datiq
Datenschutz. Praktisch.

Whitepaper: Erkenntnisse aus dem Datenschutz-Tätigkeitsbericht 2024 des HBDI

Der am 25. Mai 2025 veröffentlichte Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit (HBDI) bietet wertvolle Einblicke in aktuelle Entwicklungen, Schwerpunkte und Problemfelder rund um Datenschutz und Informationssicherheit. Der aktuelle Bericht für das Jahr 2024 bezieht sich auf das Berichtsjahr 2023 und zeigt deutlich: Die Anforderungen an Unternehmen steigen weiter, die rechtlichen Rahmenbedingungen werden konkreter, und die Erwartungshaltung der Aufsichtsbehörden nimmt zu. Dieses Whitepaper fasst die wesentlichen Erkenntnisse des Berichts zusammen und bietet eine Grundlage für strategische Entscheidungen in Unternehmen, Organisationen und öffentlichen Stellen.

1. Zunahme der Beschwerden und Anfragen

Im Berichtsjahr 2023 verzeichnete der HBDI einen deutlichen Anstieg der Eingaben. Mehr als 6.500 Beschwerden, Anfragen und Hinweise gingen ein – ein Anstieg um ca. 15 % im Vergleich zum Vorjahr. Die meisten Eingaben betrafen klassische Problemfelder wie:

- Ungewollte Werbung (z. B. E-Mail, Telefon, Post)
- Verzögerte oder verweigerte Löschungen
- Unzureichende oder ausbleibende Auskünfte
- Rechtswidrige oder nicht gekennzeichnete Videoüberwachung

Bemerkenswert: Auch vermeintlich einfache Anfragen führen immer häufiger zu aufsichtsrechtlichen Verfahren, wenn Verantwortliche sich nicht fristgerecht oder gar nicht äußern.

2. Aufsichtliche Schwerpunkte

Die Aufsichtsbehörde legt ihren Fokus auf typische Schwachstellen, die in der Praxis häufig vorkommen:

- **Messenger-Dienste** wie WhatsApp oder Telegram, die im Unternehmens- oder Schulkontext ohne ausreichende Absicherung eingesetzt werden
- **Cloud-Dienste**, bei denen unklar bleibt, wer genau Zugriff auf welche Daten hat und ob ausreichende Schutzmechanismen bestehen
- **Datenschutzverletzungen**, die entweder nicht gemeldet oder unzureichend behandelt werden
- **Technisch-organisatorische Maßnahmen (TOMs)**, die nur auf dem Papier existieren, aber nicht gelebt werden

Der HBDI weist nachdrücklich darauf hin, dass TOMs nicht nur dokumentiert, sondern auch wirksam umgesetzt und regelmäßig überprüft werden müssen.

3. Verträge zur Auftragsverarbeitung (AVV)

Ein immer noch großes Problem stellen mangelhaft ausgestaltete AV-Verträge dar. Viele Verantwortliche behandeln den AVV als reine Formalie. Der Bericht betont:

- Verträge müssen **konkret und risikoorientiert** sein

- Die **technischen und organisatorischen Maßnahmen** müssen beschrieben, aktuell und tatsächlich umgesetzt sein
- Eine **klare Regelung zur Meldepflicht bei Datenschutzverletzungen** muss enthalten sein

Entscheidend: Die rechtliche Verantwortung für die Datenverarbeitung bleibt beim Verantwortlichen. Die Beauftragung eines Dienstleisters bedeutet **keine Haftungsfreistellung**, sondern erfordert sorgfältige Auswahl, Kontrolle und Dokumentation.

4. Meldung von Datenschutzverletzungen

Nach wie vor melden viele Verantwortliche Datenschutzverletzungen zu spät oder gar nicht. Der HBDI erinnert an die gesetzliche 72-Stunden-Frist gemäß Art. 33 DSGVO. Häufige Fehler:

- Die Bewertung wird vom Auftragsverarbeiter vorgenommen, nicht vom Verantwortlichen
- Informationen an die Behörde sind unvollständig oder unsystematisch
- Betroffene Personen werden nicht oder nur mit Verzögerung informiert

Die Aufsichtsbehörde macht deutlich: Auch bei einer Verarbeitung im Auftrag muss der Verantwortliche **eigenständig prüfen, bewerten und entscheiden**, ob eine Meldung notwendig ist.

