Der Landesbeauftragte für den DATENSCHUTZ und die INFORMATIONSFREIHEIT Rheinland-Pfalz

Pressegespräch

Best of Datenschutz - Lebensnahe Datenschutzfälle aus 2023 und 2024

I. Überblick: Zusätzliche Fragen stellen sich

Im Jahr 2023 trat der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, Prof. Dr. Dieter Kugelmann, seine **zweite Amtszeit** an. Vom Landtag war er zuvor mit großer Mehrheit wiedergewählt worden. Im Februar 2024 konnte das Land Rheinland-Pfalz zudem das **50. Jubiläum des Landesdatenschutzgesetzes** feiern – des drittältesten Datenschutzgesetzes der Welt. Die von uns schon im Jahr 2015 gegründete und kürzlich umfassend modernisierte Jugendwebseite www.youngdata.de durfte sich im vergangenen Herbst über einen dritten Platz beim **renommierten Medienpreis** TOMMI freuen.

Die Aufgabenerfüllung des Landesbeauftragten folgt **neuen Schwerpunkten**:

Im Hinblick auf das Datenschutzrecht war in 2023 vieles in Bewegung. Verhandlungen auf Bundesebene zur Änderung des **Bundesdatenschutzgesetzes** wurden intensiv von den Datenschutzaufsichtsbehörden begleitet. Parallel dazu ist die Diskussion um **Künstliche Intelligenz** in exponentiellem Maße angewachsen. Beide Themen beschäftigen gerade auch den LfDI Rheinland-Pfalz, der in entsprechenden Gremien **Leitungspositionen** innehat: dem Arbeitskreis „DSK 2.0“ sowie der „Taskforce KI“ der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz / DSK).

Im Alltag der rheinland-pfälzischen Bürgerinnen und Bürger spielen datenschutzrechtliche Fragen eine ungebrochen große Rolle. Die **Zahl der Beschwerden** ist – nach einer Hochphase während der Corona-Jahre – leicht auf 822 (in 2022: 1.107) zurückgegangen. Gleiches gilt für die Zahl der gemeldeten **Datenpannen**: 678 (in 2022: 715). Zugleich erhöht sich die Zahl der Fälle (494), in denen wir aufgrund von **Hinweisen oder von Amts wegen** tätig werden mussten. Auch die Komplexität der **Beratungen** von öffentlichen Stellen und von Unternehmen stieg angesichts des oft angestrebten Einsatzes von KI-Tools erheblich an.

II. Fälle

1. Datenverarbeitung in rheinland-pfälzischen Gesundheitsämtern

Im Rahmen des Digitalpakts des Bundes zur **Digitalisierung der Gesundheitsämter** läuft in Rheinland-Pfalz seit Herbst 2022 das Projekt „Einheitliche EDV-Plattform für den Öffentlichen Gesundheitsdienst (ÖGD) in Rheinland-Pfalz“. Der Projektverantwortliche, das Ministerium für Wissenschaft und Gesundheit des Landes Rheinland-Pfalz, verfolgt dabei das Ziel, die im Lande bislang bestehende dezentrale, heterogene IT-Landschaft, die den organisatorischen Prinzipen einer Aufbauorganisation folgt und unterschiedliche Softwareprodukte primär eines Herstellers nutzt, zu harmonisieren und an die Anforderungen des digitalen Verwaltungshandelns anzupassen.

Der LfDI bot dem Ministerium für Wissenschaft und Gesundheit Rheinland-Pfalz frühzeitig eine **beratende Begleitung** des Projektes an. Auf Initiative des LfDI hin wurde eine zusätzliche Arbeitsgruppe zur Umsetzung datenschutzrechtlicher Vorgaben geschaffen. Der LfDI erhielt im Rahmen seiner Begleitung regelmäßig Statusberichte über den aktuellen Entwicklungsstand sowie den projektbezogenen Newsletter. Eine aktive Einbindung in die konkrete Projektarbeit erfolgte nicht. Lediglich bei datenschutzrelevanten Fragen konsultierte das Gesundheitsministerium den LfDI anlassbezogen und bat um Beratung.

Im Zusammenhang mit dem Digitalisierungsprojekt erschienen im November 2023 **Presseberichte über mögliche IT-Sicherheitsdefizite** in rheinland-pfälzischen Gesundheitsämtern. Dabei standen neben den Kreisverwaltungen und dem das Digitalisierungsprojekt koordinierenden Ministerium der Hersteller der im ÖGD eingesetzten Software und der LfDI Rheinland-Pfalz im Fokus. Der LfDI nahm die Berichterstattung zum Anlass, die darin behaupteten Defizite sowie grundsätzlich den Stand der Datensicherheit in den rheinland-pfälzischen Gesundheitsämtern zu klären. Zu diesem Zweck wurden das zuständige Fachministerium, der Software-Hersteller und die 24 Kreisverwaltungen detailliert um Auskunft gebeten. Zudem führte der LfDI zwischen Ende April und Anfang Mai 2024 vier örtliche Feststellungen zum Datenschutz in rheinland-pfälzischen Gesundheitsämtern durch.

Im Ergebnis stellten sich die in der Presse aufgekommenen Befürchtungen hinsichtlich einer unzureichenden IT-Sicherheit in den Gesundheitsämtern als **weniger gravierend** heraus als zunächst angenommen. Anhaltspunkte für ein unbefugtes Abfließen von Gesundheitsdaten der Bürger:innen an Stellen außerhalb der Verwaltung bestanden nicht. Allerdings deckte der LfDI im Rahmen seiner Prüfungen **diverse datenschutzrelevante Schwachstellen** auf, die zum Teil bereits Gegenstand der Berichterstattung in der Presse waren, teilweise aber auch zuvor nicht aufgefallen waren.

Bei den vorgefundenen Missständen war zwischen **softwarebedingten Defiziten** und **Mängeln bei der Umsetzung der datenschutzrechtlichen Vorgaben** durch die Kommunalverwaltungen zu unterscheiden. So verfügte die eingesetzte IT-Anwendung weder über eine datenschutzkonforme **Protokollierungsfunktion** noch über die gebotene Unterstützung für eine hinreichende **Verschlüsselung** der Datenbanken. Auch hatte die Software im Auslieferungszustand bislang das Prinzip der **datenschutzfreundlichen Voreinstellungen** nicht ausreichend beachtet. Auf der

Seite der Kreisverwaltungen wiederum entsprach das **Datenschutzmanagement** häufig nicht den rechtlichen Anforderungen. Zudem waren die zum Schutz der Daten gebotenen technisch-organisatorischen Vorkehrungen nur rudimentär oder gar nicht dokumentiert, so dass bei einigen Maßnahmen unklar blieb, ob diese tatsächlich in der Praxis umgesetzt wurden.

In den im Juli 2024 übersandten **Prüfberichten** benannte der LfDI die jeweiligen Defizite und forderte die Kreisverwaltungen auf, diese zu beseitigen, soweit dies ihrerseits möglich ist. Im Hinblick auf das landesweite Digitalisierungsprojekt sprach der LfDI zugleich gegenüber dem federführenden Ministerium für Wissenschaft und Gesundheit konkrete **Empfehlungen** zur datenschutzkonformen Digitalisierung des Öffentlichen Gesundheitsdienstes in Rheinland-Pfalz aus. Zudem wird der Austausch mit dem Hersteller der in den Gesundheitsämtern eingesetzten IT-Anwendung fortgesetzt.

Empfehlungen an das Ministerium für Wissenschaft und Gesundheit: siehe Anlage.

