehrt und in großem Stil für illegale Zwecke ausgenutzt werden, sollten Schwächungen des Schutzes vermieden werden, statt absichtlich Bruchstellen in den technischen Infrastrukturen einzubauen.

Die vorgesehene anlasslose Massenüberwachung greift fundamental in die Grundrechte auf Achtung des Privat- und Familienlebens, der Vertraulichkeit der Kommunikation und zum Schutz personenbezogener Daten ein. Vor dem Hintergrund der anstehenden Beratungen im Rat der Europäischen Union warnt die Datenschutzkonferenz

davor, den Wesensgehalt dieser Grundrechte anzutasten, und appelliert an den EU-Gesetzgeber, bei der Regulierung von Maßnahmen zur Bekämpfung schwerster Kriminalität die Grenzen der Rechtsstaatlichkeit einzuhalten und insbesondere Erforderlichkeit und Verhältnismäßigkeit zu wahren.

## 19.4 Datenschutz in der Forschung durch einheitliche Maßstäbe stärken

(Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 23. November 2023)

Medizinische Forschungsprojekte werden in Deutschland häufig nicht nur in einem Bundesland durchgeführt. Vielmehr sind zunehmend verschiedene Forschungseinrichtungen aus unterschiedlichen Ländern daran beteiligt (zum Beispiel länderübergreifende Verbundforschung, multizentrische Studien). Je nach Forschungsstandort sind unterschiedliche datenschutzrechtliche Anforderungen zu beachten. Dies erschwert nicht nur

die Forschung, sondern wirkt sich auch nachteilig auf den Datenschutz für die betroffenen Personen aus. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) fordert den Bundesgesetzgeber und die Landesgesetzgeber daher auf, durch aufeinander abgestimmte gesetzliche Regelungen auf hohem Datenschutzniveau den Datenschutz in der länderübergreifenden Forschung zu stärken. Hierfür hat sie Eckpunkte erarbeitet. Im Einzelnen:

In vielen Ländern enthalten verschiedene Landesgesetze, die beispielsweise die Datenverarbeitungen durch Krankenhäuser und Behörden des öffentlichen Gesundheitsdienstes betreffen, konkrete Befugnisse der jeweiligen Stellen zur Verarbeitung von Gesundheitsdaten zu Forschungszwecken, die den allgemeinen Vorgaben vorgehen. Diese gesetzlichen Regelungen stellen unterschiedliche datenschutzrechtliche Anforderungen. Bei länderübergreifender Forschung müssen von den Verantwortlichen die jeweils für sie geltenden Gesetze angewandt werden. Unterschiede bestehen insbesondere in Bezug auf die Zulässigkeit der Datenverarbeitung (gesetzliche Grundlage oder Einwilligung mit jeweils unterschiedlichen Anforderungen), die Definition von Schutzbereichen (unter anderem Patientinnen und Patienten, Angehörige) und zulässige Zwecke der Verarbeitung. Die rechtliche Bewertung und Umsetzung der jeweils geltenden Rechtsgrundlage führte in der Vergangenheit zu einem gesteigerten Beratungsbedarf und zu Unsicherheiten bei den Forschenden und Rechtsanwendern. Auch ergeben sich aus unterschiedlichen Regelungen Herausforderungen für eine transparente und verständliche Informationserteilung nach Artikel 13 und 14 der Datenschutz-Grundverordnung (DSGVO).

Das Bundesgesundheitsministerium hat mit dem Gesetzentwurf eines Gesundheitsdatennutzungsgesetzes (GDNG) eine Vereinheitlichung der forschungsrelevanten Rechtsgrundlagen vorgeschlagen. Geplant ist insoweit eine Rechtsgrundlage für die "Weiterverarbeitung von Versorgungsdaten zur Qualitätssicherung, zur Förderung der Patientensicherheit und zu Forschungszwecken" durch eine Gesundheitseinrichtung für die bei ihr rechtmäßig gespeicherten Daten.

