



DSG/DSGVO/NIS-RL

Best-Practice-Maßnahmenkatalog & Self-Assessment für Gemeinden

FH-Prof. DI Robert Kolmhofer

- Projektgenese
 - Projektinhalte und –ziele
 - Projektstruktur und Zeitplan
 - Projektorganisation und Team
- Projektergebnis
 - I Self-Assessment und Muster Verarbeitungsverzeichnis
 - II Betroffenen Rechte
 - III DSGVO Maßnahmenkatalog
 - IV Schulungskonzept

- 80. FIT Graz 27.1.2017
 - Vortrag „DSGVO Stand der Technik und Stand der Dinge“
- Follow-Up Gespräche mit
 - OÖ Gemeindebund, gemdat, Kremsmünster
 - Idee: Assessment für Gemeinden um DSGVO konform zu werden, Umsetzungs-/Maßnahmenkatalog
 - Einfache Handhabung (auch für nicht DSB)
 - Erweiterung um NIS-RL (Trinkwasserversorgung)
 - Städtebund
 - Bundeskanzleramt (R. Ledinger)
- Entwicklung F&E Projekt

Projekthalte und -ziele



- Self Assessment Methode für Gemeinden
 - Einfache Methodik für Positionsbestimmung der Gemeinden hinsichtlich
 - DSG/DSGVO Auflagen
 - Wenn vorhanden: Betrieb wesentlicher Dienster
 - Informationsverarbeitungssysteme, IT-Assets
 - Anwendbarkeit von
 - Muster Verarbeitungsverzeichnis und Betroffenenrechte
 - Best-Practice-Maßnahmenkatalog
 - Ev. notwendige Individual-Analyse

Projekthinhalte und -ziele



- Entwicklung Maßnahmenkatalog für Datenschutz-/Informationssicherheit
 - Standardisiert für alle Gemeinden (mit/ohne eigenem Systembetrieb, groß/klein, mit/ohne BwD)
 - Einbeziehung der IT-Dienstleister (zB gemdat)
 - Einfach und aufwandsoptimiert umsetzbar, risikoadäquat
 - Best-Practice Anleitungen/Vorgaben, kompatibel zu
 - Ö Informationssicherheitshandbuch (Subset ISO27001)
 - BSI Grundschutzkataloge
 - Normen, Stand der Technik, ...
 - Abdeckung DSGneu/DSGVO/NIS-RL(NISG)
- Entwicklung Inhaltsstruktur für Schulungsprogramm

Projektstruktur und Zeitplan



- Projektphase 1 (Oktober/November 2017)
 - Analyse von 2 Gemeinden (mit/ohne eigenem Anwendungsbetrieb) und Dienstleister nach DSGVO/DSG/NIS-RL/Informationssicherheit/Stand der Technik
 - Erfassung Verarbeitungen, Daten, Systeme, ...
 - Ableitung des „Standardfalls“ für Maßnahmen im Best-Practice-Katalog
 - Erstellen „Verzeichnis von Verarbeitungstätigkeiten“ (§49 DSG) für „Standard Anwendungen“, Dienstleister-Anwendungen, eigene Anwendungen

Projektstruktur und Zeitplan



- Projektphase 2 (Oktober-Dezember 2017, Finalisierung Februar 2018)
 - Entwicklung Best-Practice Maßnahmenkatalog
 - Organisatorische Maßnahmen (Zuständigkeiten, Prozesse, Risikoanalyse, Notfallmanagement, ...)
 - Technische Maßnahmen (Zugangskontrolle, Rechtevergabe, Systemschutz, Vernichtung/Löschung, ...)
 - Einfache Anwendbarkeit (nicht überborden, „Standardschutz“ um DSGVO/DSG grundsätzlich zu erfüllen)
 - Für Nicht-IT Fachleute

Projektstruktur und Zeitplan



- Projektphase 3 (Jänner 2018)
 - Entwicklung Struktur und Inhalte Trainingsprogramm
 - „Userschulung“ für Gemeinden
 - Anwendung Self-Assessment
 - Anwendung Best-Practice Maßnahmenkatalog

- Finanzierung
 - Bundeskanzleramt, Städtebund, Gemeindebund

Projektorganisation und Team

DANKE für die
Zusammenarbeit!

■ Projektteam

- FH OÖ F&E Hagenberg, Sichere Informationssysteme
 - Prof. Robert Kolmhofer (technisch, Projektleitung)
 - Prof. Peter Burgstaller (legal, compliance)
 - 2 wiss. Mitarbeiter (Christoph Sonnberger, Christoph Keplinger)
- Städtebund
 - Johannes Eschenbacher, Ronald Sallmann, Gerd Soritz
- Gemeindebund
 - Bernhard Haubenberger, Daniel Holzer
- Externe Beratung
 - Alexander Leitner (ISO 27001 Lead Auditor)
 - Karin Neußl (zertifizierte DSB), Simone Krammer
- Gemeinden für Assessment
 - Gemeinde Kremsmünster: Wolfgang Jankulik
 - Gemeinde Pettenbach: Thomas Zehetner

- Gliederung der Arbeitsbehelfe/Unterlagen/Musterdokumente
 - I Self-Assessment und Muster Verarbeitungsverzeichnis
 - Prozess für Self-Assessment mit Entscheidungsbaum und Checkliste
 - Musterverarbeitungsverzeichnis für Gemeinden
 - II Betroffenen Rechte
 - Erörterung der Betroffenenrechte, Bearbeitungsprozesse, Minimalanforderungen an erforderlichen Daten
 - III DSGVO Maßnahmenkatalog
 - Organisatorische und technische Informationssicherheitsmaßnahmen, Checkliste
 - Ergänzende Dokumente
 - IV Schulungskonzept

I. Self-Assessment und Muster Verarbeitungsverzeichnis

- Prozess für Self-Assessment mit Entscheidungsbaum und Checkliste
- Check, ob das Muster Verarbeitungsverzeichnis und die anderen Vorlagendokumente verwendet werden können, oder ob individuelle Erweiterung/Betrachtung erforderlich ist
- Musterformular als Hilfsmittel für die Abarbeitung und zur Dokumentation der Bearbeitung

4. Anhang – Muster-Formular

Anteilnehmer/Magistratsdirektor:
Nachname: _____ Vorname: _____

Self-Assessment durchgeführt am: _____

Wurden 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:
Auflistung der zusätzlichen Verarbeitungen (Name/Bezeichnung):

- _____
- _____
- _____

Seite 9

6. Musterdokumente und -vorlagen Betroffenrechte

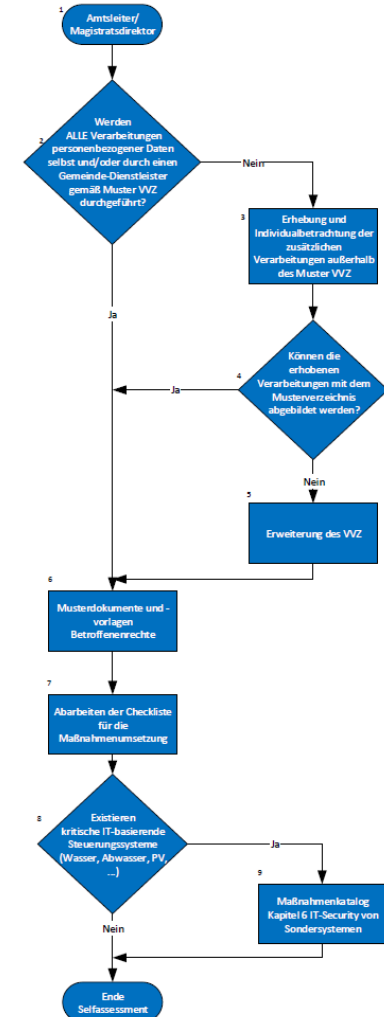
7. Abarbeiten der Checkliste für die Maßnahmenumsetzung

8. Existieren kritische IT-basierende Steuerungssysteme (Wasser, Abwasser, PV, ...)?
Ja ☐ Nein ☐

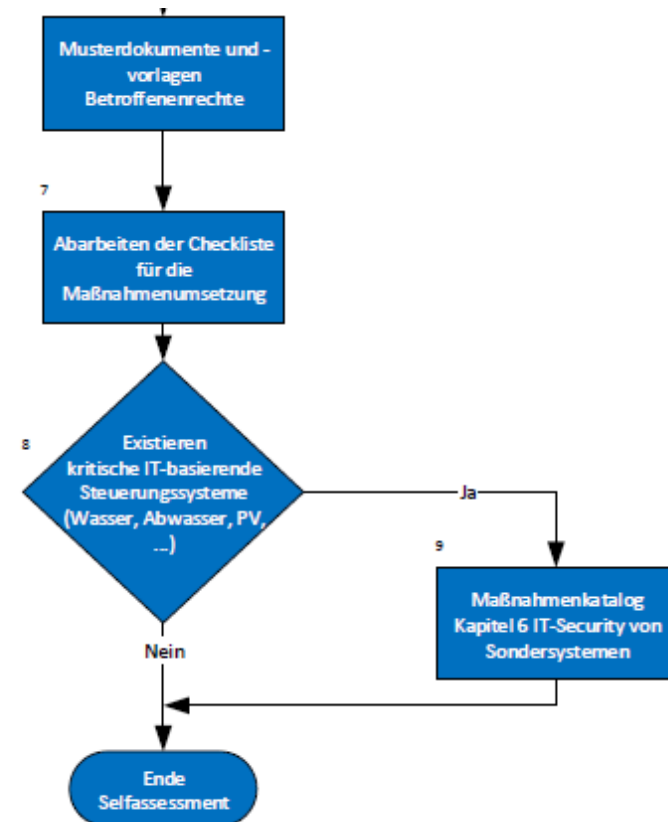
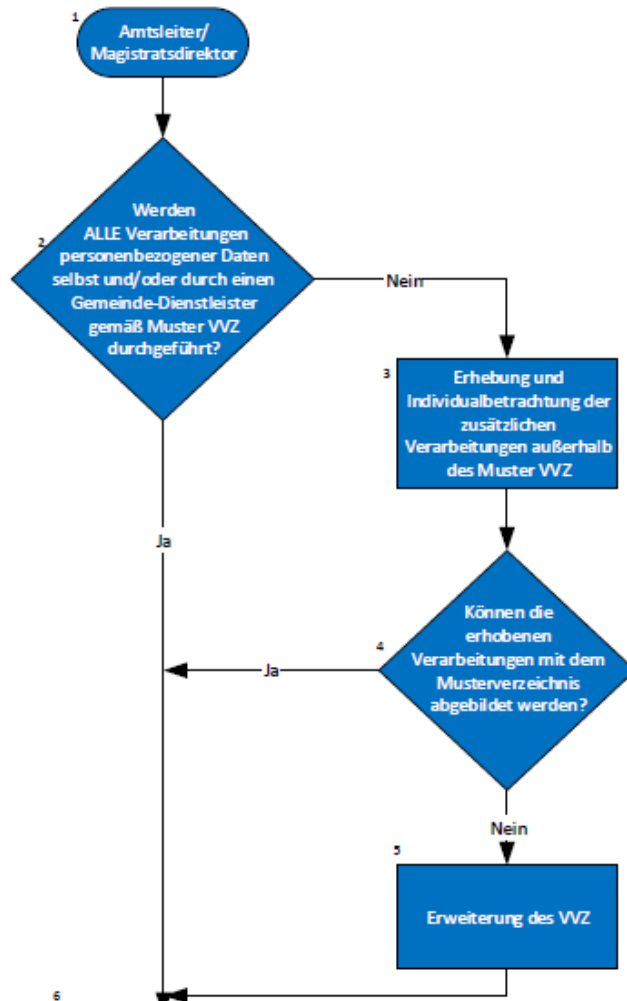
Maßnahmenkatalog Kapitel 6 (IT-Security von Sondersystemen)

Ende Selfassessment

Seite 10



I. Self-Assessment und Muster Verarbeitungsverzeichnis



I. Self-Assessment und Muster Verarbeitungsverzeichnis



FH OO F&E

DSGVO Self-Assessment Fragenkatalog

V1.1

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)		
• _____ • _____ • _____ • _____		

Seite 9

FH OO F&E

DSGVO Self-Assessment Fragenkatalog

V1.1

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		

Seite 10

I. Self-Assessment und Muster Verarbeitungsverzeichnis



- **Musterverarbeitungsverzeichnis für Gemeinden**
 - Erstellt durch Analyse der Verarbeitungen von
 - Kremsmünster (eigene IT)
 - Pettenbach (gemdat serviciert)
 - Gemdat (als Muster Gemeinde Auftragsverarbeiter)
 - Informationen von Großstädten/Bezirkshauptmannschaften/...
 - Enthält Verarbeitungen gemäß DSGVO Vorgabe samt allen erforderlichen Angaben
- **Verwendung**
 - Seite 5 befüllen
 - Nicht benötigte Verarbeitungen können gelöscht werden
 - Bei jeder Verarbeitung erforderliche Angaben ergänzen (Fachabteilung, Ansprechpartner, