

Tanja Roßmann, kommunit IT-Zweckverband • Ramskamp 71-75 • 25337
Elmshorn

Amtsangehörige Gemeinde Kollmar
Der Bürgermeister
Amt Horst-Herzhorn
Der Amtsvorsteher
Elmshorner Straße 27
25358 Horst



IT-Zweckverband Schleswig-Holstein
Der Verbandsvorsteher

Behördliche Datenschutzbeauftragte
Tanja Roßmann



Elmshorn, 27.04.2026

Tätigkeitsbericht vom 01.01.2025 bis 31.12.2025

Sehr geehrter Herr Meinert,

dieser Bericht beinhaltet eine Zusammenfassung meiner Tätigkeiten als Datenschutzbeauftragte. Er gibt einen Grobnachweis der erfolgten Tätigkeiten im Kontext mit der Erfüllung der Aufgaben von Datenschutzbeauftragten nach Art. 39 DSGVO in Verbindung mit §§ 5 des zwischen Ihrer Behörde und dem kommunit IT-Zweckverband zur „Aufgabenübertragung für die Tätigkeit als externer behördlicher Datenschutzbeauftragter“ geschlossenen Vertrages. Er dient auch dazu, Optimierungsbedarf anzuzeigen und Verbesserungsmöglichkeiten aufzuzeigen. Gemäß der vertraglichen Vereinbarung ist die Datenschutzschnittstelle des Amtes Horst-Herzhorn für die Steuerung und Koordinierung des Datenschutzes zuständig. Der Datenschutz folgt den Verantwortlichkeiten/Zuständigkeiten nach Maßgabe der Kommunalverfassung und berücksichtigt die Aufgabewahrnehmung durch das Amt Horst-Herzhorn. Soweit nicht im Folgenden besonders hervorgehoben, bezieht sich daher der Bericht auf die datenschutzrelevanten Feststellungen im Amt Horst-Herzhorn.

Der Bericht bezieht sich auf den Zeitraum vom 01.01.2025 bis zum 31.12.2025.

Inhalt

| | |
|---|----|
| Auditierung der Webseite | 3 |
| Zur Datenschutzorganisation..... | 3 |
| Sanktionen und Haftungsrisiken | 4 |
| „Datenpannen“ und andere Datenschutzverletzungen..... | 4 |
| Kontrollmaßnahmen von Aufsichtsbehörden | 5 |
| Kontrollen von Auftragsverarbeitern | 5 |
| Beratung und Unterrichtung..... | 5 |
| Datenschutz-Folgenabschätzungen (DSFA) | 5 |
| Status des Verarbeitungsverzeichnisses..... | 6 |
| Anfragen von Betroffenen | 6 |
| „Abmahnungen“ | 6 |
| Relevante Entwicklungen im Kontext Datenschutz..... | 6 |
| „Status“ des Datenschutzmanagements..... | 9 |
| Team BDSB..... | 10 |
| Ausblick auf den nächsten Berichtszeitraum | 11 |

Auditierung der Webseite

Gemäß Art. 39 Abs. 1 b) DSGVO obliegt der Datenschutzbeauftragten eine Überwachungspflicht, sodass regelmäßige Datenschutzkontrollen in Form von Audits durch mich durchgeführt werden.

Im Jahr 2025 erfolgte eine Auditierung der Webseite der Gemeinde Kollmar (E-Mail vom 02.04.2025). Für das Jahr 2026 ist eine erneute Überprüfung geplant.

Zur Datenschutzorganisation

Die Beschäftigten wissen, wie die Datenschutzbeauftragte zu erreichen ist. Meinen Erfahrungen nach ist auch hinreichend bekannt, in welchen Szenarien eine Einbindung der Datenschutzbeauftragten frühzeitig zu erfolgen hat, um die Anforderungen aus Art. 38 Abs. 1 DSGVO einhalten zu können.

Die datenschutzrechtlichen Aufgaben im Amt Horst-Herzhorn wurden weiterhin durch die Datenschutznchnittstelle koordiniert.

- Jeder Datenschutznchnittstelle wird ein monatlicher Jour fixe mit unserem Datenschutzteam angeboten, welcher durch die Datenschutznchnittstelle des Amtes Horst-Herzhorn wahrgenommen wird.
- Darüber hinaus führen wir quartalsweise Datenschutznchnittstellentreffen unter Beteiligung aller Datenschutznchnittstellen der durch kommunit im externen Datenschutz betreuten Verbandsmitglieder durch. Dies erfolgt vor dem Hintergrund der Nutzung der Synergie-Effekte und der Steigerung der Zusammenarbeit untereinander. Folgende Treffen haben mit den folgenden Inhalten stattgefunden:
 - 22.04.2025: Vgl. Protokoll + Präsentation im Anlagenkonvolut 1
 - ✓ Wir besprechen die Sensibilisierung der Mitarbeitenden und präsentieren in dem Rahmen unseren Newsletter „Datenschutzinfo“ als Teil des Schulungskonzeptes
 - ✓ Wir informieren über die von uns geplanten Special E-Learning-Schulungen als Teil des Schulungskonzeptes
 - ✓ Wir diskutieren die Möglichkeit der Verwendung eines Tools für ein Datenschutz-Managementsystem
 - ✓ Anregungen/Wünsche/Fragen
 - 25.09.2025: Vgl. Präsentation im Anlagenkonvolut 2
 - ✓ Wir präsentieren Neues von Aufsichtsbehörden und aus der Rechtsprechung
 - ✓ Wir berichten zum Thema E-Learning Schulungen sowie zu unseren Mustern eines Verzeichnisses der Verarbeitungstätigkeiten, der Schwellwertanalysen und Datenschutzerklärungen, die wir im Laufe des Jahres noch aktualisieren
 - ✓ Wir gehen auf weitere Themen/Fragen/Wünsche im Treffen ein

- 17.12.2025: Vgl. Präsentation im Anlagenkonvolut 3
 - ✓ Wir präsentieren Neues von Aufsichtsbehörden und aus der Rechtsprechung
 - ✓ Wir berichten zu den Themen M365 bei kommunit, der KI-Strategie von kommunit sowie zur Aktualisierung des Datenschutzhandbuches samt mitgeltender Unterlagen
 - ✓ Weitere Themen/Fragen/Wünsche
- Gleichzeitig bieten wir eine regelmäßige Berichterstattung der behördlichen Datenschutzbeauftragten gegenüber dem Verantwortlichen an. Dieses Angebot ist von Ihrer Behörde wahrgenommen worden. Die entsprechenden Protokolle aus den Terminen finden Sie beigefügt im Anlagenkonvolut 4

Sanktionen und Haftungsrisiken

Im Berichtszeitraum sind meiner Kenntnis nach keine Sanktionen durch eine Aufsichtsbehörde oder ein Gericht zu Ihrem Nachteil verhängt worden und keine Schadensersatzansprüche geltend gemacht worden.

Nach § 19 Abs. 1 LDSG werden gegenüber Behörden Geldbußen nicht verhängt. Straftaten nach § 19 Abs. 2 bis 4 LDSG sind mir nicht bekannt geworden.

„Datenpannen“ und andere Datenschutzverletzungen

Nach Art. 33 und 34 DSGVO sind bestimmte Verletzungen des Datenschutzes der zuständigen Aufsichtsbehörde und bei hohen Risiken auch den betroffenen Personen zu melden.

Nach *Art. 33 Abs. 1 DSGVO* ist eine Meldung nicht erforderlich, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu *einem Risiko* für die Rechte und Freiheiten natürlicher Personen führt. Dies folgt aus dem risikobasierten Ansatz der DSGVO. Mit dieser gesetzlichen Formulierung meint der Normgeber jedoch nicht ein (in der realen Welt nicht existierendes) Null – Risiko, sondern ein *geringfügiges Risiko*, also ein Verhältnis von Eintrittswahrscheinlichkeit und Schadenshöhe, das eine Meldung bei einer rationalen Abwägung aller relevanten Gefahrenaspekte entbehrlich macht. Die Rechtslage insoweit ist nicht ganz unstrittig, z.T. wird auch eine Meldepflicht bei einem geringfügigen Risiko angenommen – eine Auffassung, die ich nicht teile. Eine Anpassung des Gesetzes auf „mittleres Risiko“ ist bisher jedoch nicht erfolgt. Aussicht auf Änderungen gibt es jedoch. Die EU-Kommission schlägt vor, die Meldepflicht sogar auf ein „hohes Risiko“ zu begrenzen und auch die Frist für die Meldung zu verlängern. Wir halten Sie insoweit auf dem Laufenden.

Bei einem hohen Risiko muss *gemäß Art. 34 DSGVO* auch der Betroffene informiert werden.

Es bedarf daher einer *Prognose zu den Folgen eines Datenschutzverstoßes*. Diese erstellt *der Verantwortliche selbst*. Wichtig ist, die Prognoseentscheidung hinreichend zu dokumentieren, damit sie gegebenenfalls im Nachgang auch durch Aufsichtsbehörden überprüfbar ist. Alle erforderlichen Prüf – und Dokumentationsunterlagen stellen wir mit

entsprechenden Erläuterungen zur Verfügung. Diese befinden sich auch im Datenschutzhandbuch, bzw. wurden in den regelmäßigen Newslettern kommuniziert. Soweit diese Vorlagen in der Verwaltung implementiert wurden, liegen daher auch geeignete Prozesse zur Abarbeitung diese Thematik vor. Nach meiner bisherigen Wahrnehmung erfolgt die Abarbeitung von Datenschutzverletzungen fundiert dem vorgeschlagenen Prozess folgend.

Aus dem Jahr 2025 sind mir *keine Datenschutzverletzungen* mitgeteilt worden.

Kontrollmaßnahmen von Aufsichtsbehörden

Es sind keine Kontrollmaßnahmen durchgeführt worden.

Kontrollen von Auftragsverarbeitern

Die Durchführung von Kontrollen von Auftragsverarbeitungen erfolgt nur aufgrund ausdrücklichen Wunsches und Beauftragung durch die kommunale Stelle. Entsprechende Aufträge wurden an mich nicht herangetragen. Kontrollen sind daher nicht durchgeführt worden. Die überwiegende Anzahl der Auftragsverarbeitungsverträge wird überdies bei kommunit geführt.

Beratung und Unterrichtung

Im Berichtszeitraum sind keine Beratungsanfragen an mich als Datenschutzbeauftragte herangetragen und beantwortet worden.

Zur Pflege und Aktualisierung des Datenschutzhandbuches, sowie zur Information über wichtige aktuelle Themen erhalten Sie regelmäßig einen Newsletter. Folgende Newsletter haben Sie im Jahr 2025 erreicht (vgl. Anlagenkonvolut 5):

- Nr. 001_kommunit_Datenschutzinfo_BASIS_2025 - Schulungskonzept
- Nr. 002_kommunit_Datenschutzinfo_BASIS_2025 - Datenminimierung
- Nr. 003_kommunit_Datenschutzinfo_BASIS_2025 - Löschen
- Nr. 004_kommunit_Datenschutzinfo_SPEZIAL_2025 – E-Payment
- Nr. 005_kommunit_Datenschutzinfo_SPEZIAL_2025 – Facebook Fanpage
- Nr. 006_kommunit_Datenschutzinfo_SPEZIAL_2025 - Löschkonzept
- Nr. 007_kommunit_Datenschutzinfo_SPEZIAL_2025 – keine Monatsfrist bei Auskunft
- Nr. 008_kommunit_Datenschutzinfo_BASIS_2025 – Datenschutz im Alltag

Datenschutz-Folgenabschätzungen (DSFA)

Nach Art. 35 DSGVO ist eine Datenschutz-Folgenabschätzung durchzuführen, wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Dann führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.

Gerade im behördlichen Bereich ist eine DSFA nach Art. 35 Abs. 10 DSGVO jedoch häufig bereits aus Rechtsgründen nicht erforderlich.

Grundsätzlich erforderlich ist eine DSFA allerdings, wenn das Ergebnis der Schwellwertanalyse dies erfordert. Die Schwellwertanalysen werden durch die Verwaltung zu jeder Verarbeitungstätigkeit erstellt und im Anschluss die Entscheidung getroffen, ob eine DSFA veranlasst ist oder nicht. Alle hierzu erforderlichen Vorlagen und Muster werden durch uns im Datenschutzhandbuch zur Verfügung gestellt. Auf Anfrage werden Schulungen hierzu angeboten.

Im Jahr 2025 sind unter meiner Beteiligung keine Datenschutz-Folgenabschätzungen durchgeführt worden.

Status des Verarbeitungsverzeichnisses

Beim Amt Horst-Herzhorn wird ein Verzeichnis von Verarbeitungstätigkeiten geführt. Um dieses auf den neuesten Stand zu bringen, haben wir (Team Datenschutz) uns mit 2 repräsentativen öffentlichen Stellen in Verbindung gesetzt. Wir haben dort vor Ort gemeinsam mit der Mitarbeiterschaft das vorhandene Muster-Verzeichnis aktualisiert. Dieses ist anonymisiert worden und wird Ihnen wie angekündigt zusammen mit Muster-Datenschutzerklärung und Muster-Schwellwertanalysen, die von uns vorgeschlagen werden, zur Verfügung gestellt. Diese sollten dann mit den aktuellen Verarbeitungstätigkeiten im Amt abgeglichen und gegebenenfalls angepasst werden.

Anfragen von Betroffenen

Die Betroffenenrechte ergeben sich aus Art. 12 bis 23 DSGVO

Im Berichtszeitraum hat es nach meinen Informationen keine Anfragen betroffener Personen gegeben.

„Abmahnungen“

Abmahnungen bzgl. eines Verstoßes gegen die DSGVO von Betroffenen sind meines Wissens im Berichtszeitraum nicht vorgekommen.

Relevante Entwicklungen im Kontext Datenschutz

Im Jahr 2025 hat sich zum Thema Datenschutz viel getan – alle relevanten Entwicklungen finden Sie in unseren beigefügten Newslettern (Anlagenkonvolut 5), sowie in dem beigefügten Protokoll nebst Anlagen zu den Schnittstellentreffen (Anlagenkonvolut 1-3), sowie den regelmäßigen Berichten gegenüber dem Verantwortlichen (Anlagenkonvolut 4).

Rund um M365

Besonders interessant war die Entwicklung der Rechtsansicht der Aufsichtsbehörden zu M365, insbesondere in der öffentlichen Verwaltung.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) erachtet die Datenverarbeitung in Microsoft 365 für unzulässig. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (kurz DSK) ist ein informeller Zusammenschluss deutscher Aufsichtsbehörden.

Im Jahre **2022** hatte die Datenschutzkonferenz noch eine Stellungnahme verfasst, wonach der Hauptkritikpunkt und zugleich der offizielle Beschluss der DSK („Festlegung“ vom 24.11.2022) wie folgt lautet:

„Die DSK stellt unter Bezugnahme auf die Zusammenfassung des Berichts fest, dass der Nachweis von Verantwortlichen, Microsoft 365 datenschutzrechtskonform zu betreiben, auf der Grundlage des von Microsoft bereitgestellten „Datenschutznachtrags vom 15. September 2022“ nicht geführt werden kann. Solange insbesondere die notwendige Transparenz über die Verarbeitung personenbezogener Daten aus der Auftragsverarbeitung für Microsofts eigene Zwecke nicht hergestellt und deren Rechtmäßigkeit nicht belegt wird, kann dieser Nachweis nicht erbracht werden.“

In der Rechtswissenschaft wird die Nutzung von M365 in weiten Teilen ganz anders beurteilt. Eine obergerichtliche Entscheidung hierzu gibt es nicht.

Die Rechtsauffassung von Aufsichtsbehörden hat sich in den Folgejahren **gravierend geändert und eine positive Entwicklung** genommen.

Spannend ist aus unserer Sicht vor allem die Wendung zur Einschätzung der Aufsichtsbehörden zur Verwendung von **M365 in der öffentlichen Verwaltung**, hier insbesondere der Bericht des hessischen Beauftragten für Datenschutz und Informationsfreiheit zum Einsatz von Microsoft 365 vom 15. November 2025 - **M365-Bericht des HBDI (Stand: November 2025, Vers. 1.0)** (Der Bericht befindet sich in der Anlage 3 zum Schnittstellentreffen am 17.12.2025).

Unverändert ist, dass die **Rechtslage insoweit immer noch als offen** einzustufen ist. Es gibt insoweit keine einschlägige Rechtsprechung, die für mehr Rechtssicherheit sorgen könnte. **Es gibt also keine absolute Rechtssicherheit – weder in die eine noch in die andere Richtung.** Keineswegs ist die Nutzung von Microsoft 365 eindeutig risikofrei oder unproblematisch. Andererseits steht auch nicht fest, dass der Einsatz eindeutig und unvermeidlich unzulässig ist.

Gleichzeitig gilt, dass es ohnehin um **Einzelfallbetrachtungen** geht.

Ausschlaggebend für die datenschutzkonforme Verwendung von M365 in der Behörde ist die konkrete tatsächliche, vertragliche und technische/technologische Situation in der kommunalen Stelle. Davon hängt es ab, ob im Ergebnis eine datenschutzkonforme und datensichere Lösung gefunden worden ist.

Nun aber zur neuen Richtung der hessischen Aufsichtsbehörde:

Der **M365-Bericht des HBDI (Stand: November 2025, Vers. 1.0)**, behandelt sämtliche von der DSK bishervorgebrachten Einwände in Abstimmung mit MS führt sie geeigneten Lösungsvorschlägen und Handlungsempfehlungen für Verantwortliche zu.

Die avisierten Änderungen zur bisherigen normativen Situation hat MS bereits umgesetzt. Damit dürften die Einwände, die die DSK **2022** bisher gegen den Einsatz von M365 insoweit vorgebracht hat, **drei Jahre später** keine belastbare Relevanz mehr haben.

M365-Bericht des HBDI (Stand: November 2025, Vers. 1.0)

Im Sommer 2024 hatte das Hessische Digitalministerium (HMD) den Hessischen Beauftragten für Datenschutz und Informationsfreiheit (HBDI) in seine Überlegungen zu etwaigen Nutzungsszenarien von Microsoft 365 (M365) in der Hessischen Landesverwaltung eingebunden. Am Beispiel des Einsatzes von MS Teams fanden in der Folge zwischen Microsoft (MS) – geführt durch die Microsoft Deutschland GmbH – und dem HBDI im Sommer 2024 erste Gespräche zur abstrakten Evaluierung der Anforderungen eines DSGVO-konformen Einsatzes von M365 in der Hessischen Landesverwaltung statt.

Parallel gab es seitens MS das Angebot ausgelöst aus dem nicht-öffentlichen Bereich, mit dem HBDI Gespräche über die grundsätzlichen Voraussetzungen eines DSGVO-konformen Einsatzes von M365 zu führen.

Aufgrund dieser parallel stattfindenden Entwicklungen im öffentlichen und im nicht-öffentlichen Bereich **vereinbarten MS und der HBDI, Gespräche aufzunehmen**, um – **unabhängig von konkreten Projektvorhaben oder aufsichtsbehördlichen Verfahren – über die Bedingungen eines DSGVO-konformen Einsatzes von M365 zu sprechen**.

Ziel der Gespräche sollte es nach dem **gemeinsamen Willen von MS und dem HBDI** sein, unter Berücksichtigung zwischenzeitlicher Entwicklungen (insb. **Weiterentwicklung des Vertragswerks von MS, veröffentlichter Kundendokumentation, rechtlicher Änderungen wie dem Angemessenheitsbeschluss der Europäischen Kommission betreffend Datentransfers in die USA sowie technischer Entwicklungen wie dem Ausbau der „EU-Datengrenze“ von MS**) und der Schlussfolgerungen und Forderungen der **Datenschutzkonferenz (DSK - Zusammenschluss der Datenschutzbehörden in Deutschland)** zu überprüfen, ob diese **Feststellung drei Jahre später noch zutrifft** oder ob **praxistaugliche und datenschutzkonforme Ergebnisse** in Hinblick auf die Anforderungen des Art. 28 DSGVO für den öffentlichen und den nicht-öffentlichen Bereich erarbeitet werden können.

Ausgehend von der zusammenfassenden Feststellung der DSK, dass „der Nachweis von Verantwortlichen, Microsoft 365 datenschutzrechtskonform zu betreiben, auf der Grundlage des von Microsoft bereitgestellten ‚Datenschutznachtrags vom 15. September 2022‘ nicht geführt“ werden könne und angesichts der Verantwortung der Verantwortlichen für die durch Auftragnehmer unterstützte Datenverarbeitung, sollte mit Blick auf die Handlungsmöglichkeiten von Auftragnehmern **und** Verantwortlichen geprüft werden, ob und wie die Rechtssicherheit für beide **zusammen** und sich ergänzend erreicht werden kann. Sie sollten in die Lage versetzt werden, ihre Nachweispflichten zum datenschutzkonformen Einsatz von M365 bezüglich der oben genannten Kritikpunkte der DSK erfüllen zu können.