Das Verhältnis dieser geplanten Neuregelungen zu den Landeskrankenhausgesetzen ist jedoch unklar. Mit der Gesetzgebungskompetenz der Länder für den Bereich der Krankenhäuser hat sich der Gesetzentwurf nicht auseinandergesetzt. Daher bestehen erhebliche Zweifel, dass mit diesem Gesetzentwurf eine rechtssichere und tragfähige Neuregelung erreicht wird, die die länderübergreifende Forschung erleichtert.

Die DSK hat in ihrer Stellungnahme zum GDNG-Gesetzentwurf vom 14.08.2023 hierauf hingewiesen und weiteren Korrekturbedarf aufgezeigt.[3]

In dieser Stellungnahme und in der "Petersberger Erklärung" vom 24.11.2022 hat die DSK wichtige Hinweise für gesetzliche Neuregelungen formuliert.[4] Sie beschreiben wesentliche Anforderungen zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung, insbesondere zu den Rechtsgrundlagen und den besonderen Einwirkungsmöglichkeiten für betroffene Personen.

Um eine weitgehende Nutzung von Gesundheitsdaten zu Forschungszwecken im Einklang mit den Grundrechten zu normieren, sind konkrete Garantien und Maßnahmen gesetzlich festzulegen. Es gilt der Grundsatz: Je höher der Schutz der betroffenen Personen durch geeignete Garantien und Maßnahmen, desto umfangreicher und spezifischer können die Daten zu Forschungszwecken genutzt werden.[5] Abhängig von den jeweils verarbeiteten Datenarten – zum Beispiel personenbezogenen Daten (Artikel 4 Nummer 1 DSGVO), Gesundheitsdaten (Artikel 4 Nummer 15 DSGVO) oder genetische Daten (Artikel 4 Nummer 13 DSGVO) – bedarf es eines angemessenen Schutz- und Vertrauensniveaus und spezifischer Regelungen für die Verarbeitungen in den jeweiligen Bereichen der Forschung.

Für besondere Forschungsgegenstände, bei denen eine ausreichende Anonymisierung nicht immer gewährleistet werden kann (etwa für radiologische Bilddaten), sollten spezifische Regelungen getroffen werden, um einen angemessenen Schutz der Grundrechte der betroffenen Personen sicherzustellen, zum Beispiel durch zusätzliche technische und organisatorische Maßnahmen.

Darüber hinaus sind die Regelungen des Artikel 9 Absatz 2 Buchstabe j in Verbindung mit Artikel 89 Absatz 1 DSGVO zu beachten. Insbesondere müssen im Gesetz selbst angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person festgelegt werden. Diese Festlegung der spezifischen Anforderungen darf nicht an die Verantwortlichen delegiert werden. Die Umsetzung darf sich auch nicht in generalklauselartigen oder in solchen Regelungen erschöpfen, die die DSGVO ohnehin für die Datenverarbeitung vorsieht, wie etwa die Betroffenenrechte nach Artikel 15 fortfolgende DSGVO oder Maßnahmen nach Artikel 32 DSGVO. Stattdessen müssen konkrete Maßnahmen benannt werden.

---

[3] Die Stellungnahme der DSK vom 14.08.2023 zum Entwurf eines Gesetzes zur verbesserten Nutzung von Gesundheitsdaten (Gesundheitsdatennutzungsgesetz – GDNG – Stand 03.07.2023) ist abrufbar unter https://datenschutzkonferenz-online.de/media/st/23_08_14_DSK_Stellungnahme_GDNG-E.pdf

[4] Die Entschließung der DSK vom 24.11.2022 (Petersberger Erklärung) ist abrufbar unter: https://www.datenschutzkonferenz-online.de/media/en/20221124_en_06_Entschliessung_Petersberger_Erklaerung.pdf

[5] Vergleiche Empfehlung Nummer 2 der Petersberger Erklärung.

