I.

DSGVO Self-Assessment Fragenkatalog

für Österreichs Gemeinden/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 1.2

Stand 25.03.2018

Inhaltsverzeichnis

Nutzungsrechte

Disclaimer

1. Hinweise zur Nutzung

Die vorliegenden Dokumente und Arbeitsbehelfe sollen es den Österreichischen Städten und Gemeinden ermöglichen, in strukturierten und angeleiteten Schritten, die für die Umsetzung von Datenschutzmaßnahmen erforderlichen organisatorischen und technischen Maßnahmen mit möglichst geringem Aufwand umzusetzen, um die Vorgaben aus dem ab Mai 2018 geltenden neuen Datenschutzrecht auf Basis der EU Datenschutzgrundverordnung (DSGVO) zu erfüllen.

Die Arbeitsbehelfe wurden dazu in der Reihenfolge der empfohlenen Bearbeitung in nachfolgende Teile gegliedert und entsprechend der Reihenfolge der Durchführung nummeriert:

I. DSGVO Self-Assessment Fragenkatalog (diese Dokument)
Ausgehend vom Self-Assessment Fragenkatalog wird in strukturierten Schritten eine Anleitung zur Prüfung der Anwendbarkeit der Musterdokumente und allfällig notwendiger zusätzlicher Bearbeitungsschritte/Ergänzungen gegeben. Im Zuge der Bearbeitung des Self-Assessments wird das für die Gemeinde/Stadt erforderliche Verarbeitungsverzeichnis ausgehend vom zur Verfügung gestellten Muster Verarbeitungsverzeichnis erstellt und bei Bedarf individuell erweitert. Die bei den einzelnen Verarbeitungen vorausgewählten technischen und organisatorischen Informationssicherheitsmaßnahmen (TOMs) entsprechen dabei der Gliederung im DSGVO-Maßnahmenkatalog, wo konkrete Umsetzungsempfehlungen gegeben werden.

II. Leitfaden Betroffenenrechte

Zur Sicherstellung der korrekten Behandlung der Betroffenenrechte (zB Auskunftsbegehren, Löschanträge, …von Betroffenen), ist in einem zweiten Schritt die Umsetzung gemäß Leitfaden Betroffenenrechte durchzuführen.

III. DSGVO Maßnahmenkatalog

Die zur Erfüllung der Vorgaben aus dem Datenschutzgesetzt/DSGVO empfohlenen organisatorischen und technischen Informationssicherheits-/IT-Security-Maßnahmen nach Stand der Technik sind im DSGVO Maßnahmenkatalog in Form von direkten Umsetzungsbeschreibungen mit Arbeitsbehelfen enthalten. Um die Notwendigkeit/Anwendbarkeit der einzelnen Maßnahmen nachvollziehbar zu dokumentieren, ist mithilfe einer Checkliste jede Maßnahme zu prüfen und das Prüfungsergebnis zu vermerken.

IV. DSGVO-Schulungskonzept

Für die Erstellung von Schulungsprogrammen (sei es durch die Gemeinde/Stadt selbst oder auch für externe Dienstleister) sind im „DSGVO-Schulungskonzept“ Empfehlungen für die Entwicklung von Schulungsprogrammen im Kontext Datenschutz für unterschiedliche Zielgruppen in den Gemeinden enthalten.

Hagenberg, 28.02.2018

FH-Prof. DI Robert Kolmhofer
FH-Prof. Mag. Dr. Peter Burgstaller, LL.M. (London)