5. Informationssicherheit als Grundpfeiler

Informationssicherheit wird zunehmend als integraler Bestandteil des Datenschutzes verstanden. Der Bericht empfiehlt explizit:

- Regelmäßige Tests der Notfall- und Wiederanlaufkonzepte
- Sichere Authentifizierungsverfahren, insbesondere im Homeoffice
- Prüfung von Zugriffsrechten und deren Dokumentation

Die Zahl der Vorfälle durch Ransomware, Social Engineering und Fehlkonfigurationen steigt stetig. Organisationen sind aufgefordert, die Anforderungen des BSI aktiv umzusetzen, auch wenn sie nicht direkt unter KRITIS oder NIS2 fallen.

6. Internationale Datentransfers

Die neuen Regelungen zum EU-US Data Privacy Framework schaffen eine gewisse Rechtssicherheit. Trotzdem bleiben Drittlandübermittlungen ein risikobehaftetes Thema. Die Aufsichtsbehörde weist darauf hin:

- Die Nutzung von US-Diensten (z. B. Microsoft, Google, Meta) muss begründet und technisch abgesichert werden
- Standardvertragsklauseln allein reichen nicht – es braucht konkrete Schutzkonzepte
- Eine "Datenflusstransparenz" ist zwingend erforderlich

7. Spezifische Problemfelder

Der Bericht widmet sich auch branchenspezifischen Risiken und typischen Fehlerquellen:

- **Gesundheitswesen**: Unverschlüsselte Kommunikation, keine Zugangsbeschränkungen
- **Schulen**: Einsatz privater Geräte ohne Absicherung, unzureichende Elterninformation
- **Behörden**: Faxversand von sensiblen Daten, mangelhafte Protokollierung

Diese Beispiele zeigen: Datenschutz ist kein Spezialthema der IT, sondern ein Querschnittsthema für alle Bereiche einer Organisation.

8. Empfehlungen des HBDI

Der Bericht schließt mit konkreten Praxishinweisen, die Unternehmen direkt umsetzen können:

- **Datenschutzorganisation aufbauen oder professionalisieren** (DSB, Prozesse, Dokumentation)
- **Verträge, Verzeichnisse und Policies regelmäßig überarbeiten**
- **Beschäftigte sensibilisieren**, insbesondere bei Datenzugriff und Mobilgeräten
- **Risiken aktiv erfassen und bewerten**, z. B. durch Datenschutz-Folgenabschätzungen

Fazit
Der Datenschutz bleibt für Unternehmen, öffentliche Stellen und Institutionen eine Daueraufgabe. Der Bericht 2024 zeigt: Aufsicht wird konkreter, Kontrollen intensiver, und die Anforderungen an Verantwortung, Nachweis und Umsetzung steigen. Wer Datenschutz ernst nimmt, minimiert Risiken, verbessert die Resilienz und stärkt das Vertrauen von Kunden, Mitarbeitenden und Geschäftspartnern.

Dieses Whitepaper bietet eine fundierte Grundlage für interne Strategiegespräche, Audits, Schulungsmaßnahmen und organisatorische Anpassungen. Es empfiehlt sich, zentrale Themen aus dem Bericht gezielt im eigenen Unternehmen zu reflektieren und in konkrete Handlungspläne zu übersetzen.

Für Fragen zu den einzelnen Punkten oder Umsetzung von Maßnahmen stehen Ihnen unsere Datenschutzbeauftragten der Datiq GmbH zur Verfügung. Sie erreichen uns per Mail, Telefon oder direktem Online-Meeting über unsere Kontaktadressen unter https://www.datiq.de/kontakt