Angemessene und spezifische Maßnahmen in diesem Sinne können etwa sein:

- Vorgaben für die Datenschutz-Folgenabschätzung (zum Beispiel Betrachtungstiefe, Aufgabenzuweisungen für die Durchführung),
- die Schaffung weiterer, über die in Artikel 15 fortfolgende DSGVO hinausgehender Betroffenenrechte (zum Beispiel spezifische Widerspruchsrechte, Vernichtung von Bioproben),
- die Festlegung angemessener Sperrfristen, die den betroffenen Personen ermöglichen, ihre Rechte auszuüben, bevor mit ihren Daten geforscht werden darf (zum Beispiel bei einem Widerspruchsrecht),
- die Einbindung einer unabhängigen Treuhandstelle insbesondere zur Verschlüsselung, Anonymisierung oder Pseudonymisierung der Daten,
- die Einrichtung von Datenintegrationszentren oder Forschungsplattformen, soweit konkrete, der DSGVO entsprechende Anforderungen an deren Ausgestaltung formuliert werden,
- die Verpflichtung beteiligter Stellen zur Verschwiegenheit und die Schaffung korrespondierender Prozessrechte wie ein Beschlagnahmeverbot und Zeugnisverweigerungsrechte,
- konkrete Festlegungen zur Ausgestaltung und Gewährleistung der Datenminimierung.

Diese Aufzählung ist nicht abschließend. Es ist die Aufgabe des Gesetzgebers, die Risiken zu erkennen, die mit einer Verarbeitung von Gesundheitsdaten verbunden sind, sie zu benennen und ihnen angemessene Schutzmaßnahmen für die Rechte und Interessen der betroffenen Personen gegenüberzustellen.

Die DSK weist darauf hin, dass medizinische personenbezogene Daten in bestimmten Fallkonstellationen dem absoluten Schutz des Kernbereichs privater Lebensgestaltung unterliegen.

Die Verarbeitung solcher menschenwürderelevanter Daten kann selbst zu Forschungszwecken nicht auf Grundlage einer gesetzlichen Regelung legitimiert werden.

Schließlich ist eine uneingeschränkte Datenschutzaufsicht in dem sensiblen Bereich der Verarbeitung von Gesundheitsdaten zu garantieren. Diese bietet Schutz für die betroffenen Personen. Etwaig bestehende Einschränkungen der Befugnisse der Datenschutzaufsichtsbehörden hinsichtlich der Verhängung von Bußgeldern und des Vollzugs gegenüber öffentlichen Stellen sind zumindest im Anwendungsbereich entsprechender Regelungen aufzuheben.

Die DSK setzt sich für die Schaffung eines hohen Datenschutzniveaus in der medizinischen Forschung durch eine aufeinander abgestimmte zeitnahe rechtsklare und systematische Neustrukturierung der entsprechenden rechtlichen Regelungen ein. Sie appelliert an die Gesetzgeber des Bundes und der Länder, durch klarstellende Regelungen einen wirksamen Kernbereichsschutz sicherzustellen.

Die Datenschutzaufsichtsbehörden bieten an, in Wahrnehmung ihrer Beratungsfunktion die Gesetzgeber vor und bei entsprechenden Gesetzesvorhaben zu unterstützen.

## 19.5 Rahmenbedingungen und Empfehlungen für die gesetzliche Regulierung medizinischer Register

(Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 23. November 2023)

Das Vorhaben der Bundesregierung, für die ausgesprochen heterogene Vielfalt medizinischer Register einen allgemeinen Rahmen und eine einheitliche Basis zu schaffen, um Daten im öffentlichen Interesse nutzen zu können, ist aus datenschutzrechtlicher Perspektive nachvollziehbar. Allerdings muss sichergestellt sein, dass auch im konkreten Anwendungsfall die datenschutzrechtlichen Vorgaben eingehalten werden und das Grundrecht auf Datenschutz stets gewährleistet ist. Sowohl für die Befüllung der Register als auch für die registerinterne Verarbeitung und die Bereitstellung sowie die mögliche Nutzung der Daten durch Dritte sind die spezifischen datenschutzrechtlichen Voraussetzungen für die Verarbeitung von Gesundheitsdaten, insbesondere aus den Artikeln 9, 25, 32 und gegebenenfalls Artikel 89 Absatz 1 Datenschutzgrundverordnung (DSGVO), maßgeblich.

