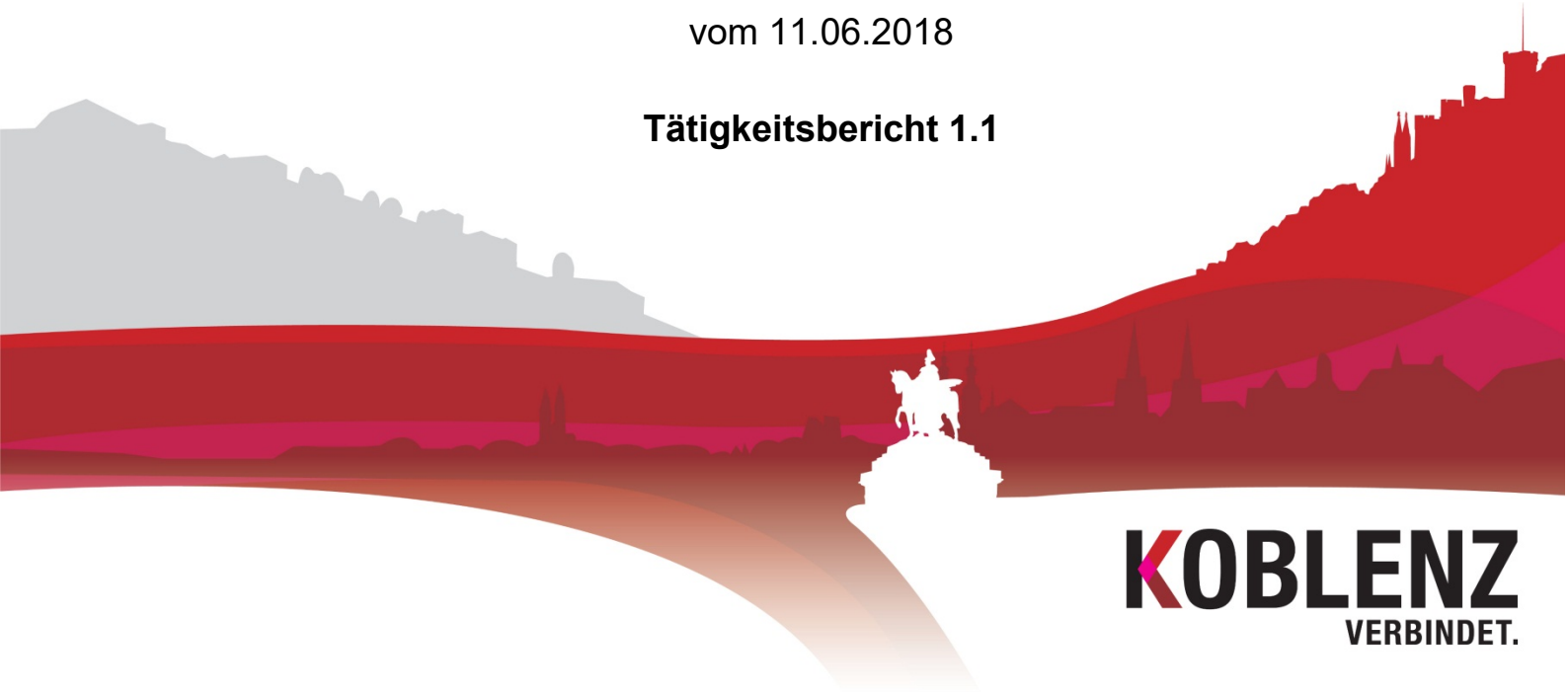
Informationssicherheits- und Datenschutz-Management
STADTVERWALTUNG KOBLENZ

Bericht zum Stand des Informationssicherheits- und Datenschutz-Managements

Erster Bericht

vom 11.06.2018

Tätigkeitsbericht 1.1



KOBLENZ
VERBINDET.

