IV.

DSGVO-Schulungskonzept

für Österreichs Gemeinden und Städte

Entwickelt von der
FH OÖ Forschungs und Entwicklungs GmbH
Research Group Sichere Informationssysteme
Hagenberg

In Kooperation mit
Österreichischem Bundeskanzleramt
Österreichischer Städtebund
Österreichischer Gemeindebund

Version 1.1

Stand 11.03.2018

Inhaltsverzeichnis

Inhaltsverzeichnis 2
1. Vorwort, Verwendungshinweise 5
2. Schulungsplanübersicht 6
2.1. Rolle: Behördenleiter (auch: Geschäftsführer oder Datenschutzbeauftrager von Dienstleister), Bürgermeister 6
2.2. Rolle: IT-Leiter 6
2.3. Rolle: Mitarbeiter Gemeinde/Stadt 7
2.4. Rolle: Mitarbeiter Dienstleister 7
3. Modul Datenschutzgrundlagen 8
3.1. Rechtliche Grundlagen (was sind personenbezogene Daten, warum schützen wir die, gesetzliche Rahmenbedingungen, DSG, DSGVO) 8
3.2. Verarbeitungsgrundsätze 8
3.3. Betroffenenrechte 8
3.4. Meldepflichten und Verantwortlichkeiten 8
4. Modul Überblick über die Maßnahmen für Datenschutz und Informationssicherheit 8
4.1. Warum werden Schutzmaßnahmen getroffen 9
4.1.1. Grundsätze der Informationssicherheit 9
4.1.2. Vertraulichkeit 9
4.1.3. Integrität 9
4.1.4. Verfügbarkeit 9
4.1.5. Least-Priviledge Prinzip (warum sieht nicht jeder alles, warum sind nicht alle Admins?) 9
4.1.6. Need-To-Know-Prinzip (warum Zugriffsbeschränkungen) 9
4.1.7. Nachvollziehbarkeit, Dokumentation 9
4.1.8. Korrektes Verhalten im Notfall 9
4.2. Physische Schutzmaßnahmen 9
4.2.1. Anlagen/Objektschutz 9
4.2.2. Zusperren 9
4.2.3. Clean-Desk-Policy 9
4.3. Informationssicherheits-/IT-Schutzmaßnahmen 9
4.4. Verhaltensregeln, DOs and DON'Ts 10
4.4.1. Weitergabe von Informationen, Umgang mit Datenträgern 10

4.4.2. Situation in Büroräumen, Besprechungsräumen 10
4.4.3. Korrekte Entsorgung von Datenträgern 10
4.4.4. Social Media 10
4.4.5. Social Engineering Angriffe / Fake President Fraud 10
4.4.6. Umgang mit Bürgern, Gästen – Besucherregelungen 11
4.5. Besondere Regeln für den Notfall 11
4.5.1. Datenverlust - Data Breach Notification 11
4.5.2. Schadsoftwarebefall 11
4.5.3. Fehlverhalten von Mitarbeitern 11
5. Modul Grundlegende Verhaltensregeln bei Datenschutzanliegen von Betroffenen 11
5.1. Beschwerden 11
5.2. Informationsrecht 11
5.3. Auskunftsrecht 11
6. Modul Self-Assessment 12
7. Modul Verarbeitungsverzeichnis 12
7.1. Sinn und Zweck 12
7.2. Musterverarbeitungsverzeichnis 12
7.3. Erweiterungen des VVZ 12
7.4. Risikobetrachtung und Datenschutz-Folgenabschätzung 12
8. Modul Maßnahmenumsetzung 13
8.1. Festlegung von Zuständigkeiten/ Verantwortlichkeiten (DSB, Auskunfts-/Meldestelle, …) 13
8.2. Wahrung der Betroffenenrechte im Außenverhältnis 13
8.3. Verträge mit Auftragsdatenverarbeitern 13
8.4. Umsetzung organisatorische und technische Maßnahmen 13
8.4.1. Zugriffskontrolle (Passwörter, Zutritt, Clean-Desk) 14
8.4.2. Schutz vor unautorisierter Datennutzung und Datenverlust (Rollen/Rechte, Verwahrung/Transport/Vernichtung) 14
8.4.3. Endgerätesicherheit (Zugriffsregelung, Benutzerrechte, Virenscanner, …) 14
8.4.4. Firewall/IPS – Schutz Gemeinden/Städtenetz/LAN gegenüber Internet, Gemeinde WLAN, Gäste-WLAN und HotSpots 14
8.4.5. Remotezugriff (VPN) und Fernwartungszugänge 14
8.4.6. Ausfallssicherheit: Sicherungskonzept (Backup/Recovery) 14
8.4.7. E-Mail-Sicherheit 14
8.4.8. Mobilgeräte (Smartphone, Laptop, BYOD) 14
8.4.9. Sonstige Maßnahmen 14

Nutzungsrechte

Den Verantwortlichen des öffentlichen Bereichs iSd § 26 Abs 1 Z 1 DSG idF des DS-AG 2018, dabei insb den Gemeinden und Städten Österreichs, dem Österreichischen Gemeindebund samt Landesverbänden und dem Österreichischen Städtebund samt dessen Landesgruppen, den Gemeindeverbänden, derer sich eine oder mehrere Gemeinde/n zur Besorgung ihrer Aufgaben bedient/bedienen sowie den Dienststellen der öffentlichen Verwaltung des Bundes und der Länder Österreichs, kommt am gegenständlichen Dokument ein umfassendes, zeitlich unbefristetes, Recht zur eigenen Nutzung und Bearbeitung zu. Bedienen sich die obzitierten Verantwortlichen des öffentlichen Bereichs Auftragsverarbeiter iSd Art 4 Z 8 DSGVO zur Erfüllung einzelner Aufgaben, so kommt auch diesen Auftragsverarbeitern am gegenständlichen Dokument ein einfaches Nutzungsrecht zur Erfüllung der übertragenen Aufgaben zu. Eine Weitergabe an Dritte ist untersagt.

Disclaimer

Das gegenständliche Dokument wurde nach bestem Wissen und bester Fachkenntnis erstellt – dafür wird auch gewährleistet. Eine darüberhinausgehende Gewährleistung sowie eine Haftung für Nachteile, die aus leicht fahrlässigem Handeln herrühren, sowie eine Haftung für mittelbare/indirekte Schäden, wird nicht abgegeben. Angaben, die auf Rechtsansichten von Behörden oder allgemein anerkannten Institutionen (im EU-Raum) basieren, sind lege artis; gleiches gilt für mit guten Gründen vertretbare Rechtsansichten, die sich letztlich aber nicht mit künftigen Entscheidungen von Behörden oder Gerichten decken.

1. Vorwort, Verwendungshinweise

Dieses Dokument stellt eine Rahmendefinition (Strukturierung, Vorschläge für Schulungsinhalte) für die Erstellung von detaillierten Schulungsprogrammen für die Mitarbeiter in den österreichischen Gemeinden/Städten sowie bei deren Unternehmen (isb. auch Auftragsverarbeiter) zur korrekten Umsetzung der Vorgaben aus der EU DSGVO und des österreichischen Datenschutzgesetzes, dar.

Da sich die Schulungsinhalte abhängig von der Zielgruppe der Schulungsteilnehmer zu unterscheiden haben, wurde eine Strukturierung der vorgeschlagenen Inhalte in der Form vorgenommen, dass eine Empfehlung für die Mindestinhalte gemäß den Zuständigkeitsbeschreibungen/Rollen aus dem DSGVO-Maßnahmenkatalog und Verarbeitungsverzeichnis angeführt wird. Dazu werden Module definiert, wo einzelne Struktur-/Mindestinhaltsvorgaben beschrieben werden.

In einer Schulungsplanübersicht werden die für die einzelnen Rollen empfohlenen Module zusammengestellt. Wichtig in der Erstellung ist zu beachten, dass die Schulungsinhalte zielgruppenspezifisch zusammengestellt werden, so sollten zB „normale“ Mitarbeiter mit den Grundzügen des Datenschutzes („Warum machen wir das?“) vertraut gemacht werden und sie sollen grundlegende Verhaltensregeln für die tägliche Arbeit verstehen und beherzigen. Es ist aber nicht notwendig, dass diese Mitarbeiter mit einem Verarbeitungsverzeichnis „belastet“ werden oder eine taxative Aufzählung von DSGVO Artikeln vorgetragen bekommen.