Es gibt eine Vielzahl medizinischer Register in Deutschland in unterschiedlichen Strukturen und Formen. Wenige sind spezialgesetzlich geregelt oder basieren auf allgemeinen gesetzlichen Grundlagen. Die meisten stützen sich zur Datenverarbeitung auf Einwilligungen: verschiedene stammen aus abgeschlossenen Forschungsvorhaben, andere werden auf Patienteninitiative oder von Fachgesellschaften zu bestimmten Erkrankungen betrieben; nicht alle werden noch aktiv genutzt.

Anknüpfend an die Festlegungen im Koalitionsvertrag "Mehr Fortschritt wagen" vom November 2021 (Seite 83), wonach neben einem Gesundheitsdatennutzungsgesetz auch ein Registergesetz im Einklang mit der DSGVO geschaffen werden soll, sieht die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) Anlass, ergänzend zu ihren bisherigen Forderungen und Empfehlungen die datenschutzrechtlichen Anforderungen und Bedingungen für die Regulierung einer Datenverarbeitung in medizinischen Registern zu präzisieren. Soweit die Datenverarbeitung den Zwecken

wissenschaftlicher Forschung dient, gelten daneben die Hinweise in der "Petersberger Erklärung" der DSK aus dem November 2022.[6]

Die DSK begrüßt, dass durch das vom Bundesministerium für Gesundheit (BMG) beauftragte Gutachten zur Weiterentwicklung medizinischer Register[7] ein nahezu vollständiger Überblick[8] über die vorhandenen Register und die darin enthaltenen Daten vorliegt. Zugleich schließt sich die DSK der darin enthaltenen Empfehlung an, durch die nun geplante Gesetzgebung ein entsprechendes Registerverzeichnis zu verstetigen und dauerhaft öffentlich zugänglich zu gestalten. Die DSK befürwortet insbesondere die Überlegungen zur Schaffung einer Zentralstelle für medizinische Register, die das Registerverzeichnis führen und die eine Auditierung und Zuordnung medizinischer Register je nach vorhandener Qualitätsstufe (im Gutachten als "Reifegrad" bezeichnet) verantworten soll. Aufgrund der Aufgaben der Zentralstelle für medizinische Register, die maßgeblich für die weitere Verarbeitung der in den medizinischen Registern enthaltenen Daten sind, hält es die DSK für geboten, hiermit eine unabhängige Körperschaft des öffentlichen Rechts zu betrauen. Dieser Zentralstelle könnte zudem eine besondere Funktion als Ansprechpartner und Lotse für die betroffenen Personen sowie bei der Erfüllung der Betroffenenrechte zukommen.

Die DSK teilt das aus dem Koalitionsvertrag erkennbare Anliegen, durch die gesetzliche Regelung die bislang heterogene Registerlandschaft zu strukturieren und zum Aufbau fachlich qualitätsgesicherter Register beizutragen. Entsprechend den Ausführungen im Gutachten bietet es sich an, bei der Zuordnung der Register je nach Qualitätsstufe zu verschiedenen Kategorien die Datenqualität, die Datenstruktur und die Standards bei der Verarbeitung zu berücksichtigen.

Insbesondere folgende Rahmenbedingungen sind aus datenschutzrechtlicher Sicht bei der gesetzlichen Regulierung medizinischer Register vorzusehen:

- Werden personenbezogene Daten an die Register übermittelt und von diesen erhoben, die nicht unmittelbar für das Register, sondern zu einem anderen Zweck erhoben worden sind, bedarf es hierfür – soweit dies nicht durch Einwilligungen gedeckt ist – klarer gesetzlicher Festlegungen zu den Voraussetzungen der zweckändernden Datenverarbeitung, die den Anforderungen aus Artikel 6 Absatz 4 DSGVO entsprechen.
- Es sind rechtsklare und verhältnismäßige Regelungen über die Aufbewahrungsdauer und Löschfristen der Registerdaten unter der Maßgabe der Grundsätze der Datenminimierung und Speicherbegrenzung zu treffen.