Wichtige Informationen zu diesem Dokument

Dokumentenklasse:	Öffentlich
Dokumententitel:	Erster Tätigkeitsbericht zum Stand des Informationssicherheits- und Datenschutz-Management
Verantwortliche/r Autor/in:	Merlin Wolf und Oliver Philippsen
Dateiname:	2018-06-11_IDaMa_Tätigkeitsbericht1.1
Fassung vom:	11.06.2018
Letzte Veröffentlichung:	11.06.2018
Seitenzahl:	11
Versionsfreigabe:	1.1
Freigegeben durch:	Informationssicherheits- und Datenschutz-Management

Änderungsnachweis

Version	Datum	Status	Bearbeiter/in	Änderung/Bemerkung

Impressum

Informationssicherheits- und Datenschutz-Management
STADTVERWALTUNG KOBLENZ
Der Oberbürgermeister

Informationssicherheitsbeauftragter
Schängel-Center, 3. OG, Zimmer 303
Rathauspassage 2
56068 Koblenz

Tel: 0261 / 129 -1263
Fax: 0261 / 129 -1250

Datenschutzbeauftragter
Rathausgebäude II, 1. OG, Zimmer 110
Willi-Hörter-Platz 2
56068 Koblenz

Tel: 0261 / 129 -1214
Fax: 0261 / 129 -1200

E-Mail: security.managment@stadt.koblenz.de

Inhaltsverzeichnis

1. Vorwort

Zum 25.05.2018 wurde die bereits in Kraft getretene neue Europäische Datenschutz Grundverordnung (DS-GVO) geltendes Recht und findet als direktes supranationales Recht unmittelbar Anwendung.

In der Stadtverwaltung Koblenz werden Unmengen von Informationen und Daten verarbeitet. Je nach Sachgebiet unterliegen diese den Vorgaben der Informationssicherheit oder des Datenschutzes (z.B. personenbezogene Daten oder schützenswerte sowie wettbewerbsrelevante Informationen ortsansässiger Unternehmen).

Die neue DS-GVO sowie eine Vielzahl von nationalen Gesetzen zum Datenschutz und darüber hinaus die Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) geben den Handlungsrahmen, was den Schutz der personenbezogener Daten und informationssicherheitsrelevanter Informationen in der Verwaltung betrifft.

Nicht nur die neue DS-GVO auch die stetig voranschreitende technische Weiterentwicklung von IT-System und Verfahren, die Digitalisierung der Datenverarbeitung sowie die steigende Bedrohung durch Angriffe stellen immer höhere Anforderungen an das Informationssicherheits- und Datenschutz-Management der Stadtverwaltung Koblenz. Durch die zunehmende Vernetzung und Zentralisierung von EDV-Komponenten und Verfahren wiederholen sich IT-Trends auf einem höheren technischen Niveau (bspw. E-Government, E-Payment, DMS, Mobile Devices, Cloud Computing, Social Media).

Im Bereich der Informationsverarbeitung und Kommunikation müssen deshalb Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität der verarbeiteten und übertragenen Informationen durch angemessene technische und organisatorische Maßnahmen gewährleistet werden. Mit der Dienstanweisung für das Informationssicherheits- und Datenschutz-Management der Stadtverwaltung Koblenz sollen die Einhaltung und Überwachung der Informationssicherheit und des Datenschutzes in kompetenter, effizienter sowie effektiver Art und Weise sichergestellt werden. Bürgerinnen und Bürger können erwarten, dass mit ihren Daten vorsichtig und pflegsam umgegangen wird.

Mithin ist Transparenz ein wesentlicher Grundsatz des Datenschutzes und von essenzieller Bedeutung für betroffene Personen (z.B. Bürgerinnen und Bürger, deren Daten durch die Verwaltung erhoben werden). Betroffene Personen sollen in der Lage sein, die Datenverarbeitung zu prüfen oder zumindest wissen, wer was wann und bei welcher Gelegenheit über sie weiß.

Die Informationssicherheit und der Datenschutz werden zu einer unverzichtbaren Grundlage für ein Verwaltungshandeln, dem die Bürgerinnen und Bürger, die Unternehmen und alle unsere Partner ihr Vertrauen schenken können.

2. Begriffsdefinitionen und Schnittstellen

2.0 Informationssicherheit

Informationssicherheit ist eine wesentliche Voraussetzung zur Umsetzung des Datenschutzes. Sie umfasst neben der Sicherheit von IT-Systemen und den damit verarbeiteten und darin gespeicherten Daten auch die Sicherheit von nicht-elektronisch verarbeiteten Informationen, z.B. von Papierakten oder Erfahrungswissen von Bediensteten. Sie umfasst somit den Schutz **von Daten oder Informationen** vor Beeinträchtigung bei der Verarbeitung.