Die Module und Schulungsplanübersicht sind eine Mindestempfehlung, die von den einzelnen Schulungsanbietern beliebig ausgestaltet werden können, insbesondere sind weitere Module zu speziellen Anwendungen oder auch Geschäftsprozesse/Verarbeitungen, die zB von Gemeinde-IT-Dienstleistern angeboten werden, sinnvoll, wenn dort spezielle Datenschutzaspekte zu betrachten sind.

Gleiches gilt für spezielle Schulungen zu Spezialthemen, wie z.B. im Bereich technische Realisierungen, Gesundheitswesen, …, die im Einzelfall und projektbezogen sinnvoll sein können.

Hagenberg, im Februar 2018

FH-Prof. DI Robert Kolmhofer
FH-Prof. Mag. Dr. Peter Burgstaller

2. Schulungsplanübersicht

Die für eine Schulung der Mitarbeiter empfohlenen Module werden abhängig von deren Rolle wie nachfolgend angeführt in der Durchführung empfohlen:

2.1. Rolle: Behördenleiter (auch: Geschäftsführer oder Datenschutzbeauftrager von Dienstleister), Bürgermeister

Die Behördenleitung trägt die Gesamtverantwortung für die Implementierung von organisatorischen und technischen Informationssicherheitsmaßnahmen zur Sicherstellung des Schutzes von personenbezogenen Daten der Betroffenen, aber auch anderen vertraulichen Informationen (Verträge, …) und von IKT-Assets der Gemeinden/Städte. Der Behördenleitung obliegt auch die Verantwortung für die Initiierung der notwendigen Maßnahmen, Rollendefinitionen usw., sodass eine umfassende Schulung erforderlich ist.
Aufgrund der Exponiertheit der Bürgermeister (zB gegenüber Medienvertretern, aber auch Bürgern), sollte auch für diese eine umfassende Schulung durchgeführt werden, sodass ein Überblick über alle in einer Gemeinde gesetzten Datenschutz-/Informationssicherheits-maßnahmen, Zuständigkeiten, … besteht.

Empfohlene Module:
Modul Datenschutzgrundlagen
Modul Überblick über die Maßnahmen für Datenschutz und Informationssicherheit
Modul Grundlegende Verhaltensregeln bei Datenschutzanliegen von Betroffenen
Modul Self-Assessment
Modul Verarbeitungsverzeichnis
Modul Maßnahmenumsetzung

2.2. Rolle: IT-Leiter

Der IT-Leiter hat für die Sicherstellung des Datenschutzes in der Gemeinde/Stadt bzw. beim Dienstleister durch Umsetzung von organisatorischen und technischen Informationssicherheitsmaßnahmen zu sorgen, die dem Risiko für die Informationen (z.B. personenbezogene Daten der Betroffenen) oder IT-Assets (IT-Anlagen, Systeme, Serverräume, …) angemessenen Schutz gemäß dem Stand der Technik sorgen.

Empfohlene Module:
Modul Datenschutzgrundlagen
Modul Überblick über die Maßnahmen für Datenschutz und Informationssicherheit
Modul Maßnahmenumsetzung

2.3. Rolle: Mitarbeiter Gemeinde/Stadt

Die Mitarbeiter sind in den Grundzügen des Datenschutzes, vor allem aber im grundsätzlichen Umgang mit den Anliegen der Bürgerinnen und Bürger vertraut zu machen, wenn Sie z.B. mit Beschwerden konfrontiert werden. Im Vordergrund soll das Schaffen eines grundsätzlichen Verständnisses für die umzusetzenden Datenschutz-/Informationssicherheitsmaßnahmen stehen, es ist aber kein Detailwissen erforderlich (wie zB was ist eine Datenschutzfolgeabschätzung, was sind TOMs, was steht in einem Verarbeitungsverzeichnis und wie ist das zu erstellen). Den Mitarbeitern sollen auch die klaren Verhaltensregeln bei zB Beschwerden, Vorfällen, … erörtert werden, und dass sie keine eigenmächtigen Entscheidungen oder Notlösungen treffen sollen, wenn sie dazu nicht ermächtigt sind, sondern dass sie vorgegebene Abläufe und Melde-/Eskalationswege einzuhalten haben.

Empfohlene Module:

- Modul Datenschutzgrundlagen
- Modul Überblick über die Maßnahmen für Datenschutz und Informationssicherheit
- Modul Grundlegende Verhaltensregeln bei Datenschutzanliegen von Betroffenen

2.4. Rolle: Mitarbeiter Dienstleister

Mitarbeiter der Dienstleister der Gemeinden/Städte (z.B. der Auftragsdatenverarbeiter der Gemeinden/Städte) sind in den Grundzügen des Datenschutzes zu unterweisen, und warum die Datenschutzaspekte auch von ihnen zu beachten sind. Da kein direkter Kontakt mit den Bürgern existiert, sind die Wahrung der Betroffenenrechte, usw. nicht von Relevanz.

Empfohlene Module:

- Modul Datenschutzgrundlagen
- Modul Überblick über die Maßnahmen für Datenschutz und Informationssicherheit

3. Modul Datenschutzgrundlagen

In diesem Modul soll ein Überblick über die gesetzlichen Grundlagen des Datenschutzes für Nicht-Juristen gegeben werden, und vor allem ein Verständnis für die Notwendigkeit von Informationssicherheitsmaßnahmen zum Schutz der Daten der Betroffenen (Bürger) geschaffen werden. Selbstverständlich soll auch ein Hinweis darauf gegeben werden, dass es Strafen bei Missachtung geben kann (die aber die Mitarbeiter kaum direkt treffen wird).
Wichtig ist auch zu erklären, dass die Wahrung der Betroffenenrechte nicht von den Mitarbeitern zu verantworten ist, sondern sich diese unbedingt an die definierten Prozesse laut Behördenleitung halten sollen. Ebenso ist es wichtig, dass die Mitarbeiter sich bei Notfällen klar an die Vorgaben halten, und nicht eigenmächtige Entscheidungen oder gut gemeinte Notfallmaßnahmen treffen.
Auf keinen Fall soll ein „Herunterbeten“ von Artikeln der DSGVO erfolgen, es ist auch nicht sinnvoll, zB über Löschfristen oder Details eines Verarbeitungsverzeichnisses, oder auch die zu setzenden Maßnahmen nach Artikel 25 oder 32 aufzuzählen (was in der DSGVO steht, versteht ein Laie nicht, selbst Fachleute können nicht unmittelbar mit den Begriffen ohne nähere Erläuterungen und stundenlangen Erklärungen umgehen).

3.1. Rechtliche Grundlagen (was sind personenbezogene Daten, warum schützen wir die, gesetzliche Rahmenbedingungen, DSG, DSGVO)

3.2. Verarbeitungsgrundsätze

3.3. Betroffenenrechte

3.4. Meldepflichten und Verantwortlichkeiten

4. Modul Überblick über die Maßnahmen für Datenschutz und Informationssicherheit

In diesem Modul soll ein Überblick über die in der Gemeinde/Stadt oder beim Dienstleister aus Sicht der Mitarbeiter wirksamen und sichtbaren und auch umgesetzten Maßnahmen gegeben werden. Der Charakter der Schulung sollte dem einer Informationssicherheitsschulung mit Bezug zu Datenschutz entsprechen und so gestaltet sein, dass auch IT-Laien der Schulung folgen können.
Die Inhalte zu den einzelnen Schulungspunkten können den Umsetzungsempfehlungen aus den Dokumenten Betroffenenrechte sowie Maßnahmenkatalog direkt entnommen werden, und werden daher nachfolgend nicht extra angeführt.

4.1. Warum werden Schutzmaßnahmen getroffen

4.1.1. Grundsätze der Informationssicherheit

4.1.2. Vertraulichkeit

4.1.3. Integrität

4.1.4. Verfügbarkeit

4.1.5. Least-Priviledge Prinzip (warum sieht nicht jeder alles, warum sind nicht alle Admins?)

4.1.6. Need-To-Know-Prinzip (warum Zugriffsbeschränkungen)

4.1.7. Nachvollziehbarkeit, Dokumentation

4.1.8. Korrektes Verhalten im Notfall

4.2. Physische Schutzmaßnahmen

4.2.1. Anlagen/Objektschutz

4.2.2. Zusperren

4.2.3. Clean-Desk-Policy

4.3. Informationssicherheits-/IT-Schutzmaßnahmen

Erläuterung der Maßnahmen, die getroffen werden, jedoch nicht einzelne taxative Aufzählung, sondern es sind einige grundlegende Maßnahmen zu behandeln, die im täglichen Leben eines Mitarbeiters wichtig sind (siehe dazu auch die vorgeschlagene Reihenfolge der umzusetzenden Maßnahmen in 8.4 Umsetzung organisatorische und technische Maßnahmen)
Welche Maßnahmen gibt es zB zu den Bereichen:

