Landtag von Baden-Württemberg **Drucksache 17 / 6248**

17. Wahlperiode **20.2.2024**

Kleine Anfrage

der Abg. Julia Goll FDP/DVP

und

Antwort

des Ministeriums des Inneren, für Digitalisierung und Kommunen

Einhaltung des Datenschutzes bei Behörden

Kleine Anfrage

Ich frage die Landesregierung:

1. Wie oft hat der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI) bzw. seine Behörde die Rechtswidrigkeit landesverwaltungsrechtlichen Handelns in den letzten fünf Jahren positiv festgestellt (bitte unter Benennung der genauen Anzahl festgestellter datenschutzrechtlicher Verstöße, getrennt aufgelistet für die drei Verwaltungsebenen: Ministerien, Regierungspräsidien und untere Verwaltungsbehörden)?

2. Um welche Verstöße handelt es sich dabei (bitte aufgeschlüsselt nach Arten der Verstöße und unter Zuordnung der Verstöße zu den drei Verwaltungsebenen)?

3. Wie häufig hat der LfDI dabei in den letzten fünf Jahren rechtswidriges Handeln der einzelnen Ministerien positiv festgestellt (bitte dargestellt unter Trennung der einzelnen Ministerien und unter Darstellung der jeweiligen datenschutzrechtlichen Verstöße, insbesondere der Verstöße gegen die Geheimhaltungspflicht)?

4. Wodurch wurde der LfDI bzw. seine Behörde ihrer Kenntnis nach auf die Fälle der Rechtswidrigkeit landesverwaltungsrechtlichen Handelns der letzten fünf Jahre aufmerksam (beispielsweise durch Anzeigen von Staatsanwaltschaft und Polizei, durch Eingaben von Bürgern oder durch ermittelte Vorlagen der Fachreferate der Dienststelle des LfDI)?

5. Gab es in den letzten fünf Jahren Datenpannen im landesverwaltungsrechtlichen Bereich (bitte unter Darstellung der Art der Pannen, dem zuzuordnenden Bereich der Landesverwaltung und dem Umgang der Behörden damit)?

Eingegangen: 20.2.2024 / Ausgegeben: 21.3.2024

6. Welche Untersuchungsbefugnisse (Artikel 58 Absatz 1 Datenschutz-Grundverordnung [DSGVO]), welche Abhilfebefugnisse, insbesondere Bußgeldverhängungen (Artikel 58 Absatz 2 in Verbindung mit Artikel 83 DSGVO), welche Beratungs- und Kontrollbefugnisse (Artikel 58 Absatz 3 DSGVO) wurden in den letzten fünf Jahren infolge der festgestellten Rechtswidrigkeit vom LfDI bzw. seiner Behörde gegenüber den Ministerien ausgeübt (bitte unter Darstellung jedes Buchstabens der genannten Vorschriften und getrennt für jedes Ministerium)?

7. Welche Reaktionen auf die festgestellte Rechtswidrigkeit waren im internen Bereich der Ministerien in den letzten fünf Jahren festzustellen (bitte aufgeschlüsselt nach disziplinarischen, organisatorischen und sonstigen [zu benennenden] Maßnahmen)?

8. Inwieweit bewertet sie diesen internen Umgang der Ministerien mit datenschutzrechtlichen Verstößen in den letzten fünf Jahren als ausreichend im Sinne der hohen Bedeutung des Datenschutzes?

9. Wie beurteilt sie die Zusammenarbeit der Ministerien mit dem LfDI bzw. seiner Behörde in den letzten fünf Jahren (insbesondere unter Berücksichtigung eines [nicht] transparenten Verhaltens der Ministerien im Falle eines datenschutzrechtlichen Verstoßes und unter Bewertung der Annahme von Angeboten des LfDI in Bezug auf mögliche Beratungen)?

10. Inwiefern wurden die organisatorischen und technischen Bereiche der Ministerien in den letzten fünf Jahren weiterentwickelt, um den stets gewichtiger werdenden datenschutzrechtlichen Vorgaben gerecht zu werden und den Datenschutz im Allgemeinen umfassend zu gewährleisten?

20.2.2024

Goll FDP/DVP

Begründung

Die obigen Fragen im Zusammenhang mit dem Datenschutz bei Behörden sind unmittelbar klärungsbedürftig.

Antwort

Mit Schreiben vom 13. März 2024 Nr. IM2-0557-28/19/37 beantwortet das Ministerium des Inneren, für Digitalisierung und Kommunen im Einvernehmen mit dem Staatsministerium, dem Ministerium für Finanzen, dem Ministerium für Kultus, Jugend und Sport, dem Ministerium für Wissenschaft, Forschung und Kunst, dem Ministerium für Umwelt, Klima und Energiewirtschaft, dem Ministerium für Wirtschaft, Arbeit und Tourismus, dem Ministerium für Soziales, Gesundheit und Integration, dem Ministerium der Justiz und für Migration, dem Ministerium für Verkehr, dem Ministerium für Ernährung, Ländlichen Raum und Verbraucherschutz und dem Ministerium für Landesentwicklung und Wohnen die Kleine Anfrage wie folgt:

1. *Wie oft hat der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI) bzw. seine Behörde die Rechtswidrigkeit landesverwaltungsrechtlichen Handelns in den letzten fünf Jahren positiv festgestellt (bitte unter Benennung der genauen Anzahl festgestellter datenschutzrechtlicher Verstöße, getrennt aufgelistet für die drei Verwaltungsebenen: Ministerien, Regierungspräsidien und untere Verwaltungsbehörden)?*
2. *Um welche Verstöße handelt es sich dabei (bitte aufgeschlüsselt nach Arten der Verstöße und unter Zuordnung der Verstöße zu den drei Verwaltungsebenen)?*
3. *Wie häufig hat der LfDI dabei in den letzten fünf Jahren rechtswidriges Handeln der einzelnen Ministerien positiv festgestellt (bitte dargestellt unter Trennung der einzelnen Ministerien und unter Darstellung der jeweiligen datenschutzrechtlichen Verstöße, insbesondere der Verstöße gegen die Geheimhaltungspflicht)?*

Zu 1. bis 3.:

Die Fragen 1 bis 3 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Für die Ministerien wird auf die Stellungnahme zum Antrag der Abgeordneten Julia Goll u. a. FDP/DVP „Rügen und weitere Maßnahmen des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI) gegen das Innenministerium und weitere Ministerien“, Drucksache 17/4960, verwiesen. In Bezug auf die Zeit nach der Stellungnahme zum Antrag wurde vom LfDI kein datenschutzrechtlicher Verstoß positiv festgestellt. Auf die Meldungen der in der Antwort zu Frage 5. aufgeführten Vorfälle erfolgten keine Maßnahmen des LfDI.

Im Bereich der Regierungspräsidien wurde ein Fall mitgeteilt:

In einem Anhörungsschreiben wurden der Name, die Schule und der Schulort einer dritten Person genannt.

Im nachgeordneten Bereich der Regierungspräsidien sind sechs Fälle aus den letzten fünf Jahren bekannt, in denen der LfDI die Rechtswidrigkeit landesverwaltungsrechtlichen Handelns festgestellt hat:

Einmal wurden E-Mail-Adressen an unberechtigte Personen durch Missachtung der Einstellungen zur Blindkopie („Bcc.“) mitgeteilt (Information zu impfenden Personen, Artikel 9 der Datenschutz-Grundverordnung – DSGVO), einmal ein Verstoß gegen den Sozialdatenschutz begangen und zweimal personenbezogene Daten an unbeteiligte Dritte herausgegeben.

In einem weiteren Fall wurde über das öffentliche Internet unbefugt Zugang zu personenbezogenen Daten bei einem Landratsamt erlangt. Die Daten wurden nur angezeigt, nicht heruntergeladen.

Schließlich wurde in einem Fall auf der Homepage einer nachgeordneten Behörde nicht ausreichend bezüglich der Einwilligung in Cookies informiert.

4. Wodurch wurde der LfDI bzw. seine Behörde ihrer Kenntnis nach auf die Fälle der Rechtswidrigkeit landesverwaltungsrechtlichen Handelns der letzten fünf Jahre aufmerksam (beispielsweise durch Anzeigen von Staatsanwaltschaft und Polizei, durch Eingaben von Bürgern oder durch ermittelte Vorlagen der Fachreferate der Dienststelle des LfDI)?

Zu 4.:

Die Landesregierung wird über Meldungen an den LfDI nicht unterrichtet. Der LfDI entscheidet als unabhängige oberste Landesbehörde über sein Tätigwerden.