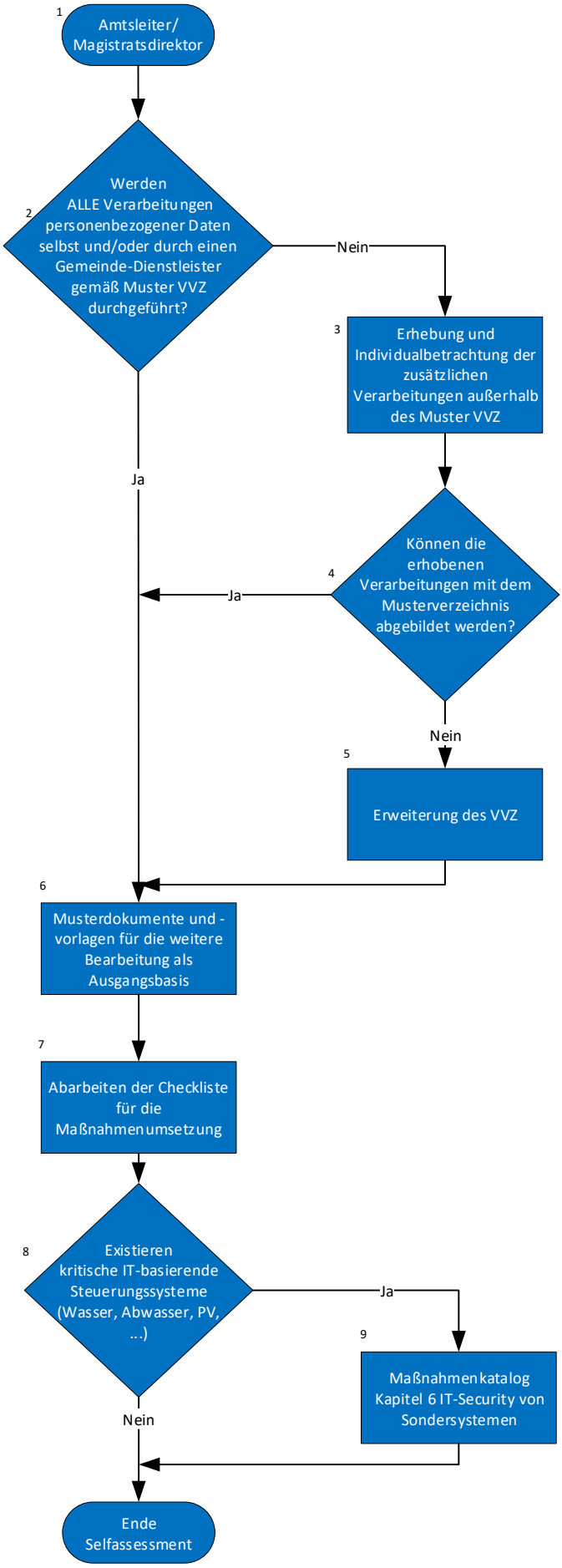
2. Self-Assessment Prozess

Mit Hilfe des Self-Assessment Fragebogens kann eine Gemeinde/Stadt in Schnellform ermitteln, ob die verfügbaren Musterdokumente zur Umsetzung der neuen Datenschutzbestimmungen inkl. zur Erstellung eines Verarbeitungsverzeichnisses angewendet werden können, oder ob zusätzliche ergänzende Betrachtungen oder eine Individualbetrachtung der Verarbeitungen erforderlich ist.

Dazu wurde dieser Self-Assessment-Prozess entwickelt, der auf Basis des nachfolgend erläuterten Entscheidungsbaumes mittels Kontrollfragen eine Beurteilung der weiteren Vorgehensweise und Anwendbarkeit der Musterdokumente erlaubt. Der Entscheidungsbaum ist als getrenntes Prozessdokument bei den Arbeitsbehelfen (Visio, PDF) beigelegt.

Der Self-Assessment Prozess ist in einfach strukturierte Bearbeitungsschritte, die im Entscheidungsbaum in der empfohlenen Reihenfolge der Bearbeitung nummeriert sind, gegliedert.

Die Beantwortung der einzelnen Kontrollfragen sind vom Amtsleiter/Magistratsdirektor als Nachweis für die jeweilige Entscheidung samt den dafür herangezogenen Grundlagen/Informationen zu dokumentieren. Im Anhang befindet sich dazu ein Muster-Formular.


1
Amtsleiter/ Magistratsdirektor
2
Werden ALLE Verarbeitungen personenbezogener Daten selbst und/oder durch einen Gemeinde-Dienstleister gemäß Muster VVZ durchgeführt?
Nein
3
Erhebung und Individualbetrachtung der zusätzlichen Verarbeitungen außerhalb des Muster VVZ
Ja
4
Können die erhobenen Verarbeitungen mit dem Musterverzeichnis abgebildet werden?
Ja
Nein
5
Erweiterung des VVZ
6
Musterdokumente und -vorlagen für die weitere Bearbeitung als Ausgangsbasis
7
Abarbeiten der Checkliste für die Maßnahmenumsetzung
8
Existieren kritische IT-basierende Steuerungssysteme (Wasser, Abwasser, PV, ...)
Ja
9
Maßnahmenkatalog Kapitel 6 IT-Security von Sondersystemen
Nein
Ende Selfassessment

3. Abarbeitung Self-Assessment

Nachfolgend sind die einzelnen Elemente des Entscheidungsbaumes mittels Nummerierung zugeordnet und erläutert. Die Abarbeitung des Prozesses ist gemäß der Nummerierung der einzelnen Elemente im Prozessablaufdiagramm vorzunehmen.

Die einzelnen Prozessschritte sind wie folgt:

1. Amtsleiter/Magistratsdirektor

Die Beantwortung der Self-Assessment Fragenkaskade hat durch den Amtsleiter/Magistratsdirektor zu erfolgen und die Entscheidungen sind mit Begründungen zu dokumentieren (siehe Formular im Anhang).

2. Werden ALLE Verarbeitungen personenbezogener Daten selbst und/oder durch einen Gemeinde-Dienstleister gemäß Muster VVZ durchgeführt?

In der initialen Frage erfolgt die grundsätzliche Entscheidung, ob die Gemeinde/Stadt ihre Verarbeitungen personenbezogener Daten gemäß den im Muster Verarbeitungsverzeichnis (Muster VVZ) enthaltenen Verarbeitungen (Vorlagen) durchführt. Dabei ist es irrelevant, ob die Verarbeitungen selbst betrieben werden oder bei einem externen Dienstleister, welcher auf die Prozesse einer Gemeinde/Stadt spezialisiert ist (z.B. Gemdat OÖ, Gemdat NÖ, Gemeindeinformatik GmbH, Kufgem, PSC, Kommunalnet, Comm-Unity EDV GmbH, …).

Um die Vollständigkeit des Verarbeitungsverzeichnisses (VVZ) sowie die Verwendung der Musterdokumente gewährleisten zu können, ist ein Vergleich der vorhandenen Verarbeitungen in der Gemeinde/Stadt zu den Verarbeitungen aus den Muster-Verarbeitungsverzeichnis durchzuführen, um zusätzliche lokale Verarbeitung zu identifizieren. Eine zusätzliche lokale Verarbeitung ist beispielsweise der Export von Daten in (Excel-) Tabellen, welche für individuelle Gemeindetätigkeiten oder für die Weitergabe an Vereine verwendet werden.

Sollte sich herausstellen, dass ALLE eigenen Verarbeitungen dem Muster VVZ entsprechen, ist die Frage mit „Ja“ zu beantworten.

Die Entscheidung, ob die Musterdokumente verwendet werden können oder ob eine Individualbetrachtung erforderlich ist, ist mit einer Begründung im Formular (siehe Anhang) zu dokumentieren.

3. Erhebung und Individualbetrachtung der zusätzlichen Verarbeitungen außerhalb des Muster VVZ

Da die in der Gemeinde/Stadt vorhandenen Verarbeitungen personenbezogener Daten nicht zur Gänze einfach durch das Muster VVZ abgebildet werden, ist eine Erhebung der zusätzlichen, nicht im Muster VVZ enthaltenen Verarbeitungen durchzuführen.

Zusätzliche oder abweichende Verarbeitungen sind mit der Bezeichnung/Name der Verarbeitungstätigkeit im Formular (siehe Anhang) zu dokumentieren.

4. Können die erhobenen Verarbeitungen mit dem Musterverzeichnis abgebildet werden?

In diesem Schritt ist zu prüfen, ob die zusätzlich erhobenen Verarbeitungen mit den im Musterverzeichnis vorhandenen Verarbeitungen abgebildet werden können. Für eine Beurteilung müssen die erhobenen zusätzlichen Verarbeitungen mit dem Muster-Verarbeitungsverzeichnis verglichen werden.