- Zugriffskontrolle (Passwörter, Zutritt, Clean-Desk)
- Schutz vor unautorisierter Datennutzung und Datenverlust (Rollen/Rechte, Verwahrung/Transport/Vernichtung)
- Endgerätesicherheit (Zugriffsregelung, Benutzerrechte, Virenscanner, …)
- Internetschutz (warum dürfen nicht alle alles im Internet, was macht dazu eine Firewall, warum gibt es eine Trennung des Gemeinde-/Städtenetzes/LAN gegenüber Internet)
- Remotezugriff (VPN) und Fernwartungszugänge
- Warum macht man eine Datensicherung und speichert nichts auf lokalen Arbeitsplätzen, wenn es wichtig ist (Sicherungskonzept, Backup/Recovery)
- E-Mail-Sicherheit
- Mobilgeräte (Smartphone, Laptop, BYOD)

4.4. Verhaltensregeln, DOs and DON'Ts

4.4.1. Weitergabe von Informationen, Umgang mit Datenträgern

In diesem Schulungsteil soll mit Nachdruck darauf hingewiesen werden, dass keine Informationen ohne Genehmigung/Ermächtigung weitergegeben werden dürfen (weder mündlich noch schriftlich noch elektronisch via E-Mail oder zB USB-Sticks). Es ist auch zu schulen, dass auf internen IT-Geräten keine Fremddatenträger (USB Sticks von Besuchern, …) angeschlossen werden dürfen (um direkten Schadsoftwarebefall möglichst auszuschließen), sondern dass elektronische Dokumente nur über die offiziell freigegebenen Kommunikationswege entgegengenommen werden dürfen. Auch ist der Umgang mit „Werbegeschenken" in Form von zB USB-Sticks, CD-Roms mit Demoprogrammen usw zu schulen (Verwendung/Einsatz ist nicht zulässig).

4.4.2. Situation in Büroräumen, Besprechungsräumen

Hier sollten grundlegende Verhaltensregeln für Büroräume der Mitarbeiter (keine Besucher alleine, Bildschirmsperre beim Verlassen des Raums, der letzte dreht das Licht ab und sperrt zu) sowie Besprechungsräume (beim Verlassen sind keine Unterlagen zurück zu lassen, Flipchartbögen mitnehmen, Tafeln löschen, keine vertraulichen Unterlagen in den Mistkübel, …) geschult werden.

4.4.3. Korrekte Entsorgung von Datenträgern

Es muss ein Verständnis dafür geschaffen werden, dass die korrekte Entsorgung von Informationsträgern (Papier, Datenträger, USB-Sticks,…) wichtig ist. zB gehört die Altpapierkiste unter dem Schreibtisch verbannt, Sammelcontainer bzw. Aktenvernichter für die datenschutzrechtlich relevanten Papierdokumente verwendet, kritische Datenträger bis zur korrekten (sicheren) Vernichtung zugriffs-/entwendungssicher gelagert.

4.4.4. Social Media

Es sollte eine kurze Schulung für den Umgang mit Social Media erfolgen. Dazu gehört zB, dass persönliche Meinungsäußerungen von Mitarbeitern über den Arbeitgeber/Gemeinde nur von den autorisierten Stellen (Behördenleitung, Presseverantwortlicher) zulässig sind. Und es ist auch auf das Verbot der Nutzung von diversen Apps, die datenschutzrechtlich nicht zulässig sind, hinzuweisen. Auch die Verwendung von Bildern mit Personen auf Webseiten/facebook/instagram ist zu behandeln.