2. Die Virtual-Reality-Brille und der Jugendschutz

Im Dezember 2023 kaufte eine Kundin in einem rheinland-pfälzischen Elektronikmarkt eine **Virtual-Reality-Brille** als Weihnachtsgeschenk für ihren Sohn. Auf die Bescherung folgte eine böse Überraschung: Mit dem Gerät waren bereits **Facebook- und Instagram-Konten** verknüpft – mit personenbezogenen Daten und vermutlich wenig kindgerechten Inhalten. Die Kundin wandte sich an den Elektronikmarkt, der die Ursache des Vorfalls rekonstruieren konnte: Bei der VR-Brille handelte es sich um ein Gerät, das bereits einmal verkauft war und innerhalb der Rückgabefrist an den Elektronikmarkt zurückgegeben wurde. Im hektischen Vorweihnachtsgeschäft hatte ein Mitarbeiter vergessen, die beiliegende Speicherkarte zu löschen, sodass die VR-Brille datenunbereinigt wieder ins Verkaufsregal gelangte. Der Elektronikmarkt meldete die **Datenpanne** umgehend an unsere Behörde. Der betroffene erste Käufer der VR-Brille hatte keine Kontaktdaten bei seinem Einkauf hinterlegt und konnte somit nicht informiert werden. Da es sich um menschliches Versehen in einem Einzelfall handelte und geeignete Clearing-Prozesse grundsätzlich in dem Elektronikmarkt existierten, wurde von Sanktionsmaßnahmen abgesehen.
Unabhängig vom Einzelfall macht die Angelegenheit deutlich, wie schnell und unerwartet in Zeiten der Vernetzung selbst trivialer Unterhaltungs- und Haushaltsgeräte personenbezogene Daten in unbefugte Hände geraten können. Die **umsichtige Löschung von Daten** dürfte bei der Weitergabe oder Entsorgung anderer Geräte wie smarter Staubsauger, Internet-Radios, Netzwerkkameras, Smartwatches oder Großdrucker ähnlich wichtig sein.

3. Doppelkopf

Im April 2024 meldete sich Frau S. schriftlich zu einem Doppelkopf-Kurs bei einer rheinland-pfälzischen **Volkshochschule** an. Im Rahmen der Anmeldung erfasst die Volkshochschule als Kontaktdatum grundsätzlich auch die E-Mail-Adresse, um Teilnehmer:innen im Falle kurzfristiger Änderungen informieren zu können. Da Frau S. auf dem Anmeldeformular hierzu keine Angaben

gemacht hatte, recherchierte die Volkshochschule in ihrem Kursverwaltungsprogramm, ob bereits bei **früheren Anmeldungen** eine E-Mail-Adresse zu der Frau erfasst wurde. Tatsächlich fand sich bei einer Anmeldung aus dem Jahr 2018 eine E-Mail-Adresse zu einer Person desselben Namens, die jedoch - wie sich später herausstellte - nicht Frau S. gehörte. Diese falsche E-Mail-Adresse wurde daraufhin im Rahmen der Sachbearbeitung auch der aktuellen Kursbuchung zugewiesen, mit der Folge, dass nicht Frau S., sondern eine dritte Person per E-Mail über den Ausfall eines Kurstages informiert wurde. Nachdem die Empfängerin der Volkshochschule mitgeteilt hatte, dass sie nicht zum Doppelkopf-Kurs angemeldet sei, versandte die Geschäftsstelle der Volkshochschule in der Annahme, mit Frau S. zu kommunizieren, im Mai 2024 eine **Kopie der Anmeldung** an die Inhaberin der **falsch erfassten E-Mail-Adresse**. Darin enthalten waren **zahlreiche personenbezogene Daten** wie beispielsweise die Bankverbindung von Frau S.
Aufgrund des Verstoßes gegen die Grundsätze der Rechtmäßigkeit der Datenverarbeitung, der Datenrichtigkeit und der Vertraulichkeit wurde gegen die Volkshochschule eine **Beanstandung** ausgesprochen. Die Volkshochschule wurde außerdem aufgefordert, zukünftig sorgsam zu prüfen, ob der Versand einer Anmeldekopie mit allen darin enthaltenen personenbezogenen Daten in alltäglichen Verwaltungsvorgängen wie oben beschrieben tatsächlich erforderlich ist.

4. Mitarbeitergewinnung per Datenschutzverstoß

Ein Vertriebsdienst aus Koblenz hielt es für eine gute Form der Eigenwerbung, mehrere **Originale von Gehaltszetteln** auf Facebook zu veröffentlichen, mit dem Zusatz: „Es gibt keine Grenze bei uns; jeder mit bisschen Disziplin kann sein Gehalt selbst gestalten“.
Zwar wurde der Name auf den Gehaltsabrechnungen geschwärzt, aber Angaben zu Geburtsdatum, Eintrittsdatum, Krankenkassennummer, Steuer-ID sowie Brutto- und Nettolohn waren nach wie vor ersichtlich. Von einer **hinreichenden Anonymisierung** konnte daher keine Rede sein.