Ein zentraler Bestandteil der Informationssicherheit ist die Datensicherheit. Die Datensicherheit verfolgt das Ziel, alle dienstlichen Daten zu schützen.

2.1 Datenschutz

Der Datenschutz im Sinne der Datenschutzgesetze befasst sich mit dem **Inhalt der verarbeiteten Daten** und schützt konkrete dienstliche Daten, insbesondere alle Angaben über persönliche und sachliche Verhältnisse von natürlichen Personen (nur die Daten natürlicher lebender Personen, grundsätzlich nicht die von juristischen oder toten Personen). Der Datenschutz umfasst somit den Schutz vor missbräuchlicher Verwendung **personenbezogener Daten** und die Wahrung **schutzwürdiger Belange** Betroffener vor Beeinträchtigungen durch die Verarbeitung.

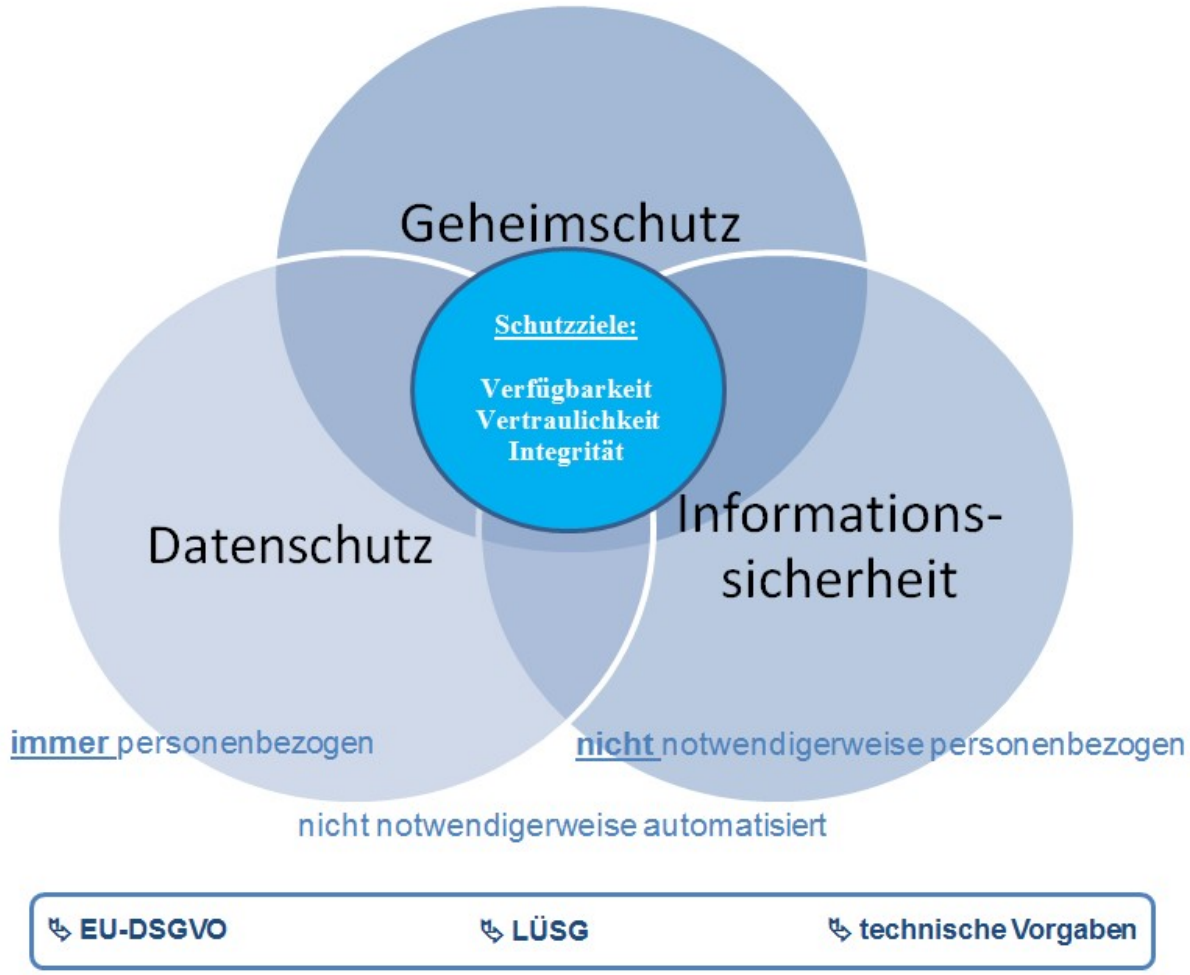
2.2 Geheimschutz

Der Geheimschutz und der vorbeugende personelle Sabotageschutz nach den Maßgaben des Landessicherheitsüberprüfungsgesetzes (LSÜG) und dazugehörigen weiteren Rechtsvorschriften soll die im öffentlichen Interesse geheimhaltungs-bedürftigen Angelegenheiten vor der Kenntnisnahme durch Unbefugte schützen und die Zugangsbefugnis zu einer sicherheitsempfindlichen Tätigkeit auf Personen beschränken, bei denen kein Sicherheitsrisiko besteht.

2.3 Schnittstellen und Zusammenarbeit

In Theorie und Praxis gibt es zwischen den Aufgaben der Informationssicherheit und dem Datenschutz, aber auch zum Geheimschutz, viele Schnittstellen, welche eine enge Zusammenarbeit des Informationssicherheitsbeauftragten und des Datenschutz-beauftragten erforderlich machen. Diese drei Bereiche verschmelzen immer mehr miteinander. Mit der DS-GVO verfolgen die Informationssicherheit und der Datenschutz die Einhaltung der gleichen Schutzziele:

- Verfügbarkeit
- Vertraulichkeit
- Integrität
- Authentizität



3. Allgemeine Sicherheitslage

Die allgemeine Sicherheitslage ist geprägt von Angriffen, die hauptsächlich über E-Mails oder über mit Schadsoftware bestückte Webseiten lokale Rechnersysteme infizierten. Insbesondere waren es die sogenannten Ransomwareangriffe, bei denen die Daten auf den Rechnersystemen verschlüsselt wurden. Gegen eine Lösegeldzahlung wurden diese Daten von den Hackern in einigen Fällen wieder freigegeben. In diesem Zusammenhang sind die Schadprogramme, sogenannte Trojaner wie „Wannacry“, „Petya“, bzw. „NotPetya“ und „Goldeneye“ zu nennen.

Auf die Systeme der Stadt Koblenz und des KGRZ Koblenz hatten diese Schadprogramme keine gravierenden Auswirkungen. Dies ist hauptsächlich auf die umfangreiche technische Absicherung gegen Schadmails zurückzuführen.

4. Informationssicherheits- und Datenschutz-Management

4.1 Etablierung des Informationssicherheits- und Datenschutz-Management

Mit Datum vom 29.05.2017 hat der Stadtvorstand der Etablierung eines Kompetenzteams für ein Informationssicherheits- und Datenschutz-Management sowie für den Geheimschutz der Stadtverwaltung Koblenz zugestimmt.

Diesem Kompetenzteam gehören die durch den Oberbürgermeister der Stadt Koblenz bestellten Informationssicherheits- und Datenschutzbeauftragten sowie Geheimschutzbeauftragten an.

4.2 Aufgaben

Zu den Aufgaben und Pflichten der Informationssicherheits- und Datenschutzbeauftragten gehören insbesondere:

a) Aufbau, Betrieb und Weiterentwicklung der Informationssicherheits- und Datenschutzorganisation innerhalb der Stadtverwaltung Koblenz.

b) Initiierung und Kontrolle der Umsetzung von Informationssicherheits- und Datenschutzmaßnahmen.

c) Erstellung/Verabschiedung von Richtlinien und Regelungen zur Informationssicherheit und zum Datenschutz.

d) Einbindung aller Bediensteten in den Informationssicherheits- und Datenschutzprozess und die Notfallvorsorge.

e) Unterrichtung und Beratung der Organisationseinheiten, Bediensteten und Auftragsverarbeiter (AV) in allen Fragen der Informationssicherheit und des Datenschutzes sowie zu den mit den maßgebenden Bestimmungen zur Informationssicherheit und zum Datenschutz einhergehenden Pflichten.

f) Überwachung der Einhaltung maßgebender Bestimmungen zur Informationssicherheit und zum Datenschutz sowie der Strategien bei der Stadtverwaltung Koblenz oder den Auftragsverarbeitern für die Informationssicherheit und den Schutz personenbezogener Daten inklusive der Zuweisung von Zuständigkeiten, Sensibilisierung u. Schulung der Bediensteten.