4.4.5. Social Engineering Angriffe / Fake President Fraud

Es sollte eine grundsätzliche Erläuterung erfolgen, wobei es sich bei Social Engineering Angriffen handelt, wo möglich mit zB Screenshots. Mindestens behandelt werden sollten: dubiose Anrufe mit Auskunftsbegehren, E-Mail Anfragen (bis hin zu Phishing Mails) sowie auch Fake President Fraud Angriffe. Zu behandeln ist auch, wie mit derartigen (oft gut getarnten) Angriffen umzugehen ist, wie zB Rückrufen des Chefs, Verweisen der Anrufer an die korrekten Beschwerde-/Auskunftswege, Ignorieren/Löschen von E-Mails, Eskalation zur Fachabteilung, Rückversichern beim zuständigen Behördenleiter/IT-Helpdesk/…

4.4.6. Umgang mit Bürgern, Gästen – Besucherregelungen

Hier sollte der Umgang mit „Externen“ behandelt werden, dass zB diese Personen keinen Einblick in fremde Unterlagen erhalten, nicht alleine in Räumen mit schutzwürdigen Daten ohne Aufsicht verbleiben, … Auch sollten die Mitarbeiter dazu motiviert werden, „herumirrende oder suchende Gäste“ aktiv anzusprechen, um sie richtig zu „leiten“.

4.5. Besondere Regeln für den Notfall

4.5.1. Datenverlust - Data Breach Notification

Was tun, wenn einem personenbezogene Daten abhandengekommen sind (gelöscht, unabsichtlich verloren, an falsche Person/Firma übermittelt) oder man den Verdacht hat, dass die Gemeinde „gehackt“ wurde?

4.5.2. Schadsoftwarebefall

Was tun, wenn der Virenscanner am PC „Alarm schreit“?

4.5.3. Fehlverhalten von Mitarbeitern

Hier sollte erläutert werden, an wen man sich wenden kann, wenn zB ein Fehlverhalten von Arbeitskollegen beobachtet wird oder es Probleme mit Mitarbeitern von externen Firmen gibt.

5. Modul Grundlegende Verhaltensregeln bei Datenschutzanliegen von Betroffenen

In diesem Modul sollen die grundlegenden Verhaltensregeln für die Mitarbeiter für die in der Gemeinde/Stadt festgelegten Prozesse zur Abhandlung von Betroffenenanliegen im Bereich Datenschutz sowie die einzuhaltenden Abläufe und Meldepflichten geschult werden. Neben klaren Verhaltensregeln soll auch Bewusstsein dafür geschaffen werden, dass eigenmächtige Lösungen falsch sind, sondern die korrekten Melde- und Eskalationswege einzuhalten sind.

5.1. Beschwerden

5.2. Informationsrecht

5.3. Auskunftsrecht

6. Modul Self-Assessment

In diesem Modul wird die Durchführung des Self-Assessments zur Positionsbestimmung der Gemeinde/Stadt behandelt. Es soll die Abarbeitung des Self-Assessment-Fragenkatalogs anhand eines Beispiels besprochen werden, sodass die Schulungsteilnehmer erkennen können, ob in der eigenen Gemeinde/Stadt mit der Umsetzung der Standard-Dokumente (Verarbeitungen laut Muster Verarbeitungsverzeichnis, Muster Maßnahmenkatalog, Muster Betroffenenrechte) das Auslangen gefunden werden kann, oder ob aufgrund der speziellen Gegebenheiten zusätzliche Erhebungen/Analysen/Schritte erforderlich sind, weil zB Verarbeitungen existieren, die im Standard Verarbeitungsverzeichnis nicht enthalten sind.
Grundsätzlich ist dabei davon auszugehen, dass für die Gemeinden/Städte, die von einem Gemeinde- IT-Dienstleister vollständig serviciert werden (die Anwendungen von dort beziehen, selbst keine eigenen Server/Anwendungen betreiben), zur Abdeckung der wichtigsten Auflagen aus der DSGVO mit den Musterdokumenten in vielen Fällen das Auslangen gefunden werden kann.
Bei Gemeinden/Städte mit eigenem IT-Betrieb, besonderen Einrichtungen im Eigentum der Gemeinde/Stadt (wo zB Gesundheitsdaten verarbeitet werden), sollte im Rahmen der Schulung für dieses Modul explizit darauf hingewiesen werden, dass eine detaillierte Betrachtung mit Expertenbegleitung erfolgen muss, da mit großer Wahrscheinlichkeit die Mustermaßnahmen nicht ausreichend sein werden.