Mit dieser Blickrichtung sieht der Hessische Bericht **Handlungsempfehlungen für Verantwortliche** vor.

Im Zuge der gemeinsamen Gespräche für öffentliche Stellen mit Sitz in Hessen wurde insbesondere **das Data Protection Addendum (DPA) für öffentliche Stellen** - nachfolgend „**DPA-ös**“ grundlegend überarbeitet. Das DPA ist nicht – wie vielfach gemeint

wird – nur ein „Data Processing Agreement“, also ein reiner Auftragsverarbeitungsvertrag. Das Dokument ist ein Rahmendokument, in dem die Datenverarbeitung bei der Nutzung von Produkten und Services von Microsoft geregelt wird. Microsoft ist hier teilweise als Auftragsverarbeiter tätig und in anderen Bereichen selbst Verantwortlicher der Datenverarbeitung. Jedenfalls ist dies aus datenschutzrechtlicher Sicht die grundlegende Vereinbarung, die es erlaubt oder erschwert Microsoft Produkte datenschutzkonform zu nutzen.

Der Bericht behandelt u.a. das durch das DPA-ös geprägte Verhältnis zwischen öffentlichen Stellen und MS.

Unter Verwendung des DPA – öS, sowie der Umsetzung der Handlungsempfehlungen für Verantwortliche kann daher in normativer Hinsicht der Datenschutz nach aktuellem Standard umgesetzt werden. Daneben sind die für eine jeweilige einrichtungsspezifischen technischen und organisatorischen Maßnahmen zu entwickeln und umzusetzen. Art und Umfang der technischen organisatorischen Maßnahmen sind immer einzelfallbezogen. Unabhängig davon sind natürlich allgemeine technische Standards zu beachten.

Die Vorgaben/Handlungsempfehlungen des **M365-Bericht des HBDI** stützen sich auch auf Verarbeitungserlaubnisse für öffentliche Stellen, die zum großen Teil aus dem hessischen Landesrecht abgeleitet werden. Wir haben dies insoweit bereits rechtlich geprüft – es ist gelungen die Rechtsgrundlagen/**Verarbeitungserlaubnisse für öffentliche Stellen** aus dem hessischen Landesrecht auf das Schleswig-Holsteinische Landesrecht zu übertragen, sodass der **M365 – Bericht des HBDI für Schleswig-Holstein kompatibel ist.**

„Status“ des Datenschutzmanagements

Das Datenschutzmanagement wird im Datenschutzhandbuch abgebildet. Das Datenschutzhandbuch liegt aktuell in der Version 2.0 (Stand: 01.01.2023) vor. Das Datenschutzhandbuch gibt einen Rahmen zum Datenschutzmanagement und beschreibt den Aufbau, sowie die Prinzipien des Datenschutzmanagements. Es ersetzt kein eigenes Datenschutzmanagement. Als Grundlage für eine umfassende Informationsquelle vermittelt es zudem die Maßgaben für die datenschutzkonforme Arbeitsweise in der Verwaltung. Darüber hinaus gibt dieses Dokument den Rahmen vor, die in der DSGVO geforderten Dokumentations- und Nachweispflichten (Rechenschaftspflicht) gem. Art. 5 Abs. 2 DSGVO zu erfüllen und dient als Grundlage für interne und externe Prüfungen und Zertifizierungen. Jeder öffentlichen Stelle steht es frei eine alternative Form zur Umsetzung der Maßgaben der DSGVO zu wählen.

Das Datenschutzhandbuch ist mit dem Datenschutzmanagement in der Verwaltung implementiert worden.

Im Jahr 2025 haben wir damit begonnen, das Datenschutzhandbuch sowie sämtliche mitgeltenden Unterlagen zu aktualisieren und zu ergänzen. Davon umfasst sind wie oben dargelegt auch das Muster eines ausgefüllten Verzeichnisses von Verarbeitungstätigkeiten sowie darauf abgestimmte Datenschutzerklärungen und Schwellwertanalysen.