Unter dem erwähnten Vorbehalt ist in Bezug auf die gemeldeten Fälle folgendes bekannt geworden:

Der gemeldete Fall auf Ebene der Regierungspräsidien wurde durch eine Beschwerde des Empfängers fremder personenbezogener Daten bekannt.

Im nachgeordneten Bereich hat sich bei dem genannten Verstoß gegen den Sozialdatenschutz der Betroffene beim LfDI beschwert. In dem Fall betreffend die nicht ausreichende Information bezüglich der Einwilligung in Cookies hatte ein Bürger dem LfDI einen Hinweis gegeben. In den anderen vier Fällen haben die verantwortlichen Behörden den LfDI in Kenntnis gesetzt bzw. gab es in dem zuletzt genannten Fall zusätzlich einen Hinweis aus der Bevölkerung.

5. Gab es in den letzten fünf Jahren Datenpannen im landesverwaltungsrechtlichen Bereich (bitte unter Darstellung der Art der Pannen, dem zuzuordnenden Bereich der Landesverwaltung und dem Umgang der Behörden damit)?

Zu 5.:

Die Landesregierung versteht unter „Datenpannen“ Vorfälle, die gemäß Artikel 33 DSGVO dem LfDI gemeldet wurden.

In der Kürze der zur Stellungnahme zur Verfügung stehenden Zeit erfolgten nicht von allen Behörden der Landesverwaltung Rückmeldungen.

Folgende Vorfälle wurden dem LfDI gemeldet:

Im Bereich des Staatsministeriums:

Art des Vorfalls	Umgang
Fehlversand einer E-Mail aus dem Bereich der Personalverwaltung.	- Unverzüglicher Rückruf der E-Mail (teilweise erfolgreich) - Unverzügliche Aufforderung an die Empfänger zur Löschung - Information der betroffenen Person - Nochmalige Sensibilisierung der beteiligten Beschäftigten .

Im Bereich des Innenministeriums:

Art des Vorfalls	Umgang
service-bw: Nachrichtenvorfall/Nachrichtenverlust: Im Zeitraum des Vorfalls wurden ca. 20 % der versendeten Nachrichten nicht zugestellt.	Unverzügliche Behebung.
service-bw: Einem Nutzer wurden fremde Antragsdaten angezeigt. Nur ein einziger nachgewiesener Vorfall am 24.6.2022.	Unverzügliche Behebung.
service-bw: Bei 273 Nachrichten, die von service-bw an Fachverfahren übertragen wurden, fehlten die Anhänge.	Unverzügliche Behebung.

Im Bereich des Finanzministeriums:

Art des Vorfalls	Umgang
Meldung als Auftraggeber in einem Auftragsverarbeitungsverhältnis.	Keine weiteren Maßnahmen notwendig, da es sich um einen nicht vergleichbaren Einzelfall handelt.
Fehlende Benachrichtigung nach Artikel 14 DSGVO.	Dto.

Im Bereich des Statistischen Landesamts als nachgeordnete Stelle des Finanzministeriums:

Art des Vorfalls	Umgang
Offener E-Mail-Verteiler bei der Information zu einer Veranstaltung.	Einsatz einer Software mit automatisierten Einstellungen.
Verlust von Unterlagen durch Erhebungsbeauftragte.	Hinweis auf Sorgfaltspflichten, Untersagung der Nutzung von E-Postscan-Aufträgen.
Versehentliche Veröffentlichung von Daten im Internet.	Einführung 4-Augen-Prinzip.
Fehlkuvertierung.	Behebung technischer Fehler an Kuvertiermaschine.
Fehlversand	Hinweis auf Sorgfaltspflichten.
Fehlerhafte Vorbelegung von Daten in Online-Meldeverfahren.	Durchführung eines Versionsupdates.

Im Bereich des Landesamts für Besoldung und Versorgung (LBV) als nachgeordnete Stelle des Finanzministeriums:

Art des Vorfalls	Umgang
Fehlsendung/Fehlerhafte Adressierung.	Datenschutzrelevante Vorgänge werden unverzüglich vom Datenschutzbeauftragten des LBV in Zusammenarbeit mit dem jeweiligen Fachbereich geprüft, bewertet und dokumentiert. Die Melde- und Benachrichtigungspflichten gemäß Artikel 33 und 34 DSGVO werden beachtet. Die Meldungen an die Aufsichtsbehörde LfDI erfolgen unverzüglich und möglichst im Zeitfenster von 72 Stunden. Erfolgt die Meldung nicht binnen 72 Stunden, wird dies begründet. Eine Überprüfung der Aufsichtsbehörde LfDI gemäß Artikel 33 Absatz 5 DSGVO ist auf Grund der Dokumentation i. R. d. Aufbewahrungsfristen sichergestellt.
Fehlkuvertierung (z. B. zwei Briefe mit Daten verschiedener Personen in einem Kuvert).	Dto.
Verarbeitung/Archivierung im falschen Kundenportalkonto.	Dto.
Fehlerhafte Daten in Schreiben.	Dto.
Falsche Kontoverbindung.	Dto.

Im Bereich von Vermögen und Bau Baden-Württemberg als nachgeordnete Stelle des Finanzministeriums:

Art des Vorfalls	Umgang
Offener E-Mail-Verteiler mit größtenteils personalisierten E-Mail-Adressen der Vertragspartner und deren Mitarbeitenden.	Hinweis auf Sorgfaltspflicht.

Im Bereich des Kultusministeriums:

Art des Vorfalls	Umgang
Im Jahr 2020 erhielt eine Prüfungsteilnehmerin von einem Seminar eine E-Mail, die nicht nur ihre eigene Themenstellung des Unterrichtsvorhabens zur Beurteilung der Unterrichtspraxis enthielt, sondern auch personenbezogene Daten und Prüfungszeiträume anderer Prüflinge.	Die Prüfungsteilnehmerin wurde aufgefordert, diese E-Mail zu löschen, die Prüfungszeiträume der anderen Prüflinge wurden verlegt. Das Seminar wurde zur Beachtung und Einhaltung der datenschutzrechtlichen Grundsätze aufgefordert.
Ebenso im Jahr 2020 wurden 12 Zeugnisurkunden über die Zweite Staatsprüfung von einer Außenstelle des Landeslehrerprüfungsamts zu einem Postdienstleister gegeben, um sie an ein Seminar zu befördern, bei dem sie jedoch nie angekommen sind.	Ein Nachforschungsantrag blieb erfolglos. Die Betroffenen wurden informiert. Ob sich ähnliche Vorfälle bei diesem Dienstleister häufen, wird beobachtet und ggf. ein Wechsel des Dienstleisters geprüft.
Im Jahr 2024 kam es im Rahmen des Transformationsprozesses Moodle zu einem Vorfall. Der Vorfall betraf einen Domainnamen, der vom Dienstleister des Kultusministeriums vor Nutzung nicht reserviert wurde. Im Anschluss an die Registrierung durch eine dritte Partei konnte eine einzige Mail durch die dritte Partei unrechtmäßig empfangen und gelesen werden. In dieser Mail waren keine personenbezogenen Daten Dritter enthalten.	Der betroffene Domainname wurde nach Bekanntwerden des Problems durch den Dienstleister geändert.

Im Bereich der Staatlichen Schulämter als nachgeordnete Stellen des Kultusministeriums:

Art des Vorfalls	Umgang
Virenbefall mit Emotet.	Anzeige des Vorfalles bei der Polizei und potenziell Betroffene wurden über die Homepage öffentlich informiert, da der Betroffenenkreis unklar war. Die Kriminalpolizei hatte den betroffenen Laptop untersucht, konnte allerdings keine Erfolg bringenden Informationen erlangen.

Im Bereich des Zentrums für Schulqualität und Lehrerbildung (ZSL) als nachgeordnete Stelle des Kultusministeriums:

Art des Vorfalls	Umgang
Im Oktober 2020 kam es zu einer behördeninternen Offenlegung von Geburtsdaten der Beschäftigten des ZSL per E-Mail an alle Beschäftigten im Zusammenhang der Vorbereitung einer Personalratswahl.	Es erfolgte ein unverzüglicher E-Mail-Rückruf.
Im März 2021 kam es zu einer nicht beabsichtigten Versendung einer E-Mail mit Anlage zu personenbezogenen Beschäftigtendaten an eine namensgleiche Person einer anderen Behörde anstelle des ZSL.	Es erging die Aufforderung zur Löschung gegenüber der anderen Behörde.
Im Juni 2021 wurden personenbezogene Daten (Name) einer im ZSL beschäftigten Person im Internet veröffentlicht mit der Folge der Abrufbarkeit über eine Internetsuchmaschine.	Es erfolgte eine Information an die betroffene Person sowie eine Löschung über den Anbieter der Internetsuchmaschine.
Im Dezember 2022 konnte auf personenbezogene Beschäftigtendaten anderer Dienststellen der Kultusverwaltung durch das Personalreferat des ZSL in einer Datenbank des LBV zugegriffen werden.	Die Zugriffsmöglichkeit auf personenbezogene Beschäftigtendaten anderer Dienststellen der Kultusverwaltung wurde technisch unterbunden, es erfolgte eine Aufklärung der Mitarbeitenden des Personalreferats, für die eine Möglichkeit des Zugriffs bestand.
Im November 2023 wurde ein fehlerhafter Weblink für ein Videokonferenz-Meeting an Teilnehmende einer Veranstaltung der amtlichen Lehrkräftefortbildung versandt, wodurch ein Webseite-Spoofing durch einen unberechtigten Dritten („Hacker“) ermöglicht wurde.	Es erfolgte die Unterrichtung aller Betroffenen, die den Vorfall verursachenden Personen wurden geschult. Auch wurden allen Beschäftigten des ZSL Handlungsempfehlungen zur datenschutzkonformen Anlage von Links für Webkonferenzen und der datenschutzkonformen Handhabung von Weblinks für Videokonferenz-Meetings gegeben.
Im November 2023 geschah eine versehentliche Offenlegung von E-Mail-Empfängern mit personenbezogenen E-Mail-Adressen durch Verwendung der Cc.- anstelle der Bcc.-Funktion.	Es erfolgte die Unterrichtung aller Betroffenen und die den Vorfall verursachende Person wurde erneut geschult.
Im Dezember 2023 kam es zu einer versehentlichen Offenlegung personenbezogener Daten (Name und Vereinbarung eines Termins) in Form einer Sprachnachricht auf dem Anrufbeantworter gegenüber unberechtigtem Dritten aufgrund falscher Rufnummerneingabe durch eine Person, die im ZSL beschäftigt ist.	Es erfolgte eine Information an die betroffene Person, die den Vorfall verursachende Person wurde erneut geschult.

Dem Wissenschaftsministerium sind keine Vorfälle gemeldet worden.

Im Bereich des Umweltministeriums:

Art des Vorfalls	Umgang
Mehrfach fehlerhaftes Versenden von E-Mails.	Sensibilisierungsmaßnahmen im Zuge der Schulung der Beschäftigten.
Daten von sicherheitsüberprüften Personen wurden nicht rechtzeitig gelöscht.	Ebenfalls Sensibilisierung der Beschäftigten.
Nutzung einer Software, bei der fälschlicherweise personenbezogene Daten sichtbar wurden.	Dies wurde sofort nach Entdeckung in engem Austausch mit dem LfDI behoben.

Im Bereich der Landesanstalt für Umwelt Baden-Württemberg als nachgeordnete Stelle des Umweltministeriums:

Art des Vorfalls	Umgang
Unerlaubter Zugriff auf einen GitLab-Server der Hochwasservorhersagezentrale (HVZ). Von wechselnden IP-Adressen wurde versucht, sich mit verschiedenen Nutzer/Passwort-Kombinationen auf dem Betriebssystem einzuloggen.	Der Server wurde unverzüglich nach Bekanntwerden des Cyberangriffs vom Netz genommen und ausgeschaltet, die zuständigen Beauftragten und Stellen sowie die Akteure des Länderübergreifenden Hochwasserportals wurden entsprechend informiert. Für die forensische Untersuchung wurde die Cybersicherheitsagentur hinzugezogen. Die ermittelten Daten wurden dem Landeskriminalamt übergeben.

Im Bereich des Wirtschaftsministeriums:

Art des Vorfalls	Umgang
Zwei Vorfälle bei einem Auftragsverarbeiter.	Die Auftragsverarbeiter haben die erforderlichen technischen und organisatorischen Maßnahmen getroffen.
Fünf Fälle betrafen einen nicht datenschutzkonformen E-Mail-Versand.	Um derartige Vorfälle in Zukunft zu vermeiden, wurden beispielsweise verpflichtende Schulungen für die Vorzimmerkräfte durchgeführt und die Problemfälle im Rahmen der regelmäßig stattfindenden Schulungen thematisiert. Darüber hinaus werden die Beschäftigten in regelmäßigen Abständen im Intranet unter der Rubrik „Aktuelles“ auf die datenschutzrechtlichen Grundsätze beim Versand von E-Mails hingewiesen. Darüber hinaus finden sich auf der Intranetseite des Wirtschaftsministeriums umfangreiche Informationen und Handreichungen zum Datenschutz.
In zwei Fällen kam es zu einer Offenlegung von personenbezogenen Daten an Personen, die dazu nicht berechtigt waren.	Dto.

Im Bereich des Sozialministeriums:

Verletzung einfacher personenbezogener Daten im Zusammenhang mit einer Rechnungszustellung an unzutreffende Adressaten.	• Fristgerechte Benachrichtigung der Betroffenen. Technische Maßnahme • Beseitigung des technischen Fehlers (SAP) unter Beteiligung LfDI, CERT, BITBW.
Unbekannter Verbleib einer Corona-Impfakte (Aufklärungsbogen, Anamnesebogen, Einwilligungserklärung) eines Bürgers, der in einem Impfzentrum während der Coronapandemie geimpft wurde.	• Fristgerechte Benachrichtigung des Betroffenen. Organisatorische Maßnahmen • Inaugenscheinnahme der sonstigen Impfakten des betroffenen Impfzentrums hinsichtlich ihrer ordnungsgemäßen Führung. • Durchführung von Prüffällen.
Versehentlicher Versand eines E-Mail-Verteilers mit ca. 50 Dienstadressen und Funktionspostfächern an einen Bürger.	Organisatorische Maßnahme • Anlassbezogener und regelmäßiger Hinweis auf bestehende Arbeitsanweisung zum Versand von E-Mails.
Umfrage im Zuge der Coronapandemie: Versehentliche Offenlegung von E-Mail-Adressen der Umfrageteilnehmer durch den Versand über „An.“ anstatt „Bcc.“ (Meldung Landratsamt Breisgau-Hochschwarzwald).	• Information Datenschutzbeauftragter Landratsamt Breisgau-Hochschwarzwald. • Versuch, die E-Mails zurückzurufen.
Unbemerkte und ungewollte Übertragung von privaten Bildern auf einen dienstlichen Account.	Technische Maßnahmen • Bilder aus der dienstlichen Cloud gelöscht. • Smartphones mit potenzieller Zugriffsmöglichkeit auf Datenaustausch identifiziert und abgemeldet. • Verwendung privater Apple-IDs auf dienstlichen Geräten untersagt und die Löschung privater Daten auf dienstlichen Geräten angeordnet. • Mittlerweile Umstellung auf gemanagte Geräte, damit automatisierte Übertragung privater Daten auf dienstliche Geräte nicht mehr möglich. Organisatorische Maßnahme • Referatsinterne Arbeitsanweisung erlassen, um einer Wiederholungsgefahr entgegenzuwirken.

Einrichtungsbezogene Impfpflicht § 20a Infektionsschutzgesetz a. F.: Für Meldungen aufgrund von § 20a Infektionsschutzgesetz a. F. wurde vom Land eine systemische Anwendung erstellt. Dabei wurde für den Zeitraum vom 16. bis 18. März 2022 versehentlich ein falscher Adressat für die Meldungen hinterlegt. Anstatt an das Gesundheitsamt der Stadt Heilbronn gingen die Meldungen an das Gesundheitsamt des Landkreises Heilbronn.	Technische Maßnahme • Der Fehler wurde am 18.3.2022, 17:00 Uhr, durch Einspielen eines Fix beim Systembetreiber behoben. Organisatorische Maßnahme • Mit dem Landratsamt Heilbronn wurde die Weiterleitung der Daten an die Stadt abgewickelt.
Versehentlicher Versand des Entwurfes eines Vorstandsdienstvertrages an den falschen Adressaten. Anstatt an die Kassenzahnärztliche Vereinigung wurde der Entwurf an die Kassenärztliche Vereinigung übermittelt.	Organisatorische Maßnahme • Daten wurden auf Mitteilung des Sozialministeriums beim falschen Adressaten umgehend gelöscht.
Versehentlicher Versand einer E-Mail-Einladung zu einer Veranstaltung im Oktober 2022 über einen offenen Verteiler.	Organisatorische Maßnahme • Unterrichtung der Betroffenen am selben Tag.

Im Bereich des Justizministeriums:

Art des Vorfalls	Umgang
Auslage einer Teilnehmerliste bei der Zweiten juristischen Prüfung und Befestigung des Rubrums und Tenors aus einem Nachteilsausgleichsverfahren am Tisch der Prüfungsaufsicht.	Information aller Außenstellen des Landesjustizprüfungsamts über den Umgang mit derartigen personenbezogenen Daten; Verzicht auf Übersendung von Rubrum und Tenor von Gerichtsverfahren an Außenstellen.
Im Bereich des IuK-Fachzentrum Justiz (Meldung erfolgte vorsorglich durch das Justizministerium): Ransomware-Angriff auf Auftragsverarbeiter/Softwareentwickler eines Fachverfahrens, wobei ein Datenbestand mit Testdaten verschlüsselt wurde.	Verbot der Datennutzung an den betroffenen Entwickler.
Fehlerhafte Zuordnungen von bestimmten Dateien im Akteneinsichtsportal, sodass in vier Fällen für Rechtsanwälte/Sachverständige eine falsche Akte abrufbar war.	Löschaufforderung an falsche Empfänger; technische Fehlerbehebung.
Versehentliche Weiterleitung einer internen E-Mail an externen Empfänger.	Löschaufforderung an den falschen Empfänger.
Fehlende Verfügbarkeit und falsche Zuordnung personenbezogener Daten in der eAkte-Software.	Soweit möglich Wiederherstellung fälschlich gelöschter Dateien; technische Fehlerbehebung.

Versand einer E-Mail an den falschen Empfänger (Gericht).	Bestätigte Löschung der E-Mail durch das fehladressierte Gericht.
Versand eines Schreibens möglicherweise in unverschlossenem Umschlag.	Sensibilisierung der Versandstelle.
Versand eines internen Vermerks an externen Empfänger.	Bestätigte Löschung durch falschen Empfänger, zudem Belehrung über Verschwiegenheitspflicht.
Fehlerhafte Administration eines Verzeichnisdienstes, was dazu führte, dass Bürgerpostfächer bei „Mein-Justizpostfach“ öffentlich auffindbar waren.	Technische Fehlerbehebung; erneute Sensibilisierung der zuständigen Administratoren.

Im Bereich des Verkehrsministeriums:

Art des Vorfalls	Umgang
Fälschliche Berechtigung einzelner Accounts des Umweltministeriums auf Postfächer des Verkehrsministerium mit lesendem Zugriff landesverwaltungsintern.	Aufklärung erfolgte durch Unterstützung der BITBW und des Umweltministeriums.

Im Bereich des Ministeriums für Landesentwicklung und Wohnen:

Art des Vorfalls	Umgang
Seit der Neugründung des Ministeriums für Landesentwicklung und Wohnen im Jahr 2021 gab es vier Verletzungen des Schutzes personenbezogener Daten. Hierbei wurden personenbezogene Daten offengelegt, insbesondere E-Mail-Adressen durch den Versand von E-Mails mit einem offenen Verteiler.	Es wurden umgehend Gegenmaßnahmen (z. B. Bitte um Löschung der E-Mail und Neuversand in „Bcc.“) ergriffen und die Mitarbeitenden nachgeschult und sensibilisiert.

Im Bereich des Regierungspräsidiums Freiburg (RPF):

Art des Vorfalls	Umgang
Im August 2022 wurde ein falscher Schülername genannt.	Nach Rücksprache mit dem behördlichen Datenschutzbeauftragten wurde der Name in allen Unterlagen geschwärzt.
Im Oktober 2022 gab es eine Personenverwechslung (falsche Eingabe durch RPF) im Personalverwaltungsprogramm DIPSY wegen Namensgleichheit. Es wurden Beschäftigtendaten, Adressdaten und Bezüge durch das LBV auf Grundlage der Eintragung in DIPSY an eine falsche Empfängerin verschickt.	Es wurden eine Korrektur im Personalverwaltungssystem vorgenommen, ein Entschuldigungsschreiben an die falsche Empfängerin verfasst und die Mitarbeitenden weiter sensibilisiert.
Im Dezember 2021 wurden bei einem Cyberangriff schädliche Links über E-Mail-Server der RPF-Außenstellen versendet.	Die Server wurden unverzüglich vom Netz genommen. Ferner wurden über die Außenstellen Benachrichtigungsschreiben an alle Betroffenen versendet.
Im August 2022 wurde bei einer internen Weiterleitung einer dienstlichen E-Mail im Homeoffice an zuständige Kollegen eine unbekannte Empfängerin (Dienstsitz Finanzamt) versehentlich in „Cc.“ über das Adressbuch eingefügt, für die die E-Mail nicht bestimmt war. Betroffen waren Firmennamen und Kontaktdaten von Kollegen.	Es erfolgte eine Kontaktaufnahme mit der falschen Empfängerin mit der Bitte um Vertraulichkeit und Löschung der E-Mail. Von einer Benachrichtigung der betroffenen Personen wurde nach Risikoabwägung/-prognose abgesehen.
Im Februar 2024 hat ein Streetworker bei der aufsuchenden Arbeit eine Liste mit ca. 60 Bewohnernamen von Bewohnern der Landeserstaufnahmeeinrichtung auf dem Gelände der Landeserstaufnahmeeinrichtung verloren. Davon betroffen waren Namen, Herkunft, Geburtsdatum und Zimmernummern.	Die Liste konnte nicht mehr rekonstruiert werden, da sie unmittelbar überschrieben wurde.

Im nachgeordneten Bereich des Regierungspräsidiums Freiburg:

Art des Vorfalls	Umgang
Ein Vorfall bei einem externen Dienstleister, es gab einen Cyberangriff.	Die Panne wurde dem Betroffenen gemeldet. Weitere Maßnahmen mussten nicht ergriffen werden.
Zwei Mal wurde ein Brief an die falsche Person verschickt.	Die Panne wurde dem Betroffenen gemeldet. Weitere Maßnahmen mussten nicht ergriffen werden.
April 2021: Gemeldete Vorfälle im Kreisimpfzentrum in Müllheim. Das Landratsamt war als Auftragsverarbeiter für das Sozialministerium tätig. An eine große Anzahl gespeicherter E-Mail-Empfänger ist eine E-Mail versandt worden, welche zur Teilnahme an einer anonymen Online-Befragung eingeladen hatte. Die Versendung erfolgte durch einen Mitarbeiter versehentlich in der Weise, dass E-Mail-Verteiler in das falsche Versende-Feld des E-Mail-Programmes eingefügt worden und deshalb jedem Empfänger zwischen 800 und 850 fremde E-Mail-Adressen offengelegt worden sind. In Verbindung mit der E-Mail-Adresse ist in vielen Fällen ein Rückschluss auf eine erhaltene Impfung einer betroffenen Person möglich geworden.	Es erfolgte eine Benachrichtigung gem. Artikel 34 DSGVO durch Veröffentlichung auf der Homepage und eine Entschuldigung, bei Versendung von E-Mails in großem Umfang, wird künftig das Vier-Augen-Prinzip angewandt.
Personenbezogene Daten wurden an den falschen Empfänger geschickt.	
Eine Schließungsverfügung wurde dem falschen Empfänger übermittelt.	
Im Bereich des Gesundheitsamts erfolgte ein Datenschutzverstoß im Rahmen der Kuvertierung eines Anschreibens mit Datum 2.3.2020 an einen Bürger. Im Sichtfenster des verschlossenen Kuverts war neben der Anschrift des Betroffenen auch der Text „Kontrollprogramm auf Drogen“ ersichtlich. Der Verstoß wurde mit Schreiben vom 7.4.2020 vom Rechtsanwalt des Betroffenen bekannt.	Da der Zeilenabstand zwischen Adressfeld und Betreff im betreffenden Formular falsch eingestellt war, soll als Abhilfemaßnahme das entsprechende Formular umgestaltet werden.

Im Bereich der Führerscheinstelle wurde der Link für die e-Akte eines Betroffenen an einen Dritten (ebenfalls Kunde der Führerscheinstelle) versehentlich übermittelt. Dieser hat den Link an seinen Psychologen weitergeleitet, ohne ihn vorher geöffnet zu haben. Der Psychologe hat den Fehler am falschen Namen sofort erkannt, die Akte geschlossen und den Dritten informiert, dieser wiederum informierte die Führerscheinstelle.	Beide Personen wurden aufgefordert den Link sofort zu löschen. Dies wurde auch entsprechend bestätigt. Es handelte sich um einen Flüchtigkeitsfehler, die Mitarbeiterin wurde nochmals datenschutzrechtlich belehrt.
Im Bereich des Gesundheitsamts beantragte eine ehemals im Jahr 2002 vom Gesundheitsamt untersuchte Person am 10.12.2021 Datenauskunft über beim Gesundheitsamt gespeicherte Unterlagen seit dem Jahr 2002. Am 14.12.2021 wurde im Gesundheitsamt festgestellt, dass die entsprechende Akte bereits vernichtet worden war, trotz Aufbewahrungsfrist von 10 Jahren. Es wurde festgestellt, dass die Akten (Dokumente/Berichte) im Schreibdienst ohne sachgemäße Beachtung der Aufbewahrungsfrist gelöscht worden sind.	Der betroffenen Person wurde mitgeteilt, dass die Akten zwar gelöscht wurden, aber noch wenige digitale Daten bei einer Recherche gefunden wurden. Der Person wurde Möglichkeit gegeben, die Daten bis zum 31.1.2022 einzusehen, im Anschluss waren auch diese Daten vollständig zu löschen.
Im Bereich des Vermessungsamts wurde am 9.8.2023 im Flurneuordnungs- und Vermessungsamt versehentlich ein falscher Anhang per E-Mail an einen Dritten übersandt. In dem versehentlich übermittelten Anhang befanden sich Eigentümerdaten zu Flurstücken in großem Umfang.	Der Vorfall wurde am 10.8.2023 durch Zuruf des Empfängers der E-Mail bekannt. Die übermittelten Daten waren 1,5 Jahre alt und eigneten sich nicht für einen Missbrauch. Außerdem hatte der versehentliche Empfänger die unmittelbare Löschung der Daten zugesichert. Daher wurde das Vorliegen eines hohen Risikos für die persönlichen Rechte und Freiheiten natürlicher Personen ausgeschlossen. Als Abhilfemaßnahme werden Anlagen künftig vor Versand doppelt gecheckt und wurde im Fachbereich auch erneut bezüglich der Verwendung gesicherter Datenübertragung hingewiesen (zudem war dies auch Teil der Datenschutzsensibilisierungen bei allen Führungskräften und Mitarbeitenden im Landratsamt).

Innerhalb der Hauspost des Landratsamts ging ein USB-Stick mit personenbezogenen Daten verloren.	Es erfolgten Sensibilisierungen der Mitarbeitenden und es dürfen nur noch verschlüsselte USB-Sticks verwendet werden.
Verlust eines ausgefüllten Meldebogens im Rahmen der Bevölkerungszählung Zensus.	Betroffene Familie wurde informiert und um Entschuldigung gebeten.
Beim Versenden von Serienbriefen wurden versehentlich zwei Anschreiben in einem Kuvert versandt. Hierdurch erlangte eine unberechtigte Person Kenntnis von Vorname, Name und Adresse einer Kindesmutter sowie Vorname und Geburtsdatum eines Kindes.	Die Betroffene wurde telefonisch und schriftlich um Entschuldigung gebeten.
Über das öffentliche Internet wurde über den Browser mittels ArcGIS-Server-Karten-Diensten, die für das Kreis-GIS notwendig sind, über Entwicklertools und durch Ausprobieren von Ingenieurbüros unbefugt Zugang zu personenbezogenen Daten beim Landratsamt Emmendingen erlangt. Die Daten wurden nur angezeigt, nicht heruntergeladen.	Umgehend wurden alle Karten-Dienste vorläufig gestoppt. Alle betreffenden ArcGIS-Server-Karten-Dienste wurden einen Tag später mit Benutzer und Passwort geschützt (Authentifizierung). Zusätzlich wurde das Listing abgestellt. Für andere externe Stellen mit Zugriff wurde vorübergehend ein eingeschränktes Projekt realisiert. Externe Sicherheitseinschätzung und Beratung wurde beim Informationssicherheitsbeauftragten des Landratsamtes eingeholt. Die Empfehlungen (Passwortablauf nach 90 Tagen, Optimierung Workflow u. a.) wurden umgehend umgesetzt. Die Nutzungsvereinbarung mit externen Stellen wurde überarbeitet und konkretisiert. Alles erfolgte sehr zeitnah.
Persönliche Daten einer Person in Verbindung mit der Information „Corona-Test positiv“ wurden versehentlich an einen ehemaligen Corona-Teststellenbetreiber weitergeleitet.	Es erfolgte eine Sensibilisierung der Mitarbeitenden. Zudem wurden die internen Abläufe optimiert.
Im Zeitraum März 2019 bis Februar 2024 wurden im Bereich der unteren Verwaltungsbehörde insgesamt 20 Vorfälle an den LfDI gemeldet. Diese teilten sich wie folgt auf die Abteilungen des Landratsamtes auf: - Gesundheit 4 - Veterinärwesen 1 - Kfz-Zulassung 6 - Fahrerlaubnisse 7 - Vermessung 1 - Bodenschutz 1	Darauf wurde die Kuvertiermaschine gewartet und wurden Hinweise für deren Benutzung erlassen.

Diese Pannen beruhten zum weit überwiegenden Teil auf dem Falschversand von einzelnen Schreiben bzw. E-Mails; bspw. wurden Schreiben an verschiedene Empfänger in denselben Umschlag kuvertiert. Außerdem kommt es vor, dass E-Mails versehentlich an eine Person mit demselben Namensanfang versandt werden, der vom E-Mailprogramm dann falsch vervollständigt wird. Vereinzelt haben Kolleginnen und Kollegen ein Schreiben aus einer Altakte verwendet, ohne das Adressfeld zu aktualisieren, oder versehentlich aktiv den falschen Adressaten eingetragen.	Die Mitarbeitenden haben eine Anleitung an die Hand bekommen, wie sie die automatische Adressvervollständigung abstellen können.
Einbruch in die Räumlichkeiten der Kfz-Zulassungsstelle.	
Im Januar 2024 wurde der Vermessungsbehörde und Bodenschutzbehörde seitens des LfDI über eine Zugriffsmöglichkeit auf Datenbestände mitgeteilt, die sich als unbeabsichtigt herausgestellt hat.	Die Zugriffsmöglichkeiten wurden geschlossen und die Betroffenen im Wege einer öffentlichen Mitteilung informiert.

Im Bereich des Regierungspräsidiums Karlsruhe:

Art des Vorfalls	Umgang
Ein Fall, in dem der dienstliche Telefonanschluss einer Mitarbeiterin des Regierungspräsidiums durch eine Kollegin versehentlich nicht auf die Erreichbarkeit der im Home-Office arbeitenden Mitarbeiterin umgeleitet wurde, sondern auf die auf dem dienstlichen Telefon als letzten Kontakt angegebene Rufnummer einer nicht beim Regierungspräsidium beschäftigten Bürgerin. Diese erhielt dadurch für das Regierungspräsidium bestimmte Anrufe; personenbezogene Daten der Anrufer wurden auf der Mailbox gespeichert.	Nach Entdeckung des Fehlers wurde das Telefon korrekt umgestellt. Die zuständigen Mitarbeitenden wurden angehalten, bei Telefonumleitungen künftig sorgfältiger vorzugehen.

Ein Fall, in dem einem Rechtsanwalt im Rahmen einer Akteneinsicht personenbezogene Daten Dritter zugänglich gemacht wurden, die geschwärzt werden sollten, aber aufgrund einer versehentlich fehlerhaften Bedienung der elektronischen Akte durch die zuständige Mitarbeiterin in dem dem Anwalt zugänglich gemachten Dokument ungeschwärzt erschienen.	Der Anwalt wurde aufgefordert, die Daten zu löschen und hat dies zugesagt. Die zuständigen Mitarbeitenden wurden auf das korrekte Vorgehen beim Schwärzen elektronischer Aktenbestandteile hingewiesen. Die von dem Vorfall Betroffenen wurden schriftlich benachrichtigt.
Zwei Fälle, in denen Anfragen bzgl. anderweitiger Beschäftigungsmöglichkeit einer Lehrkraft innerhalb der Landesverwaltung nicht wie sonst üblich und aus Gründen der Datensparsamkeit erforderlich zunächst pseudonymisiert, sondern unter Nennung des Namens der jeweils betroffenen Lehrkraft, ihrer Kontaktdaten und ihrer gesundheitlichen Einschränkungen an andere Landesbehörden gerichtet wurden.	Die betroffenen Lehrkräfte wurden nach Artikel 34 DSGVO benachrichtigt. Die Landesbehörden, an die die Daten übermittelt wurden, wurden gebeten, diese zu löschen. Anschließend wurden die Anfragen nochmals pseudonymisiert gestellt. Die zuständigen Mitarbeitenden wurden für das korrekte Vorgehen sensibilisiert.
Ein Fall, in dem vom Regierungspräsidium versehentlich nicht nur der Antrag einer Lehrkraft auf Wiederaufnahme des Dienstes an die Schulleitung gesendet wurde, sondern auch ärztliche Atteste, deren Kenntnis für die Schulleitung nicht erforderlich war.	Die unberechtigt an die Schulleitung gesandten Daten wurden dort vollständig gelöscht. Dies wurde der betroffenen Lehrkraft mitgeteilt.

Im Bereich des Regierungspräsidiums Stuttgart:

Art des Vorfalls	Umgang
Versand einer E-Mail mit personenbezogenen Daten enthaltenden Unterlagen an einen falschen Empfänger.	Es erfolgte ein unmittelbarer Rückruf der E-Mail. Im Nachgang konnte festgestellt werden, dass der Dritte die versehentlich an ihn gesendeten Unterlagen in dem kurzen Zeitraum der Zugriffsmöglichkeit nicht gesichtet hat.
Versand einer E-Mail mit personenbezogenen Daten an eine falsche Empfängerin innerhalb des Landesverwaltungsnetzes.	Die einzig betroffene Person wurde über den Vorfall informiert, die fehlerhafte Empfängerin informiert. Das Referat hat sich die Löschung zusichern lassen und mit der Mitarbeiterin (Versenderin) den Vorfall besprochen.
Im Rahmen der Erweiterung eines Wikipedia-Artikels wurden Details eingetragen, welche internes Behördenwissen darstellen.	Der Mitarbeiter wurde für die Belange des Datenschutzes sensibilisiert.

Im nachgeordneten Bereich des Regierungspräsidiums Stuttgart:

Art des Vorfalls	Umgang
Es wurden Personen in „Cc.“ in den Adressverteiler genommen, die nicht in den Verteiler gehört hätten.	Die Mitarbeitenden wurden insgesamt für datenschutzrelevante Themen sensibilisiert.
Es wurde eine Diagnose eines Arbeitnehmers gegenüber einem externen Arbeitgeber offengelegt.	Technisch wurden alle Vorfälle bzw. Lücken beseitigt und die Mitarbeitenden insgesamt für datenschutzrelevante Themen sensibilisiert.
Ransomeware Angriff.	Es wurde das Passwort geändert, der externe Zugriff auf E-Mails über OWA wurde abgeschaltet. Es erfolgte eine Sensibilisierung der Mitarbeitenden, ein externer Check, Proxy, Test Phishing Mails und es wurde Strafanzeige gestellt.
Versendung Führerschein an falsche Adressaten.	Die Mitarbeitenden wurden insgesamt für datenschutzrelevante Themen sensibilisiert.
Phishingangriff auf Passwörter.	Es wurde ein Warnhinweis für externe E-Mail Adressen angebracht.
Kundendaten wurden durch eine Terminvereinbarungssoftware veröffentlicht.	Technisch wurden alle Vorfälle bzw. Lücken beseitigt und die Mitarbeitenden insgesamt für datenschutzrelevante Themen sensibilisiert.
Gehaltsabrechnungen von Mitarbeitenden wurden offengelegt.	Technisch wurden alle Vorfälle bzw. Lücken beseitigt und die Mitarbeitenden insgesamt für datenschutzrelevante Themen sensibilisiert.
Fehlversand von Informationen.	Technisch wurden alle Vorfälle bzw. Lücken beseitigt und die Mitarbeitenden insgesamt für datenschutzrelevante Themen sensibilisiert.
E-Mail-Weiterleitung unter Offenlegung der E-Mail-Adresse und des Namens der sich beschwerenden Person.	Die Mitarbeitenden wurden insgesamt für datenschutzrelevante Themen sensibilisiert.
Versehentliche Herausgabe von personenbezogenen Daten an unbeteiligte Dritte bei Bußgeldbescheiden.	Die Betroffenen wurden informiert, die Daten zurückgefordert, die Löschung etwaiger Kopien wurde gefordert und der Vorfall wurde gemeldet.
Angriff auf Citrix-Infrastruktur, Netscaler-Angriff über Sicherheitslücke CVE-2019-19781. Die Entdeckung eines entsprechenden Exploits auf dem Netscaler Server erfolgte	Abschaltung der Netscaler, Rekonstruktion der Netscaler über nicht kompromittierte Datensicherung, Rücksetzung der Passwörter der betroffenen Citrix-Benutzer sowie der

Art des Vorfalls	Umgang
über eine Prüfroutine durch einen externen Dienstleister. Ursache war eine Sicherheitslücke CVE-2019-19781.	Admins, Scan der gesamten Citrix-Infrastruktur auf Schadsoftware.
Einige Edupool-Accountdaten (E-Mails und Passworthashes, in wenigen Fällen auch Passwörter) wurden abgegriffen. Weitere Daten wurden nicht abgegriffen.	In der der Folge wurden vom Software-Hersteller Maßnahmen ergriffen. Es fand ein Umzug des Servers statt und ferner wurden die Betroffenen angeschrieben und deren Passwörter zurückgesetzt.
Verlust dienstlicher Unterlagen.	Personalgespräche mit den jeweiligen Mitarbeitenden.
Fehlversand von Gesundheitsdaten.	Vernichtung der fehlversendeten Unterlagen und Personalgespräche mit den jeweiligen Mitarbeitenden.
Untergang von versendeten Akten während des Postversandes.	Personalgespräche mit den jeweiligen Mitarbeitenden.
Fehlversand einer Rundmail. Alle Mail-Adressen der Erhebungsbeauftragten wurden statt im Feld „Bcc.“ im Feld „An.“ eingetragen. Ein Rückruf der E-Mail war nicht mehr möglich.	
Angriff auf den Server eines Anbieters einer Verleihsoftware, Accountdaten wie etwa E-Mails und Passwörter von registrierten Nutzern (z. B. Lehrkräfte und andere Medienzentren) wurden abgegriffen. Laut dem Softwareanbieter sind die Daten höchstwahrscheinlich unbrauchbar und für einen Login im System nicht brauchbar.	Die betroffenen Kunden und Kundinnen wurden direkt vom Anbieter über das Datenleck informiert und dabei die Passwörter zurückgesetzt.
In zwei Angelegenheiten erfolgte ein Fehlversand einer E-Mail (Verteiler offen statt „Bcc.“).	Nachschulung der Mitarbeitenden.
In fünf Angelegenheiten erfolgte ein Fehlversand eines Briefes an den falschen Empfänger (Kuvertierfehler).	Nachschulung der Mitarbeitenden, Rückholung der fehlversandten Unterlagen.
Programmierfehler im EDV-Programm.	Fehlerbehebung durch den Anbieter.
Aufdruck Kfz-Kennzeichen und persönlicher Angaben auf von Kfz-Behörde versandtem Umschlag zu einer Postzustellungsurkunde.	Anweisung an Rechenzentrum, automatischen Eindruck entsprechend zu ändern; Antwort an den Eingebenden.
Unbefugte Offenlegung einer Betroffenheit durch Erzählung im Bekanntenkreis.	Belehrung des Mitarbeitenden, Gespräch mit dem Betroffenen.

Art des Vorfalls	Umgang
Es erfolgte ein Versand einer E-Mail an mehrere Kunden mit Mailadressen in „An.“ statt „Bcc.“.	Belehrung der Mitarbeitenden; Information der anzeigenden Person aus dem Verteiler.
Versand eines Mailverteilers mit ca. 550 Adressaten über „An.“ statt „Bcc.“.	Belehrung der Mitarbeitenden; Information der Betroffenen über Intranet/Homepage.
Gesundheitsdaten in Terminvereinbarungstool COSAN für Corona-Tests waren für Bürgerinnen und Bürger über Suchmaschinen auffindbar.	Anpassung der robot.txt; Information der Betroffenen.
Verlust eines Datenträgers (SD-Karte).	Nochmalige Sensibilisierung der Mitarbeitenden.
Mitteilung von E-Mail-Adressen an unberechtigte Personen durch Missachtung der Verwendung von „Bcc.“.	Sensibilisierung der Mitarbeitenden.
Sicherheitsleck im Rahmen einer Distributionsplattform für Medien.	Sensibilisierung der Mitarbeitenden.
Mitteilung der Zugangsdaten zu digitalem Anhörungsbogen im Brieffenster durch unsachgemäßes Falten des Briefes.	Sensibilisierung der Mitarbeitenden.
Offenlegung eines Vergleichs in einer Unterhaltssache gegenüber unberechtigten Personen.	Sensibilisierung der Mitarbeitenden.
Virenfund (2019).	Einsatz von Trendmicro Office Scan, Pflege von Spamfilterlisten, weitere TOM’S, Warnung an Mitarbeitende inkl. Anweisungen, Info über Homepage und Kreiszeitung.
Es wurden personenbezogene Daten in einem offenem Papiercontainer vor der Außenstelle festgestellt (2021).	Der Container wurde sichergestellt und professionell entsorgt. Die Ursache war nicht mehr feststellbar. Es erfolgte eine Überprüfung der internen Vorgänge und Sensibilisierung der Mitarbeitenden, den Papiermüll nur datenschutzkonform zu entsorgen.
Möglicher Versuch einer Infiltration (2023).	Einziehung der dienstlichen Endgeräte der Mitarbeiterin und weitere Überwachung der IT-Vorgänge. Sensibilisierung der Mitarbeitenden.
Cyberattacke Bitlocker Malware (2023).	Sämtliche externe Anbindungen wurden unterbrochen, Cybersecurity BW wurde um Unterstützung gebeten, ebenso das kommunale Rechenzentrum Komm.One. Überprüfung interner Vorgänge und Sensibilisierung der Mitarbeitenden.

Im Bereich des Regierungspräsidiums Tübingen:

Art des Vorfalls	Umgang
Es kam zu einer falschen Entsorgung von datenschutzrelevanten Dokumenten/Inhalten von Lehrkräften aus dem Regierungsbezirk.	Die Behandlung des Vorfalls erfolgte im Rahmen der Prozesse des Datenschutz- und Informationssicherheitsmanagementsystems.
Durch eine Programmfehlbedienung des Bewerbungs- und Einstellungsverfahrens für alle Lehrkräfte in Baden-Württemberg – Online-Verfahren „LEIN“ – waren Daten von Bewerberinnen und Bewerbern im Hauptausschreibungsverfahren für die Gymnasien kurzfristig sichtbar.	Die Behandlung des Vorfalls erfolgte im Rahmen der Prozesse des Datenschutz- und Informationssicherheitsmanagementsystems.
Versand dreier verschiedener Bescheide in unterschiedlichen Verfahren an den falschen Adressaten.	Die Behandlung des Vorfalls erfolgte im Rahmen der Prozesse des Datenschutz- und Informationssicherheitsmanagementsystems.

6. Welche Untersuchungsbefugnisse (Artikel 58 Absatz 1 Datenschutz-Grundverordnung [DSGVO]), welche Abhilfebefugnisse, insbesondere Bußgeldverhängungen (Artikel 58 Absatz 2 in Verbindung mit Artikel 83 DSGVO), welche Beratungs- und Kontrollbefugnisse (Artikel 58 Absatz 3 DSGVO) wurden in den letzten fünf Jahren infolge der festgestellten Rechtswidrigkeit vom LfDI bzw. seiner Behörde gegenüber den Ministerien ausgeübt (bitte unter Darstellung jedes Buchstabens der genannten Vorschriften und getrennt für jedes Ministerium)?

Zu 6.:

Zur Beantwortung der Frage wird auf die Landtagsdrucksache 17/4960 verwiesen. Da im Übrigen keine datenschutzrechtlichen Verstöße festgestellt wurden, erübrigen sich weitere Ausführungen.

7. Welche Reaktionen auf die festgestellte Rechtswidrigkeit waren im internen Bereich der Ministerien in den letzten fünf Jahren festzustellen (bitte aufgeschlüsselt nach disziplinarischen, organisatorischen und sonstigen [zu benennenden] Maßnahmen)?

8. Inwieweit bewertet sie diesen internen Umgang der Ministerien mit datenschutzrechtlichen Verstößen in den letzten fünf Jahren als ausreichend im Sinne der hohen Bedeutung des Datenschutzes?

Zu 7. und 8.:

Die Fragen 7 und 8 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Die Landesregierung nimmt den Schutz personenbezogener Daten ernst und nimmt Datenschutzverletzungen stets zum Anlass einer kritischen Prüfung.

Wie dargestellt handelt es sich bei den festgestellten Verstößen um Einzelfälle. Soweit notwendig, ist eine Sensibilisierung der Mitarbeitenden erfolgt.

9. Wie beurteilt sie die Zusammenarbeit der Ministerien mit dem LfDI bzw. seiner Behörde in den letzten fünf Jahren (insbesondere unter Berücksichtigung eines [nicht] transparenten Verhaltens der Ministerien im Falle eines datenschutzrechtlichen Verstoßes und unter Bewertung der Annahme von Angeboten des LfDI in Bezug auf mögliche Beratungen)?

Zu 9.:

Für alle Ressorts kann mitgeteilt werden, dass mit dem LfDI eine vertrauensvolle Zusammenarbeit besteht. Der LfDI wird regelmäßig bei datenschutzrechtlichen Fragestellungen eingebunden, um datenschutzrechtliche Probleme beispielsweise im Rahmen der Regelungserstellung bereits im Vorfeld lösen zu können. Zudem stehen die behördlichen Datenschutzbeauftragte der Ressorts und der Regierungspräsidien im Rahmen eines Arbeitskreises zweimal jährlich mit dem LfDI im direkten Austausch. Auch Schulungen und das Informationsangebot des LfDI werden gerne genutzt.

10. Inwiefern wurden die organisatorischen und technischen Bereiche der Ministerien in den letzten fünf Jahren weiterentwickelt, um den stets gewichtiger werdenden datenschutzrechtlichen Vorgaben gerecht zu werden und den Datenschutz im Allgemeinen umfassend zu gewährleisten?

Zu 10.:

Im Geschäftsbereich des Staatsministeriums werden im Hinblick auf die Onlinekommunikation kontinuierlich Maßnahmen getroffen, die sicherstellen, dass die Vorschriften über den Schutz der personenbezogenen Daten beachtet werden. In den letzten fünf Jahren wurde der den Webseiten der Ministerien zugrundeliegende Typo3-Baukasten stetig weiterentwickelt, um den zunehmenden datenschutzrechtlichen Vorgaben gerecht zu werden und eine umfassende Gewährleistung des Datenschutzes im Allgemeinen zu ermöglichen. Dazu gehören unter anderem beispielsweise die Umsetzung eines datenschutzkonformen Cookie-Banners auf den Webseiten sowie die datenschutzkonforme Einbindung externer Plattformen wie YouTube. Zudem wurde die Kartenfunktion verbessert, indem „Google Maps“ durch „Open Street Map“ ersetzt wurde. Dadurch wird die Verarbeitung von Standortdaten transparenter und datenschutzfreundlicher gestaltet. Außerdem wurde eine „Social Wall“ eingerichtet, wodurch eine datenschutzkonforme Darstellung von Social-Media-Inhalten auf den Webseiten der Ministerien gewährleistet ist. Die Maßnahmen tragen dazu bei, die Privatsphäre der Nutzer besser zu schützen und die Anforderungen an einen verantwortungsvollen Umgang mit personenbezogenen Informationen zu erfüllen. Alle sich auf das Onlineangebot bezogenen Maßnahmen finden sich in der Datenschutzerklärung, welche über folgenden Link dauerhaft transparent abrufbar ist: *https://www.baden-wuerttemberg.de/de/header-und-footer/datenschutz/*.

Der Datenschutz nimmt traditionell und weiter verstärkt seit der Geltung der DSGVO eine sehr gewichtige Rolle im Arbeitsalltag des Innenministeriums ein. Die Einhaltung der jeweils spezifisch zu berücksichtigenden datenschutzrechtlichen Vorgaben wird bei allen Aufgaben und Projekten geprüft und sichergestellt; neue Mitarbeitende werden bei der Einweisung in die Aufgaben auch auf Regelungen zur Sicherstellung des Datenschutzes hingewiesen. Im Innenministerium wurde eine Regelung zum Verzeichnis von Verarbeitungstätigkeiten auf der Grundlage der DSGVO eingeführt, des Weiteren eine Regelung zur Meldung von Verletzungen des Schutzes von personenbezogenen Daten erlassen. Darüber hinaus gibt es eine Regelung zu den Informationspflichten gegenüber Bürgerinnen und Bürgern nach Artikel 13 und 14 DSGVO. Für die Mitarbeitenden des Ministeriums wurden Informationsveranstaltungen zur Sensibilisierung und zur Stärkung des Rechtsschutzes von Bürgerinnen und Bürgern durchgeführt. Der behördliche Datenschutzbeauftragte steht mindestens zweimal jährlich im Rahmen eines Arbeitskreises mit dem LfDI im Austausch.