7. Modul Verarbeitungsverzeichnis

In diesem Modul wird die rechtliche Grundlage für den Zwang zum Führen eines Verarbeitungsverzeichnisses, die Struktur des Musterverarbeitungsverzeichnisses (Inhalte, Datenkategorien, Empfänger, Schutzmaßnahmen,…) und wie das Musterverarbeitungsverzeichnis für die eigenen Zwecke erweitert werden kann (und muss) behandelt. Auch die Durchführung der Risikobetrachtung und der daraus möglicherweise resultierenden Datenschutzfolgeabschätzung ist zu behandeln.
Für die detaillierten Inhalte wird auf das Musterverarbeitungsverzeichnis und dessen Anhänge mit Arbeitsbehelfen verwiesen.

7.1. Sinn und Zweck

7.2. Musterverarbeitungsverzeichnis

7.3. Erweiterungen des VVZ

7.4. Risikobetrachtung und Datenschutz-Folgenabschätzung

8. Modul Maßnahmenumsetzung

In diesem Modul sind die notwendigen einzelnen Schritte der Maßnahmenumsetzungen zu behandeln, die von Seite der Gemeinde/Stadt oder auch der Dienstleister durchzuführen sind. Es ist explizit darauf hinzuweisen, dass abhängig vom konkreten Fall in der Gemeinde/Stadt oder beim Dienstleister auch die nicht im Weiteren taxativ aufgezählten, aber zB im Maßnahmenkatalog enthaltenen Empfehlungen/Maßnahmen/…, zu betrachten und bei Bedarf umzusetzen sind.

8.1. Festlegung von Zuständigkeiten/ Verantwortlichkeiten (DSB, Auskunfts-/Meldestelle, …)

In diesem Teil wird behandelt, welche Festlegungen in der Gemeinde/Stadt auf Basis der zur Verfügung gestellten Musterdokumente/Musterbausteine im Außenverhältnis zu den Bürgern, der Datenschutzbehörde, … zu treffen sind.

8.2. Wahrung der Betroffenenrechte im Außenverhältnis

In diesem Teil der Schulung ist zu behandeln, wie die Mindestprozesse auf Gemeinde-/Stadtseite zur Wahrung der Betroffenenrechte umzusetzen sind. Die Inhalte sind dem Musterdokument für Betroffenenrechte zu entnehmen.

8.3. Verträge mit Auftragsdatenverarbeitern

In diesem Schulungsteil ist darauf einzugehen, dass die Verträge mit Auftragsdatenverarbeitern dahingehend zu prüfen sind, dass die Gemeinde/Stadt die Betroffenenrechte wahren kann. Insbesondere ist die Verpflichtung der Auftragsverarbeiter zur Einhaltung der Datenschutzgrundsätze, der Meldepflichten und der Mitwirkungspflichten sicherzustellen.

8.4. Umsetzung organisatorische und technische Maßnahmen

Für diesen Schulungsteil wird empfohlen, die unten stehenden Maßnahmenkatalog-Bausteine im Detail zu betrachten, und auch die zugehörigen Arbeitsbehelfe anhand von Ausfüllbeispielen zu erläutern. Die Reihenfolge der unten angeführten Maßnahmenschulung entspricht dabei auch einer möglichen Umsetzungsreihenfolge der Maßnahmen in der Gemeinde/Stadt bzw. beim Dienstleister. Es soll jedoch darauf explizit hingewiesen werden, dass aufgrund der vorhandenen IKT-Systeme, Verarbeitungen, Dienstleister eine andere Reihung oder sogar explizit ein Vorziehen von Maßnahmen, die nicht explizit angeführt sind, vorzunehmen ist.

8.4.1. Zugriffskontrolle (Passwörter, Zutritt, Clean-Desk)

8.4.2. Schutz vor unautorisierter Datennutzung und Datenverlust (Rollen/Rechte, Verwahrung/Transport/Vernichtung)

8.4.3. Endgerätesicherheit (Zugriffsregelung, Benutzerrechte, Virenscanner, …)

8.4.4. Firewall/IPS – Schutz Gemeinden/Städtenetz/LAN gegenüber Internet, Gemeinde WLAN, Gäste-WLAN und HotSpots

8.4.5. Remotezugriff (VPN) und Fernwartungszugänge

8.4.6. Ausfallssicherheit: Sicherungskonzept (Backup/Recovery)

8.4.7. E-Mail-Sicherheit

8.4.8. Mobilgeräte (Smartphone, Laptop, BYOD)

8.4.9. Sonstige Maßnahmen