(Um Strategien überwachen zu können, muss unter anderem ein Informationssicherheits- und Datenschutzkonzept pro Fachverfahren erstellt werden. Dieses dient u.a. einer Schutzbedarfsfeststellung, Abwägung von Eintrittswahrscheinlichkeiten und Erstellung von Sicherheits- und Löschkonzepten)

g) Beratung (auf Anfrage) im Zusammenhang mit Datenschutz-Folgenabschätzung sowie deren Überwachung.

h) Zusammenarbeit mit dem Landesbeauftragten für die Informationsfreiheit und den Datenschutz Rheinlandpfalz (LFDI) = „Aufsichtsbehörde“.

i) Anlaufstelle für die Aufsichtsbehörde inklusive vorherige Konsultation und Beratung.

j) Betroffene Personen können den Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß den maßgebenden datenschutzrechtlichen Bestimmungen im Zusammenhang stehenden Fragen zu Rate ziehen.

4.3 Flächendeckende Umsetzung

Die Organisationseinheiten müssen sicherstellen und nachweisen können, dass die Verarbeitung im Einklang mit der DS-GVO und den Bausteinen des IT Grundschutzkompendium des BSI (Bundesamt für Sicherheit in der Informationstechnik) erfolgt. Es ist also bis auf die Ebene der einzelnen Organisationseinheiten der Stadtverwaltung Koblenz eine Vorgehensweise sicherzustellen (u.a. durch Leitlinie/n, Richtlinien, Dienst-/Arbeitsanweisungen oder Sicherheitskonzepte), um die gesetzlichen und betrieblichen Anforderungen der Informationssicherheit und des Datenschutzes systematisch zu planen, zu organisieren, zu steuern und zu kontrollieren.

5. Informationssicherheit im KGRZ

5.1 Umsetzung der Anforderungen des neuen Grundschutzes

Im Oktober 2017 legte das BSI (Bundesamt für Sicherheit in der Informationstechnik) mit dem Grundschutzkompendium eine erneuerte Fassung des Grundschutzkataloges vor, in dem die Bausteine und die erforderlichen Maßnahmen zur Umsetzung sicherheitstechnischer Vorgaben an die IT-Betreiber in Behörden und Unternehmungen aufgeführt sind.

Da sich die Vorgaben des neuen Grundschutzkompendiums in Teilen von den vorhergehenden unterscheiden, sind diese zu analysieren und sukzessive umsetzen.

5.2 Ausbau des Informationssicherheitsmanagementsystems (ISMS) des KGRZ

Im Zuge der Neuregulierung des Grundschutzes durch das BSI wurden auch die Standards hinsichtlich des Informationssicherheitsmanagements im BSI-Standard 200-1 neu gefasst. Das KGRZ sieht es als laufende Aufgabe an, den weiteren Ausbau des ISMS zur Verbesserung des IT-Grundschutzes kontinuierlich zu verfolgen, ebenso wie die Beachtung eines weiteren neuen Standards der BSI-Standard 200-3 zum Risikomanagement. In einem ersten Schritt wurde die Informations-sicherheitsleitlinie und Notfallleitlinie des KGRZ auf den neuen Grundschutz hin angepasst.

5.3 Sichereres Rechenzentrum (KGRZ.SRZ)

Aktuell werden die im Neubau des sicheren Rechenzentrums (KGRZ.SRZ) nach dem alten Grundschutz umgesetzten Maßnahmen des BSI mit den Maßnahmen des neuen Grundschutzkompendiums abgeglichen um sicherstellen zu können, dass alle nach neuem Grundschutz geforderten Punkte umgesetzt wurden. Zu jetzigen Zeitpunkt konnten noch keine Abweichungen zum neuen Grundschutz festgestellt werden.

5.4 Umsetzung von Anforderungen der DS-GVO im KGRZ

Das KGRZ Koblenz ist gehalten, als Auftragsverarbeiter von personenbezogenen Daten, die Anforderungen der DS-GVO u.a. in den Bereichen Anonymisierung, Pseudonymisierung und prozessverarbeitender Tätigkeiten umzusetzen. Diese Anforderungen sollen im kommenden Jahr analysiert und daraufhin sukzessive realisiert werden.