Da das Finanzministerium den Schutz der personenbezogenen Daten sehr ernst nahm und nimmt, wurden im Zuge des Inkrafttretens der DSGVO die bisheri-

gen Hinweise zur Einhaltung der datenschutzrechtlichen Vorgaben aktualisiert und weiterentwickelt. Die Beschäftigten des Finanzministeriums werden unter anderem mittels Informationen im Intranet und einer spezifischen Handlungshilfe zur Wahrnehmung der Aufgaben des Datenschutzes entsprechend sensibilisiert. In dieser Handlungshilfe werden insbesondere die Festlegungen zur Zusammenarbeit zwischen den Beschäftigten des Finanzministeriums und den Datenschutzbeauftragten geregelt.

Das Kultusministerium legt großen Wert auf die Einhaltung der datenschutzrechtlichen Vorgaben und misst dem Datenschutz eine hohe Bedeutung zu. Das Ministerium beteiligt den LfDI rechtzeitig bei der Ausarbeitung von Rechts- und Verwaltungsvorschriften, die die Verarbeitung personenbezogener Daten betreffen. Zudem steht der behördliche Datenschutzbeauftragte des Kultusministeriums im Rahmen eines Arbeitskreises mindestens zweimal jährlich mit dem LfDI im Austausch.

Im Jahr 2019 wurden insgesamt 25 neue Stellen für behördliche Datenschutzbeauftragte geschaffen. Vier Stellen hiervon sind bei den Regierungspräsidien, 21 bei den staatlichen Schulämtern verankert. Dadurch werden Schulen entlastet und die Aufgabe kann gebündelt werden. Eine weitere Stelle ist beim ZSL verortet.

Die Schulverwaltung wurde und wird regelmäßig über die üblichen Kommunikationswege (Infodienst Schulleitung, einschlägige Informationsplattformen) über die DSGVO informiert. Auf *www.it.kultus-bw.de* und im Intranet der Kultusverwaltung stehen umfangreiche zielgruppenorientierte Handlungsanleitungen, Informationen, Hinweise, FAQs, Vorlagen, Formulare und Erläuterungen zur Verfügung. Eine web-basierte Plattform mit vielen detaillierten und konkreten Hilfestellungen, Leitfragen und Vorlagen bzw. Mustern erleichtert das Führen des von der DSGVO geforderten „Verzeichnisses der Verarbeitungstätigkeiten“. Die amtliche Lehrkräftefortbildung bietet durch Juristinnen und Juristen der Regierungspräsidien und durch technisch versierte Pädagogen geleitete Fortbildungen zum Thema Datenschutz an. Die Fortbildungen werden für unterschiedliche Zielgruppen angeboten (Schulleiterinnen und Schulleiter, Datenschutzbeauftragte an Schulen, Moodle-Administratorinnen und -Administratoren, Multimediaberaterinnen und Multimediaberater, Fachberaterinnen und Fachberater, Lehrkräfte, die „Urheberrecht“ und „Datenschutz“ im Unterricht behandeln). Das Kultusministerium hat somit mit einer Vielzahl von Maßnahmen die Umsetzung der DSGVO unterstützt und wird dies auch künftig tun.

Das Umweltministerium hat Leitlinien erarbeitet sowie entsprechende Meldeprozesse etabliert, um die Einhaltung der datenschutzrechtlichen Vorgaben sicherzustellen. Des Weiteren gibt es – neben der behördlichen Datenschutzbeauftragten – in den jeweiligen Abteilungen zusätzliche Ansprechpersonen für den Datenschutz. Die behördliche Datenschutzbeauftragte, das für die organisatorische Umsetzung zuständige Organisationsreferat und die Ansprechpersonen stehen dabei in engem Austausch. Zudem findet ein reger Austausch mit der Informationssicherheitsbeauftragten statt. Es finden außerdem regelmäßig hausinterne Schulungen zum Datenschutz statt und die Beschäftigten finden im Intranet entsprechende Informationsangebote und Arbeitshilfen.

Bereits vor Inkrafttreten DSGVO wurde im Wirtschaftsministerium ein Datenschutzteam eingerichtet, das die Vorgaben der DSGVO umgesetzt hat und seither allen Beschäftigten beratend zur Verfügung steht. Im Zuge der Umsetzung des vom Datenschutzteam des Wirtschaftsministeriums erarbeiteten Datenschutzmanagementsystems wurden in allen Fachabteilungen und sonstigen Organisationseinheiten Ansprechpartner für den Datenschutz benannt. Den organisatorischen Rahmen bildet die Datenschutzverfügung des Wirtschaftsministeriums, in der unter anderem Zuständigkeiten, Prozesse und Meldewege festgelegt sind. Die Sensibilisierung und Schulung der Beschäftigten in den Grundlagen des Datenschutzrechts ist Gegenstand regelmäßig stattfindender Schulungen. Im Intranet des Wirtschaftsministeriums finden die Beschäftigten eine umfangreiche Sammlung von Handreichungen und Arbeitshilfen zum Datenschutzrecht. Der Daten-

schutzbeauftragte, das Datenschutzteam und der Informationssicherheitsbeauftragte arbeiten eng zusammen und tauschen sich regelmäßig aus. In technischer Hinsicht setzt das Wirtschaftsministerium die von der BITBW festgelegten technischen Maßnahmen wie z. B. Passwortrichtlinie etc. um.

Im Sozialministerium nimmt der Datenschutz einen hohen Stellenwert ein. In den vergangenen Jahren wurden in allen Fachabteilungen Ansprechpartner für den Datenschutz etabliert, welche die Fachreferate in enger Zusammenarbeit mit der behördlichen Datenschutzbeauftragten bei der Umsetzung datenschutzrechtlicher Regelungen und Vorgaben bei vielfältigen Projekten unterstützen und begleiten. Die Mitarbeitenden werden außerdem regelmäßig im Datenschutzrecht geschult und in Abstimmung mit dem IT-Sicherheitsbeauftragten für etwaige Sicherheitsrisiken und potenzielle Datendiebstahlsquellen sensibilisiert. Im Intranet stehen zudem für die Beschäftigten umfangreiche Informationen, Vorlagen und Arbeitshilfen zu verschiedenen Datenschutzthemen bereit.

Die Einhaltung der rechtlichen Vorgaben zum Datenschutz ist für das Justizministerium eine Selbstverständlichkeit. Die technisch-organisatorischen Maßnahmen des Justizministeriums werden regelmäßig evaluiert. Da die aktuelle Evaluation derzeit läuft, kann noch keine Aussage zu deren Ergebnissen getroffen werden. Datenschutzverletzungen werden aber auch außerhalb des Evaluierungsturnus stets zum Anlass einer Prüfung von notwendigen Veränderungen genommen.

Durch die Implementierung des Datenschutz-Teams als Teil des Datenschutzmanagementsystems (DSMS), der Einführung und des Nachhaltens von internen Pflichtschulungen sowie der Verankerung datenschutzrechtlicher Vorgaben in Prozessen wird im Verkehrsministerium den Anforderungen datenschutzrechtlicher Vorgaben nachgekommen und ein hohes Datenschutzniveau bei allen Arbeitsabläufen gewährleistet.

Im Ministerium Ländlicher Raum wurde ein toolgestütztes Datenschutzmanagementsystem etabliert. Zudem wurde eine Stelle für den operativen Datenschutz, die BSI-zertifiziert ist, eingerichtet. Im Rahmen der Rezertifizierung 2022 wurde der Baustein CON.2 Datenschutz erfolgreich geprüft, ohne Abweichungen und ohne Empfehlungen. Zudem werden regelmäßig in Zusammenarbeit mit der Informationssicherheit Pflichtschulungen für die Beschäftigten durchgeführt.

Im Ministerium für Landesentwicklung und Wohnen wurde ein Datenschutzmanagement eingeführt und im April 2023 in einer Datenschutzverfügung schriftlich fixiert. Ein Datenschutzteam ist für die Implementierung des Datenschutzrechts im Ministerium für Landesentwicklung und Wohnen zuständig. Es werden regelmäßige Schulungen der Mitarbeitenden durchgeführt und umfangreiche Informationen zum Datenschutz im Intranet zur Verfügung gestellt. Auch wurden Beauftragte für den Datenschutz in den Fachabteilungen benannt, die in enger Zusammenarbeit mit dem Datenschutzteam die Umsetzung datenschutzrechtlicher Vorgaben in den jeweiligen Organisationseinheiten unterstützen. Hinsichtlich IT-technischer Maßnahmen wird zudem auf die BITBW und das BITBW-Gesetz bzw. dessen Stoßrichtung der IT-Bündelung und -Zentralisierung verwiesen. Darüber hinaus ist auch auf die Vermögensverwaltung zu verweisen, die als zentrale Dienstleisterin für die Errichtung und Renovierung von Büroflächen der Landesverwaltung organisatorische Sicherheitsthemen mitberücksichtigt.

Strobl

Minister des Inneren,
für Digitalisierung und Kommunen