5. Versetzungswillig?

Den LfDI erreichten im Sommer 2023 mehrere Beschwerden zum Portal „Versetzung online“. Das Portal wird von der Aufsichts- und Dienstleistungsdirektion ADD betrieben und bietet **versetzungsinteressierten Lehrkräften** die Möglichkeit, sich nach offenen Stellen „umzusehen“.
Die Lehrkräfte problematisierten, dass bereits bei der Registrierung in dem Portal eine Meldung für die Schulleitung ausgelöst wurde. Dies habe dazu geführt, dass Schulleitungen die betroffenen Lehrkräfte auf ihren **angeblichen Versetzungswunsch** direkt angesprochen hätten. Die Lehrkräfte hatten sich jedoch nur in dem Portal umschauen bzw. sich allgemein informieren wollen, so dass die Konfrontation mit einem angeblichen Versetzungswunsch für sie als überraschend und unangenehm empfunden wurde.
Den Nutzungshinweisen auf der Startseite des Portals war hierzu kein Hinweis zu entnehmen. Die Recherchen des LfDI ergaben, dass die Authentizität der Person, die sich anmeldet, durch Einbeziehung der Schulleitung sichergestellt werden sollte.

Aus technisch-organisatorischer Sicht war es jedoch nicht geboten, bei der Passwortvergabe für die Registrierung zum Portal die Schulleitungen zu beteiligen. So bestand beispielsweise die Möglichkeit, das Passwort per Brief an die Schule zu übersenden oder an eine dienstliche E-Mail-Anschrift des Anmeldenden, die im Registrierungsprozess abgefragt wird.
Auf Aufforderung des LfDI hin stellte die ADD den **Registrierungsprozess datenschutzkonform** um. Die Schulleiterin einer Grundschule wurde zudem per förmlichem Hinweis dafür gerügt, dass sie Informationen aus dem Registrierungsprozess (Lehrerin X ist versetzungswillig) zweckwidrig verwendet und an Dritte weitergegeben hatte.

6. Diskretion, bitte!

Im März 2024 ging die Beschwerde einer Bürgerin ein, die von Nachbarn ihres Heimatorts auf eine erhebliche **Indiskretion im Schalterraum einer nahegelegenen Sparkasse** aufmerksam gemacht wurde. Die Bürgerin hatte zuvor ein längeres Telefonat mit einer Bankmitarbeiterin geführt und darin teils **sensible persönliche Informationen** über ihre Vermögenswerte, einen bevorstehenden Umzug sowie den Gesundheitszustand naher Angehöriger angesprochen. Im Sinne des „aktiven Zuhörens“ hatte die Bankmitarbeiterin alle wesentlichen Informationen des Gesprächs laut wiederholt. Was die Kundin nicht wusste: Die Bankmitarbeiterin führte das Telefonat nicht in einem geschlossenen Büro, sondern in der **öffentlichen Schalterhalle**. Andere anwesende Kunden konnten mithören und waren über die Bankangelegenheiten der betroffenen Bürgerin nun **unfreiwillig bestens informiert**. Eine der anwesenden Personen, die die betroffene Kundin kannte, sprach diese im Nachgang auf den Vorfall an.
Die Sparkasse, von der Bürgerin mit dem Fehlverhalten konfrontiert, erkannte den Vorfall als Datenschutzverletzung nach Art. 33 DS-GVO und **meldete die Datenpanne** umgehend an den LfDI. Die Sparkasse teilte zugleich mit, dass künftig solche Gespräche nur in separaten Räumen geführt werden sollen, die Mitarbeiter:innen entsprechend sensibilisiert und die Dienstanweisung angepasst würden. Da es sich um ein individuelles Fehlverhalten handelte, keine strukturellen Defizite zu erkennen waren und die Sparkasse **datenschutzfreundliche Verbesserungen** vornahm, wurde von weiteren aufsichtsrechtlichen Maßnahmen abgesehen.

7. Auswertung von Kontobewegungen ausdrücklich erlaubt

Der Kunde einer rheinland-pfälzischen Bank erhielt im Herbst 2023 einen Anruf seines Bankberaters, der ihn nach den Hintergründen von **EC-Kartenzahlungen an ein rheinland-pfälzisches Waffengeschäft** fragte. Der Kunde war über die Auswertung seiner Kontobewegungen empört und wandte sich mit einer Beschwerde an den LfDI Rheinland-Pfalz. Jedoch: Die Überprüfung der Abwicklung eines Waffenkaufs über das Girokonto ist **zulässig**; nach dem **Geldwäschegesetz und dem Kreditwesengesetz** sind Kreditinstitute zu solchen Maßnahmen sogar verpflichtet. Nachdem der Gesetzgeber den Straftatbestand der Geldwäsche (§ 261 Strafgesetzbuch) im Jahr 2021 ausgeweitet hat, sind nunmehr alle Vergehen und Verbrechen als taugliche Vortaten der Geldwäsche anzusehen. Durch den Anruf sollte hier die Legalität des Waffenkaufs abgeklärt werden, das Vorgehen war datenschutzrechtlich nicht zu beanstanden.

Der LfDI Rheinland-Pfalz erhält regelmäßig Beschwerden zu ähnlich gelagerten Fällen, auch bei Verdacht der Teilnahme am **unerlaubten Glücksspiel**.

8. Es muss nicht der Mutterpass sein

Im Herbst 2023 erkundigte sich eine Bürgerin beim **Jugendamt** der für sie zuständigen Stadtverwaltung nach den Voraussetzungen eines **Antrags auf Vaterschaftsanerkennung** für ihr in einigen Monaten erwartetes Kind. Ihr wurde erklärt, dass in diesem Zusammenhang die **Vorlage ihres Mutterpasses** zwingend erforderlich sei. Alternative Nachweise für die bestehende Schwangerschaft wie beispielsweise eine ärztliche Bescheinigung wurden als nicht ausreichend abgelehnt. Die werdende Mutter wurde von dem Jugendamt weder auf die Freiwilligkeit der Vorlage des Mutterpasses und bestehende Schwärzungsmöglichkeiten für im Mutterpass enthaltene sensible Gesundheitsdaten hingewiesen noch wurden ihr geeignete Alternativen wie eine Erklärung der behandelnden Ärzte über den voraussichtlichen Geburtstermin genannt.
Nach Ansicht des LfDI war die angestrebte Erhebung sensibler Gesundheitsdaten ohne gültige Rechtsgrundlage **rechtswidrig**. Der LfDI **beanstandete** das Vorgehen des Jugendamtes daher formell. Die Stadtverwaltung teilte im Nachgang mit, dass das voraussichtliche Geburtsdatum eines Kindes nunmehr nach einfacher Erklärung der Eltern in die Urkunde aufgenommen werde, eine Bestätigung darüber werde nicht mehr eingefordert.

9. IT-Panne bei der Öffentlichkeitsfahndung nach einem Tankstellenräuber

Unter dem Fahndungslink https://www.polizei.rlp.de/fahndung/detailansicht/fahndung-nach-tankstellen-raeuber-von-enkenbach-alsenborn betreibt die Polizei eine **Öffentlichkeitsfahndung** zu einem Tankstellenräuber. Wohl aufgrund einer **IT-Panne** bei einem technischen Relaunch der Webseite waren dort zeitweise jedoch nicht bloß Fotos des Täters zu sehen, sondern – beim Aufruf der Vergrößerungsfunktion für die Bilder – auch **Zeugniskopien** von gänzlich unbeteiligten Praktikant:innen, ein Lichtbild eines Polizeibeamten sowie ein Video zu einem mutmaßlichen Wohnungseinbruchsdiebstahl.
Auf den Hinweis eines Bürgers hin forderte der LfDI das zuständige Polizeipräsidium zur unverzüglichen **Entfernung der fälschlich hinterlegten Dateien** auf, was auch umgehend geschah. Nach aktuellem Informationsstand kam die IT-Panne im Zusammenhang mit einer parallel zum Relaunch der Webseite stattfindenden Bewerbungsaktion der Polizei zustande. Zeugniskopien interessierter Praktikant:innen wurden zwischengespeichert, ohne dass dies erforderlich war, und im Zuge des Relaunches unbeabsichtigt verlinkt. Die entsprechenden Einstellungen wurden seitens des Landesbetriebs Daten und Information (LDI) deaktiviert und alle zwischengespeicherten Zeugniskopien wurden sofort und unwiderruflich **gelöscht**.