Ist eine Übereinstimmung der Verarbeitungen mit den Verarbeitungen in den Musterdokumenten gegeben, kann die Frage mit „Ja“ beantwortet werden und es können die Musterdokumente für die weitere Bearbeitung bzw. für die Erstellung des Verarbeitungsverzeichnisses verwendet werden. Die Zuordnung der zusätzlichen lokalen Verarbeitung zu der Verarbeitung im Musterverzeichnis ist zu dokumentieren (siehe Formular im Anhang). Im Musterverzeichnis sind die für die einzelnen Verarbeitungen erforderlichen umzusetzenden technischen und organisatorischen Maßnahmen (TOMs) im jeweiligen Abschnitt „Kurze Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen“ bereits vorausgewählt. Diese vorausgewählten Maßnahmen entsprechen der Kapitelgliederung im Dokument „III.DSGVO-Maßnahmenkatalog“, wo für die einzelnen Maßnahmenkategorien die detaillierte Maßnahmenbeschreibung samt Umsetzungsempfehlungen angeführt sind.

Sind zusätzliche Verarbeitungen oder Abweichungen bei einzelnen Verarbeitungen aus den Musterdokumenten vorhanden, ist die Frage mit „Nein“ zu beantworten und Erweiterung des Muster VVZ um die zusätzlichen Verarbeitungen durchzuführen (nächster Schritt):

Die Entscheidung, ob die Musterdokumente verwendet werden können oder ob eine Individualbetrachtung erforderlich ist, ist mit einer Begründung im Formular (siehe Anhang) zu dokumentieren.

5. Erweiterung des VVZ

Da in der Gemeinde/Stadt eigene und/oder zusätzliche Verarbeitungen zu den im Muster VVZ enthaltenen Verarbeitungen durchgeführt werden, ist eine Individualbetrachtung der einzelnen Verarbeitungen erforderlich.

Bei der Individualbetrachtung ist in einem ersten Schritt zu prüfen, ob die Verarbeitungen Übereinstimmungen mit Verarbeitungen im Muster VVZ aufweisen. Ist dies der Fall, können für die zusätzlichen Verarbeitungen aufbauend auf den Muster VVZ Vorlagen individuelle Erweiterungen vorgenommen werden.

Ist keine Verarbeitung aus den Musterdokumenten mit der vorliegenden Verarbeitung vergleichbar, muss eine neue Verarbeitung gemäß der Vorlage aus dem Muster-Verarbeitungsverzeichnis erstellt und zum Verarbeitungsverzeichnis der Gemeinde/Stadt hinzugefügt werden. Zusätzlich ist auch zu prüfen, ob weitere Maßnahmen aus dem Bereich Datenschutz-/Informationssicherheit umzusetzen sind.

6. Musterdokumente und -vorlagen Betroffenenrechte

Nach Fertigstellung des Verarbeitungsverzeichnisses (falls erforderlich mit Erweiterungen) sind ausgehend von den Musterdokumenten und -vorlagen für die Betroffenenrechte die dort angeführten Prüf- und Dokumentationsschritte durchzuführen.

7. Abarbeiten der Checkliste für die Maßnahmenumsetzung

Zur Sicherstellung der Sicherheit von personenbezogenen Informationen sind organisatorische und technische Informationssicherheits-/IT-Security-Maßnahmen gemäß Maßnahmenkatalog in der Gemeinde/Stadt umzusetzen. Da nicht alle Maßnahmen gleichermaßen im Einzelfall zutreffen, ist anhand der „DSGVO-Maßnahmenkatalog-Checkliste 0.1.xlsx“ für jede einzelne Maßnahme zu bewerten, ob die Maßnahme überhaupt erforderlich ist und wenn ja, ob schon eine Umsetzung in der Gemeinde/Stadt existiert, teilweise existiert oder erst eine Umsetzung durchzuführen ist. In der Tabelle ist auch die entsprechende Dokumentation der Abarbeitung/Begründungen/… durchzuführen, um die Nachvollziehbarkeit sicherzustellen. Die Gliederung des Maßnahmenkatalogs entspricht dabei den im Musterverarbeitungsverzeichnis angeführten und bei jeder Verarbeitung bereits vorausgewählten technischen und organisatorischen Maßnahmen (TOMs), sodass für jede Verarbeitung im Einzelnen die jeweils erforderlichen Maßnahmen zur Sicherstellung von Datenschutz und Informationssicherheit ermittelt werden können.

8. Existieren kritische IT-basierende Steuerungssysteme (Wasser, Abwasser, PV, ...)[1]

Falls von der Gemeinde/Stadt IT-basierende Steuerungssysteme eingesetzt werden, deren Störung/Ausfall Auswirkungen auf zB die Bevölkerung haben kann, so sind diese Systeme einer Prüfung hinsichtlich IT-Security zu unterziehen.

Die Erhebung der kritischen Steuerungssysteme ist zu dokumentieren (siehe Muster im Anhang).

9. Maßnahmenkatalog Kapitel 6 IT-Security von Sondersystemen

Zur automatisierten Steuerung von Infrastruktur werden vermehrt Industrielle Steuerungssysteme (Industrial Control Systems, ICS) bzw. Steuerungs- und Überwachungssysteme (Supervisory Control And Data Acquisition, SCADA) in unterschiedlichsten Bereichen eingesetzt. Beispiele dafür sind im Bereich der Ver-/Entsorgungsinfrastruktur die Bereiche Trinkwasserversorgung, Abwasserentsorgung (Steuerung von Pumpwerken, Kläranlagen), Photovoltaik-Systeme, Ortsnah- und Fernwärmesysteme, Heizungs- und Solaranlagensteuerungen.

[1] *Dieser Prüfungsteil steht zwar nicht in unmittelbarem Zusammenhang mit den Vorgaben aus der DSGVO, jedoch ist aufgrund einer möglichen Verbindung von zB DSGVO-relevanten IT-Komponenten und den Steuerungssystemen eine zeitgleiche Betrachtung und Maßnahmenumsetzung sinnvoll. Weiters kann aufgrund der EU NIS-Richtlinie, die ab Mai 2018 national durch die Gesetzgebung umgesetzt werden muss, eine gesetzliche Verpflichtung bzw. Notwendigkeit zur Absicherung kritischer Infrastrukturen (Trinkwasser, Energieversorgung, Gesundheitsbereich, …) gegen „Cyberattacken“ entstehen.*

Durch die vermehrte Verbindung der Steuerungssysteme mit dem Internet für eine Fernsteuerung, Fernüberwachung, Handy-App-Zugriff und auch Fernwartung, sind diese Systeme den gleichen Gefahren, wie auch „normale“ Office-IT-Anwendungen ausgesetzt.

Im Maßnahmenkatalog sind für derartige „Sondersysteme“ empfohlene Schritte für eine Analyse/Prüfung/Absicherung von Sondersystemen exemplarisch angeführt. Aufgrund der Komplexität der Systeme wird eine Behandlung dieser Systeme mit Expertenbegleitung empfohlen.

4. Anhang – Muster-Formular

Amtsleiter/Magistratsdirektor:
Nachname Vorname

_____ _____

Self-Assessment durchgeführt am: _____

Werden ALLE Verarbeitungen personenbezogener Daten selbst und/oder durch einen Gemeinde-Dienstleister gemäß Muster VVZ durchgeführt?	Ja ☐	Nein ☐
Dokumentation der Entscheidung		

Zusätzliche Verarbeitungen außerhalb des Muster VVZ	Ja ☐	Nein ☐
Auflistung der zusätzlichen Verarbeitungen (Name/Bezeichnung) • _____ • _____ • _____ • _____		

Können die erhobenen Verarbeitungen mit dem Musterverzeichnis abgebildet werden?	Ja ☐	Nein ☐

Zuordnung der zusätzlichen Verarbeitung mit Muster-Verarbeitung

Zusätzliche Verarbeitung	*Musterverarbeitung*
_____	_____
_____	_____
_____	_____

Falls erforderlich: Erweiterung des Verarbeitungsverzeichnisses um individuelle Verarbeitungen abgeschlossen?	Ja ☐	Nein ☐

Dokumentation

Musterdokumente und -vorlagen Betroffenenrechte abgearbeitet?	Ja ☐	Nein ☐

Dokumentation

Checkliste für die Maßnahmenumsetzung abgearbeitet?	Ja ☐	Nein ☐

Dokumentation

Existieren kritische IT-basierende Steuerungssysteme (Wasser, Abwasser, PV, ...)	Ja ☐	Nein ☐
Auflistung der kritischen Steuerungssysteme (Name/Bezeichnung) • _____ • _____ • _____ • _____		

Maßnahmen für Sondersysteme abgearbeitet?	Ja ☐	Nein ☐
Dokumentation		

_____

Datum, Unterschrift