---

[6] Entschließung der DSK "Petersberger Erklärung zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung" vom 24. November 2022.
[7] Gutachten zur Weiterentwicklung medizinischer Register zur Verbesserung der Dateneinspeisung und -anschlussfähigkeit, TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. und BQS – Institut für Qualität und Patientensicherheit, 29. Oktober 2021.
[8] Unter dem Link: https://registersuche.bqs.de/search.php sind ca. 400 Register gelistet.

- Eine Befugnis zur Übermittlung von personenbezogenen Gesundheitsdaten an das Register, zu deren Speicherung im Register sowie zu deren Übermittlung an Dritte unter Verzicht auf eine vorherige Einbindung der betroffenen Person bedarf mindestens der medizinisch-fachlichen Erforderlichkeit für einen der in Artikel 9 Absatz 2 - 4 DSGVO genannten Zwecke, der gesetzlichen Definition der zu verarbeitenden personenbezogenen Daten und bei Forschungszwecken dienenden Registern eines allgemeinen, voraussetzungslosen Widerspruchsrechts.
- Bei der Festlegung von Voraussetzungen für eine datenschutzkonforme Verarbeitung von Registerdaten, insbesondere den Anforderungen für die Übermittlung an und Erhebung durch die Register, die weitere Verarbeitung der Daten in den Registern und deren Bereitstellung für Dritte, sowie einer Definition der zu verarbeitenden Einzelangaben, sind außer den Maßgaben der Öffnungsklauseln nach Artikel 9 Absatz 2 DSGVO und gegebenenfalls den Garantien nach Artikel 89 Absatz 1 DSGVO auch die Vorgaben des Grundrechts auf Datenschutz zu berücksichtigen. Insbesondere müssen sich wesentliche Grundrechtseinschränkungen unmittelbar aus dem Gesetz ergeben.
- Bei den gesetzlichen Regelungen sollte die Rechtmäßigkeit der Datenverarbeitung abhängig von dem jeweiligen Zweck differenziert festgelegt werden. Eine Nutzung zur wissenschaftlichen Forschung erfordert beispielsweise andere Bedingungen als eine Auswertung zu Zwecken einer – gesetzlich jeweils näher zu bezeichnenden – Qualitätssicherung. Dies muss berücksichtigt werden.
- Die DSK hält es für erforderlich, dass mit der gesetzlichen Regulierung der medizinischen Register auch Vorgaben zu technisch-organisatorischen Maßnahmen standardisiert und harmonisiert festgelegt werden. Damit wird das dem Risiko angemessene Schutzniveau für die Verarbeitungen verdeutlicht und eine effektive Datenschutzaufsicht ermöglicht. Insbesondere bei besonderen Risiken, wie zum Beispiel einem Remotezugriff auf Gesundheitsdaten über digitale Portale, wird dem Gesetzgeber empfohlen, im Rahmen einer sogenannten gesetzlichen Datenschutz-Folgenabschätzung (DSFA) globale Risiken der Registersysteme zu ermitteln und so geeignete technische und organisatorische Maßnahmen zur Minimierung dieser Risiken bereits im Gesetz zu regeln. Dies kann die Verantwortlichen zwar nicht vollständig von einer eigenen DSFA entlasten, trägt aber zur Schaffung einheitlicher Mindeststandards bei.
- Die DSK empfiehlt, durch die gesetzlichen Regelungen digitale Methoden unter anderem für das Einwilligungsmanagement und die Ausübung der Betroffenenrechte zu fördern sowie – beispielsweise durch Portale – eine Partizipation der Betroffenen zu ermöglichen.
- Die DSK hält es grundsätzlich für tragfähig, für qualitätsgesicherte Register ein Zulassungsverfahren vorzusehen mit dem Ziel, dass für bestimmte im Registerverzeichnis entsprechend gelistete Register bestehende oder noch zu schaffende gesetzliche Datenverarbeitungsbefugnisse herangezogen werden können. Dabei ist hinsichtlich der einzelnen Verarbeitungsschritte der Übermittlung an das Register, der Erhebung und der

Bereitstellung der Daten durch das Register sowie der Verwendung bei der weiteren Nutzung der Registerdaten zu differenzieren.

- Für die Register sollten regelmäßig unabhängige Vertrauensstellen vorgesehen werden. Diese könnten eine zentrale Rolle bei der Anonymisierung und Pseudonymisierung von Gesundheitsdaten vor der Bereitstellung für Forschende und bei der Verwaltung bereichsspezifischer Kennzeichen als einheitliche Identifikatoren spielen.
- Im Zulassungsverfahren sollten relevante Aspekte des Datenschutzes (zum Beispiel die Rechtsgrundlagen und die Gewährleistung der Betroffenenrechte) und der Informationssicherheit geprüft werden. Die DSK empfiehlt, die Festlegung des Zulassungsverfahrens mit ihr abzustimmen, um die technisch-organisatorischen Maßnahmen und die datenschutzrechtlichen Prinzipien – wie Verschlüsselung, Pseudonymisierung, Erforderlichkeitsgrundsatz, Anonymisierung, Nutzung synthetischer Daten – bei der Datenerhebung, bei der Verarbeitung innerhalb des Registers und bei der Bereitstellung der Daten durch das Register zu gewährleisten. Zugleich sollte für die Zulassung ein Verfahren vorgesehen werden, mit dem die Einhaltung der Qualitätsstandards sowie die Angemessenheit des Schutzniveaus in regelmäßigen Abständen wiederholt geprüft und nachgewiesen wird.
- Im Zulassungsverfahren sollten auch das Verfahren, das Schutz- und Vertrauensniveau der Schnittstellen und die Voraussetzungen geprüft werden, mit denen ein Register Daten an Dritte bereitstellt oder übermittelt. Nutzungsanträge und -bewilligungen sollten aus Transparenzgründen vom Register und von der für den Nutzungsantrag zuständigen Stelle veröffentlicht werden.
- Zur Verminderung von Risiken und zur datenschutzkonformen Auswertung von Daten sollte in der gesetzlichen Regelung die Nutzung geeigneter technischer und organisatorischer Methoden einschließlich der dezentralen Speicherung und Verarbeitung gefordert werden.
- Es wird empfohlen, gesetzlich festzulegen, welche datenschutzrechtliche Rolle den beteiligten Stellen für welche Verarbeitungsvorgänge zukommt, das heißt ob eine eigene oder gemeinsame Verantwortlichkeit oder eine Auftragsverarbeitung vorliegt.
- Der datenschutzrechtliche Grundsatz der Zweckbindung nach Artikel 5 Absatz 1 Buchstabe b DSGVO steht der Verknüpfung von Datensätzen grundsätzlich entgegen. Sofern für Zwecke der wissenschaftlichen Forschung Datensätze verknüpft werden sollen, bedarf es im Hinblick auf das Grundrecht auf Datenschutz einer besonderen Rechtfertigung, die sich in der Regel aus einem öffentlichen Interesse und einem gesellschaftlichen Nutzen ergeben soll. Wegen der sich aus einer Verknüpfung ergebenden Risiken sollte sie nur anlassbezogen und temporär zulässig sein.
- Bei der Verwendung einheitlicher Identifikatoren sollten bereichsspezifische Kennzeichen eingesetzt werden. Im Bereich der Datenverarbeitung durch medizinische Register wäre ein spezifisches datenschutzfreundliches Identifikationssystem für den

Gesundheitsbereich denkbar: So könnten beispielsweise aus einer bereits vorhandenen Krankenversichertennummer nicht rückrechenbare, bereichsspezifische Pseudonyme für die Register jeweils gesondert durch geschützte Verfahren gebildet und gespeichert werden, die sich nur über eine zentrale Vertrauensstelle zuordnen ließen. Soweit die Zentralstelle für medizinische Register auch datenschutzrechtliche Aspekte prüft, sollte das Verhältnis zu den Datenschutzaufsichtsbehörden unter Beachtung der Vorgaben der DSGVO gesetzlich geklärt werden.