Security-Management

STADTVERWALTUNG KOBLENZ

Tätigkeitsbericht:

Stand des Datenschutz-Managements

Q1/2020

KOBLENZ VERBINDET.

Wichtige Informationen zu diesem Dokument

Dokumentenklasse:	vertraulich
Dokumententitel:	Tätigkeitsbericht Q1/2020 zum Stand Datenschutz-Management der Stadtverwaltung Koblenz
verantwortliche/r Autor/in:	Oliver Philippsen
Dateiname:	2020-03-31_SecMa_DSM_TB-Q1-2020
Fassung vom:	31.03.2020
letzte Veröffentlichung:	31.03.2020
Seitenzahl:	10

Impressum

Security-Management

STADTVERWALTUNG KOBLENZ
Der Oberbürgermeister

Informationssicherheitsbeauftragter: *Merlin Wolf*

Datenschutzbeauftragter*: Oliver Philippsen*

Willi-Hörter-Platz 1

56068 Koblenz

☎ +49 (0)261 129-10 17

✉ security.management@stadt.koblenz.de

Inhaltsverzeichnis

1 Überprüfungen der Datenschutz-Aufsichtsbehörde

1.1 Vor-Ort-Überprüfungen durch die Datenschutz-Aufsichtsbehörde

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (LfDI) hatte noch vor der aktuellen Corona-Krise **örtliche Datenschutzprüfungen in Kommunalverwaltungen** des Landes Rheinland-Pfalz angekündigt.

Der LfDI ist Aufsichtsbehörde und kontrolliert in dieser Funktion die Einhaltung der Vorschriften der Datenschutz-Grundverordnung (DS-GVO), des Bundesdatenschutzgesetzes (BDSG), des Landesdatenschutzgesetzes Rheinland-Pfalz (LDSG) und anderer datenschutzrechtlicher Bestimmungen. Er kann bei Verstößen gegen datenschutzrechtliche Bestimmungen unter anderem Verwarnungen aussprechen, Anweisungen verschiedener Art erteilen und dabei letztlich auch den Einsatz einzelner Verfahren gänzlich untersagen.

Um seine Aufgaben erfüllen zu können, verfügt der LfDI über verschiedene Befugnisse. Neben weiteren ihm zustehenden Untersuchungsbefugnissen kann er örtliche Kontrollen auf der Grundlage von § 16 Abs. 1 und § 17 Abs. 3 LDSG i. V. m. den Art. 57 und 58 der DS-GVO durchführen.

Im Herbst 2019 hat der LfDI mit einer umfangreichen Prüfphase von Kommunalverwaltungen begonnen. Bisher wurden drei Verbandsgemeindeverwaltungen geprüft, weitere neun Prüfungen *(hierunter auch drei Kreisverwaltungen)* sind für dieses Kalenderjahr bereits terminiert worden. Etwa vier Wochen vor einem Prüfungstermin werden die betreffenden Kommunen angeschrieben und – neben der Mitteilung des Prüfungstermins – um die Übersendung verschiedener Unterlagen gebeten. Dies sind unter anderem:

- **Alle Dienstanweisungen bzw. /-vereinbarungen** dieser Verwaltung zum Datenschutz, wie die allgemeine Dienstanweisung über die Maßnahmen zum technischen und organisatorischen Datenschutz bzw. zur Nutzung von Internet- und Intranetdiensten sowie elektronischer Post, über den automatisierten Abruf von Meldedaten (DA Abruf Meldedaten), für den Betrieb von Videoüberwachungsanlagen, zur elektronischen Zeiterfassung, zur elektronischen Zugangskontrolle
- Verzeichnis von Verarbeitungstätigkeiten
- Bereitgestellte Informationen nach Art. 13 DS-GVO
- Aufstellung der Verträge zur Auftragsdatenverarbeitung (Art. 28 Abs. 3 DS-GVO)
- Vorlage des Musters über die Verpflichtung der Mitarbeiter auf das Datengeheimnis (§ 8 LDSG)
- Übersicht über die eingesetzten IT-Verfahren inklusive eines Netzwerkplans
- Übersicht über die jeweiligen Verantwortlichen zu den eingesetzten IT-Verfahren inklusive der Dokumentation (Arbeitshinweis oder Dienstanweisung) der Rechtevergabe

Die bisherigen Prüfungen seien für alle Beteiligten sehr aufschlussreich gewesen. Gerade in den Vorstellungs- und Abschlussgesprächen mit der jeweiligen Behördenleitung haben die Mitarbeiter des LfDI hilfreich beraten und individuelle Fragen beantworten und somit wirksam aufklären können.

Es sei jedoch auch deutlich geworden, dass große Schwierigkeiten in der Umsetzung der Datenschutz-Grundverordnung in den Bereichen des technisch-organisatorischen Datenschutzes und der Datenschutz-Folgenabschätzung liegen.

Im Ergebnis der ersten Prüfungen werde der LfDI seinen bereits eingeschlagenen Weg fortsetzen und das Beratungs- und Informationsangebot auf der Webseite aber auch im Rahmen seiner regelmäßig stattfindenden Regionaltreffen der behördlichen Datenschutzbeauftragten (DSB) an den identifizierten Bedarf noch mehr anpassen.

1.2 Auswirkungen durch die aktuelle Corona-Krise

Der LfDI hat auf seiner Homepage signalisiert, angesichts der Einschränkungen des öffentlichen Lebens sowie der Beeinträchtigung von Abläufen in Wirtschaft und Verwaltung im Rahmen seiner Aufsichts- und Kontrolltätigkeit Fristen gegenüber Verantwortlichen unter Berücksichtigung der aktuellen Gegebenheiten angemessen zu handhaben. Dies gelte auch für die Verhängung und Bemessung etwaiger Zwangs- oder Bußgelder.

Dennoch müssen wir die angekündigten Vor-Ort-Prüfungen und natürlich vor allem die Umsetzung der von der DS-GVO geforderten Maßnahmen weiterhin prioritär im Blick haben. Dies nicht nur wegen der angekündigten Überprüfungen durch die Datenschutz-Aufsichtsbehörde, sondern weil es gesetzlich gefordert ist.

2 Prioritäten in der Umsetzung von Maßnahmen

Zu den wichtigsten von der DS-GVO geforderten umzusetzenden Maßnahmen gehören insbesondere:

1. Führung eines Verzeichnisses von Verarbeitungstätigkeiten (VVT)
2. Vorhaltung und Bereitstellung der Informationen nach Art. 13 DS-GVO
3. Dokumentation über die eingesetzten IT-Verfahren inklusive eines Netzwerkplans sowie über die jeweiligen Verantwortlichen zu den eingesetzten IT-Verfahren inklusive der Rollen-/ und Berechtigungskonzeptionen
4. Aufstellung und Dokumentation der Verträge zu Auftragsverarbeitungen

Im Hinblick auf die Punkte 2 und 4 ist die Stadt Koblenz bereits sehr gut aufgestellt. Die Informationen zur Verarbeitung personenbezogener Daten gemäß Artikel 12 bis 14 DS-GVO der Stadt Koblenz können dem Internetangebot www.datenschutz.koblenz.de bereichsspezifisch entnommen oder z.B. eine schriftliche Ausfertigung dieser Informationen von dem zuständigen Sachbearbeiter erhalten werden.

Auch wird automatisiert in allen E-Mail Signaturen sowie per Bandansage bei allen Zentralnummern der Stadtverwaltung Koblenz auf die Informationen zum Datenschutz hingewiesen.

Für sogenannte Auftragsverarbeitungen gemäß Art. 28 DS-GVO (AV), also immer dann, wenn Dritte mit der Verarbeitung personenbezogener Daten beauftragt werden, hat der Datenschutzbeauftragte (DSB) bereits im Jahr 2018 einen Mustervertrag ausgearbeitet und mit dem Rechtsamt abgestimmt. Gemäß den Bestimmungen der DS-GVO muss ein Vertrag mit verbindlichen Regelungen zum Datenschutz und über weisungsgebundene Tätigkeiten bei Auftragsverarbeitungen geschlossen werden.

Hierfür hat das Security-Management die Organisationseinheiten sowie die Bediensteten über das städtische Mitteilungsblatt sowie den Newsletter sensibilisiert, so dass der neue Mustervertrag schon für sämtliche bereits bestehende Auftragsvergaben wie auch für Neuvergaben Anwendung finden konnte.

Die Umsetzung der in den Punkten 1 und 3 beschriebenen Maßnahmen konnte bisher noch nicht realisiert werden und ist maßgeblich abhängig von der Einführung der neuen Datenschutzmanagement-Software (DsM-S).

2.1 Einführung der neuen Datenschutzmanagement-Software (DsM-S)

Datenschutz ist heute mehr denn je ein unerlässlicher Bestandteil moderner Verwaltungsführung und darüber hinaus ein echtes Qualitätsmerkmal geworden. Ein hohes Datenschutzniveau kann jedoch nur dann erreicht werden, wenn das Thema in der Verwaltung nicht als Belastung empfunden wird. Verwaltungsprozesse müssen datenschutzrechtlich beleuchtet und bewertet werden, um daraus Optimierungspotenzial für den Datenschutz und die Datensicherheit abzuleiten. Dabei dürfen Prozesse und Arbeitsabläufe nicht gestört und die Mitarbeiter bei ihrer eigentlichen Arbeit nicht über Gebühr behindert werden.

Aus diesem Grund wurde auf Initiative des Security-Managements im Rahmen der AG INSIDA (Arbeitsgruppe der Informationssicherheits- und Datenschutzbeauftragten der Betriebsstandorte im ZIDKOR) das Thema „Beschaffung einer DsM-S“ diskutiert.

Die AG INSIDA hat sich dazu entschieden, am Markt erhältliche DsM-S-Lösungen auf ihre Eignung hin zu untersuchen. Einstimmigkeit herrschte darüber, dass nur eine On-Premises-Lösung in Frage kommen würde. Darüber hinaus war es allen Teilnehmern wichtig, dass die zu beschaffende Software folgende Funktionalitäten abbilden kann:

- Führen eines Verzeichnisses von Verarbeitungstätigkeiten
- Melden von Datenschutzverletzungen und -Vorfällen
- Offenes E-Learning Modul, das mit eigenen Inhalten gefüllt werden kann

Der Softwarevergleich ergab, dass das Produkt „Otris Privacy“ der Firma otris software AG als einiges alle Anforderungen erfüllt.

Die AG INSIDA des ZIDKOR hat daraufhin Ende 2019 entschieden, dieses Produkt zu beschaffen und an den einzelnen Betriebsstandorten des ZIDKOR auf Abruf zur Verfügung zu stellen.

Otris Privacy ist eine Datenschutzmanagement Lösung, mit der die Einhaltung von Standards systematisch kontrolliert, analysiert und durch gezielte Umsetzung von Maßnahmen optimiert werden kann. Im Fokus der Lösung steht die Analyse und Optimierung der Arbeitsabläufe unter Datenschutzaspekten. So bietet Otris Privacy unter anderem folgende Möglichkeiten:

- Monitoring von Datenschutz-Maßnahmen
- Dokumentation von Datenschutz-Risiken „Datenschutz-Folgenabschätzung“
- Konfigurierbare Reports „Verarbeitungstätigkeiten“
- Dokumentation der Verarbeitungssicherheit „Auftragsverarbeitungen“
- Sensibilisierungsmaßnahmen „Dokumentation, Nachweis und Durchführung von Schulungen

Die Software ist also ausgewählt und Amt 10.50 / Strategisches IT-Management hat über den hierzu von Seiten des Security-Managements gestellten IT-Projektantrag vom 22.08.2019 beraten und für das Projekt "Einführung eines Datenschutzmanagements (Software: Otris Privacy" der Bildung einer Projektgruppe im Sinne der Ziffer 8 der Dienstanweisung über das IT-Management der Stadtverwaltung Koblenz (DITMa) zugestimmt.

Nun muss die Software nur noch auf der Grundlage durch die AG INSIDA einheitlich festgelegter Standards, Strukturen und Vorgaben etabliert werden. Hierdurch sollen Synergien unter den Teilnehmern der AG INSIDA genutzt und dadurch ein effektives und effizientes Arbeiten mit der Software ermöglicht werden können. **Aufgrund der aktuellen Corona-Krise hält diese Etablierungsphase noch an und es ist noch nicht absehbar, wann die Software in den Echtbetriebt gehen kann.**

Sobald die o. g. Festlegungen getroffen wurden, sind in einem ersten Schritt in dieser Software die Verwaltungsstrukturen und die jeweils verantwortlichen oder zuständigen Mitarbeiter (Führungskräfte, IT-Verantwortliche, Fachadministratoren) anzulegen.

Sodann liegt das **Hauptaugenmerk** auf der **Erstellung des Verzeichnisses der Verarbeitungstätigkeiten (VVT).**

Die Software ist so konzipiert, dass ein damit abgebildetes VVT als Basis für die Umsetzung einer Vielzahl der geforderten Maßnahmen, z. B. durch Auswertungen oder Reports, dient (u. a. für die bereichsspezifische Bereitstellung der Informationen nach Art. 13 DS-GVO, die Erstellung von Löschkonzepten, die Aufstellung der AV-Verträge sowie Dokumentation über die eingesetzten IT-Verfahren inklusive eines Netzwerkplans sowie über die jeweiligen Verantwortlichen zu den eingesetzten IT-Verfahren inklusive der Rollen-/ und Berechtigungskonzeptionen).

2.2 Verzeichnis der Verarbeitungstätigkeiten (VVT)

Für jede einzelne Verarbeitungstätigkeit ist eine Beschreibung nach Maßgabe des Art. 30 DS-GVO anzufertigen.

Als Verarbeitungstätigkeit wird nach der Auffassung des LfDI im Allgemeinen ein Geschäftsprozess auf geeignetem Abstraktionsniveau verstanden. Gemäß den Ausführungen des LfDI ist ein strenger Maßstab anzulegen, so dass nach dortiger Auffassung jeder neue Zweck der Verarbeitung eine eigene Verarbeitungstätigkeit darstellt. Bei einer nur geringen Zweckänderung müsse daher geprüft werden, ob eine bereits bestehende Beschreibung einer Verarbeitungstätigkeit angepasst werden muss oder ob eine vollständig neue Beschreibung anzufertigen ist.

Die Summe der Einzelbeiträge ergibt das Verzeichnis von Verarbeitungstätigkeiten (VVT).

Zwischen den Nutzern der Software (Ludwigshafen, Kaiserslautern, Koblenz und der KommWis) soll möglichst einheitlich vorgegangen und die Verarbeitungstätigkeiten auf gleicher Ebene beschrieben werden. So besteht auch hier die Möglichkeit der gegenseitigen Unterstützung und der Ausschöpfung von Synergien.

Als eine Variante favorisieren die Teilnehmer der AG INSIDA, die festgelegte und definierte Aufgabenwahrnehmung auf Sachgebietsebene als Maßstab für die Erstellung der Beschreibung einer Verarbeitungstätigkeit zu betrachten.

Nach dieser Betrachtung würde beispielsweise jedes der nachfolgenden aufgeführten Sachgebiete des Amtes für Personal und Organisation (Amt 10) sowie des Amtes für Jugend, Familie, Senioren und Soziales (Amt 50) jeweils mindestens eine Verarbeitungstätigkeit darstellen, welche beschrieben werden müsste:

- 10.10.10 Organisationsentwicklung und -betreuung
- 10.10.20 Stellenplanbewirtschaftung, Personalkostenplanung
- 10.20.20 Personalwirtschaft/ -recht
- 10.20.30 Personalentwicklung
- 50.20.10 Altenheimpflege / Hilfe zur Pflege
- 50.20.20 Eingliederungshilfe für behinderte Menschen
- 50.20.30 Stationäre und Ambulante Krankenhilfe
- 50.20.40 Grundsicherung / Hilfe zum Lebensunterhalt
- 50.30.10 Wirtschaftliche Leistungen nach dem Asylbewerberleistungsgesetz

Demnach müssten mindestens ca. <u>250 – 350 Verarbeitungstätigkeiten</u> beschrieben werden.

Das Verzeichnis ist insgesamt sehr umfangreich. Es müssen die wesentlichen Angaben zur Verarbeitung personenbezogener Daten gemacht werden, wie z. B. die legitimierende Rechtsgrundlage, der Zweck der Verarbeitung, die Datenkategorien, der Kreis der betroffenen Personen, die Datenempfänger und die **Löschfristen** der verschiedenen Datenkategorien.

Jedes Verzeichnis muss eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen beinhalten. Die Beschreibung sollte so konkret erfolgen, dass die Aufsichtsbehörde sich einen guten Überblick über die angewendeten Maßnahmen zur Informationssicherheit und Datensicherheit machen kann.

Zusätzlich ist eine Eintrittswahrscheinlichkeit eines Schadens und eine Schadenshöhe der jeweiligen Verarbeitungstätigkeit zu ermitteln. Von diesen Werten leitet sich ab, welche technischen und organisatorischen Maßnahmen überhaupt getroffen werden müssen, um die Daten angemessen zu schützen.

Je höher die Schutzstufe und je größer die Eintrittswahrscheinlichkeit, desto qualifiziertere technische und organisatorische Maßnahmen müssen umgesetzt werden.

Gleichzeitig muss das Verzeichnis so strukturiert sein, dass es den Anforderungen an die von der DS-DGVO geforderte Rechenschaftspflicht genügt.

Bei der Erstellung des VVT sind Detailkenntnisse über die einzelnen Verfahren unabdingbar. Deshalb ist es für eine einzelne Person (z. B. den DSB oder den Informationssicherheitsbeauftragten ISB) unmöglich, das Verzeichnis alleine zu erstellen und zu pflegen. Zudem bedarf es einer intern gut funktionierenden Kommunikation, um das Verfahren aktuell halten zu können.

Weiterer Fahrplan:

Die Erstellung des VVT steht mit Inbetriebnahme der DsM-S, neben der Bearbeitung und Beantwortung der täglich auflaufenden Anfragen und Bewertungsersuchen sowie der allgemeinen gesetzlich definierten Überwachungspflicht eines DSB (operatives Geschäft), im Fokus der Arbeit des Security-Managements.

Das VVT wird beim Security-Management zentral in der DsM-S geführt, die Beschreibungen zu den einzelnen Verarbeitungstätigkeiten erfolgen hingegen via Web Clint zur DsM-S dezentral in den Organisationseinheiten, für die Initial-Versionen gemeinsam mit dem Security-Management und den jeweils verantwortlichen Mitarbeitern.

Der **Output aus dem VVT ist maßgebend für die Umsetzung sämtlicher von der DS-GVO geforderter Maßnahmen**. Daher müssen an die einzelnen Beschreibungen sehr hohe Ansprüche gestellt werden, wodurch die Erstellung stellenweise sehr komplex ist.

Daher wird das Security-Management sehr strukturiert vorgehen, die Organisationeinheiten an die Hand nehmen und bei der Erstellung der Beschreibungen unterstützen. Es sind sowohl die fundierten Kenntnisse und das Sepzialwissen des ISB im Bereich Informationssicherheit und Datensicherheit sowie des DSB im Bereich Datenschutz und im Datenschutzrecht zwingend erforderlich

In der Annahme, dass ab der zweiten Jahreshälfte mit der Software gearbeitet werden kann, wird das Security-Management im Mai/Juni 2020 einen Fahrplan erstellen und auf die Leitungskräfte der Organisationseinheiten zugehen.

Es ist vorgesehen, dass die Initial-Version einer jeden Beschreibung zu einer Verarbeitungstätigkeit gemeinsam mit dem ISB, dem DSB und dem jeweils verantwortlichen Mitarbeiter dezentral vor Ort im betreffenden Sachgebiet erfolgt.

Vorausgesetzt, dass auf diese Art und Weise ca. 3 Verarbeitungstätigkeiten pro Woche beschrieben werden können, wird die Erstellung des VVT ab der zweiten Jahreshälfte 2020 mindestens zwei Jahre in Anspruch nehmen.

Aufgrund der sonstigen durch die Funktionsträger (ISB und DSB) zu erfüllenden Aufgaben ist die Anzahl der zu erstellenden Beschreibungen auf maximal 3 Stück pro Woche zu beschränken. Der anvisierte Zeitrahmen ist aus der Sicht des LfDI sowie des Security-Managements legitim und vertretbar.

Die Pflege der Beschreibungen sowie die Pflicht, diese aktuell zu halten, liegt in der Verantwortung und Zuständigkeit der Organisationseinheiten. Der DSB muss dies lediglich im Rahmen seiner Überwachungspflichten regelmäßig kontrollieren und die Prüfergebnisse dokumentieren.

3 Operatives Geschäft

Die durch die Informationssicherheits- und Datenschutzbeauftragten zu erfüllenden Aufgaben und Pflichten, zu denen auch das operative Geschäft zählt, sind in der DS-GVO und der Dienstanweisung für das Informationssicherheits- und Datenschutz Management der Stadtverwaltung Koblenz (IDaMa) festgeschrieben. Welche dies im Einzelnen sind, kann der Anlage 1 „Aufgabenschwerpunkte ISB/DSB“ entnommen werden.

Ab Februar 2020 erfolgte durch den DSB eine Erfassung „*Auflistung und Dokumentation*“ des täglichen operativen Geschäfts im Bereich Datenschutz. Die hierzu angelegte Übersicht ist als Anlage 2 „Übersicht Operatives Geschäft“ beigefügt.

4 Anlagen

Anlage 1: Aufgabenschwerpunkte ISB/DSB

Anlage 2: Übersicht „Operatives Geschäft“