Die Fertigstellung und Übermittlung der neuesten Version 3.0 des Datenschutzhandbuches wird voraussichtlich im 1. Halbjahr 2026 erfolgen. Über die Zwischenstände, Vor-

gehensweise und konkrete Änderungen haben wir in unseren Datenschutzschnittstellen-treffen informiert. Damit eingebunden sind dann auch die amtsangehörigen Gemeinden. Ich verweise auf die Anlagenkonvolute 2 und 3.

Team BDSB



Unsere Ausstattung im Hinblick auf Arbeitsmittel, Literatur und Schulungen wird durch kommunit zur Verfügung gestellt

➤ **Literatur/Tools/Wissensdatenbanken:**

✓ Beck Online – Die Datenbank

Datenschutz- und Informationsfreiheitsrecht PREMIUM

- Kommentare zum Datenschutzrecht
- Kommentare zum BDSG 2003 (außer Kraft)
- Kommentare zu Landesgesetzen
- Kommentare zu Sonderthemen
- Einführungen ins Datenschutzrecht
- Handbücher zum bereichsspezifischen Datenschutz
- Formulare und Checklisten
- Zeitschriften und Newsdienst
- Aufsätze und Rechtsprechung

Beck-KOMMUNALPRAXIS Schleswig-Holstein PLUS

- Kommentare
- Zeitschriften
- Aufsätze und Rechtsprechung

✓ Juris- Portal

Juris Datenschutz

- Rechtsprechung
- Gesetze/Verordnungen
- Kommentare/Bücher
- Zeitschriften
- Verkündungsblätter

- ✓ Dr. O. Koglin. (2025) Datenschutz bei Microsoft 365 und Copilot – Rechtliche Begründung, interne Freigabe, Datenschutz-Folgenabschätzung und Compliance-Prozesse, 1 Aufl. Frankfurt am Main: dfv Mediengruppe
- ✓ C. Ulbricht, D. Brajovic, T. Duhme, J. Hawighorst, M. Huber, V. Iber, C. Nemeč (2024). Praxishandbuch KI und Recht - Rechtliche Aspekte beim Einsatz von Künstlicher Intelligenz – inkl. Der neuen KI-Verordnung der EU, 1. Aufl. Freiburg, München, Stuttgart: Haufe Group
- ✓ M. Rost (2022). Das Standard-Datenschutzmodell (SDM) – Einführung, Hintergründe und Kontexte zum Erreichen der Gewährleistungsziele, 1. Aufl. Wiesbaden: Springer Fachmedien
- ✓ Decareto GmbH, Mittelweg 144, 20148 Hamburg
 - Anbieter für die Durchführung automatisierter Webseitenchecks
- **Schulungen**
 - Datenschutz-Tipps, Newsletter der Datenschutz-Guru GmbH
 - Datenschutz-Risikomanagement in der Praxis (DSFA), bitkom Consult
 - Datenschutz und KI – Vertiefungsworkshop, Workshop der bitkom Consult
 - Insider-Bedrohungen verstehen und managen, bitkom Akademie
 - KI und Ethik, bitkom Akademie

Ausblick auf den nächsten Berichtszeitraum

Für das Jahr 2026 ist insbesondere Folgendes geplant:

- *Regelmäßige Datenschutzschnittstellentreffen*
- *Regelmäßige Datenschutzinfo BASIS und SPEZIAL*
- *Gemeinsame Jahresplanung im puncto der Ziele im Datenschutz für Ihre Behörde (Vorschlag von uns wird erfolgen)*
- *thematische Datenschutzfolgenabschätzung mit den Verbandsmitgliedern in puncto M365, Arbeitskreis M365*
- *Umsetzung Schulungskonzept*
U.a. E-Learning: Ergänzung der Basisschulung über Knowbe4 durch Spezialschulung, die durch das Team BDSB erstellt und über Knowbe4 angeboten wird. Schulungen nach Bedarf und gegebenenfalls themenbereichsbezogen.
- *Fertigstellung und Übermittlung des Datenschutzhandbuches in der Version 3.0, VVT + DSE + Bürgermeistersprechstunde*
- *Auditierung/Webseitencheck*
- *DSMS-Tool GRASP - Testung*
- *KI-Begleitung und Fortentwicklung*

Mit freundlichen Grüßen



Tanja Roßmann
Behördliche Datenschutzbeauftragte