6. Tätigkeiten des Informationssicherheits- und Datenschutz-Management

6.1 Bereits umgesetzte Tätigkeiten

- Erstellung und Veröffentlichung der Dienstanweisung für das Informationssicherheits- und Datenschutz-Management der Stadtverwaltung Koblenz (IDaMa).
- Schulung der städtischen Mitarbeiter/innen zu den Basics der Informationssicherheit und des Datenschutzes.
- Kontinuierliche Sensibilisierung und generelle Information der städtischen Mitarbeiter/innen über das städtische Mitteilungsblatt, den Newsletter des IDaMa sowie das Intranet Portal zu wichtigen Themenbereichen der Informations-sicherheit und des Datenschutzes, insbesondere zu den Neuerungen einhergehend mit der DS-GVO.
- Austauschgespräche auf Leitungsebene der Organisationseinheiten.
- Erstellung eines Muster-Informationsschreibens zur Umsetzung der von der DS-GVO geforderten Informationspflichten.
- Einrichtung eines FAQ zur Informationssicherheit und zum Datenschutz.
- Erstellung eines Mustervertrages zu Vereinbarungen zur Informationssicherheit und zum Datenschutz bei Auftragsdatenverarbeitungen (Informationssicherheits- und Datenschutzvertrag der Stadtverwaltung Koblenz).
- Erstellung eines Handlungsrahmens für die Nutzung von „Sozialen Medien“ durch die Stadtverwaltung Koblenz nebst wichtigen dazugehörigen Anlagen (z.B. Vorlage Impressum, Datenschutzerklärungen für die einzelnen Social-Media Dienste, Sensibilisierungstexte, Mustervordruck zur dezentralen datenschutz-rechtlichen Konzeptionierung).
- Erstellung eines Erfassungsbogens zur Dokumentation der bei der Stadtverwaltung Koblenz eingesetzten Verfahren (Verfahrensbeschreibung) als Grundlage für das Verzeichnis von Verarbeitungstätigkeiten.
- Erstellung einer Notfallleitlinie für das KGRZ
- Teilnahme am CERT kommunal. Im letzten Jahr wurde der CERT kommunal (Computer Emergency Response Team) in Rheinland-Pfalz etabliert. Die Stadtverwaltung Koblenz hat hierbei vertreten durch das KGRZ an der Evaluierung und Etablierung des CERT teilgenommen. Aktuell erhalten nun die Stadt Koblenz und die anderen Kommunen Informationen des Warn- und Informationsdienstes des Landes.

- Erstellung einer Anleitung zur Verschlüsselung von E-Mails mit personenbezogenen Daten mittels 7-ZIP für das Amt 50.
- Vorabkontrolle von Anträgen zur Videoüberwachung.
- Wahrnehmung der Rolle des Informationssicherheits- und Datenschutzbeauftragten des ZIDKOR (Zweckverband für Informationstechnologie und Datenverarbeitung der Kommunen in Rheinland Pfalz).
- Teilnahme an der Arbeitsgruppe InSiDa (Informationssicherheit und Datenschutz) des ZIDKOR.

6.2 Anstehende Tätigkeiten

- Kontinuierliche Fortschreibung der Dienstanweisung für das Informationssicherheits- und Datenschutz-Management der Stadtverwaltung Koblenz.
- Etablierung eines softwareunterstützen Informationssicherheits- und Datenschutz-Management-Systems.
- Etablierung eines softwareunterstützen Sicherheitsvorfall- und Notfall-Management.
- Überwachung der Umsetzung der durch die DS-GVO geforderten Informations-pflichten.
- Erstellung einer Informationssicherheits- und Datenschutz-Leitlinie.
- Bereinigung der Verträge zur Auftragsdatenverarbeitung.
- Erstellung eines Informationssicherheits- und Datenschutzkonzeptes pro Fachverfahren.
- Kontinuierliche Schulungs- und Sensibilisierungskampagnen.
- Umsetzung der relevanten Maßnahmen aus dem IT-Grundschutz-Kompendium sowohl im KGRZ als auch in der Verwaltung.
- Zentrale Erfassung aller bei der Stadtverwaltung Koblenz eingesetzten Verfahren (Zentrales Verzeichnis der Verarbeitungstätigkeiten auf der Grundlage der dezentralen Verfahrensbeschreibungen).
- Unterstützung bei der Durchführung notwendiger Informationssicherheits- und Datenschutz-Folgenabschätzungen / Risiko-Folgenabschätzungen.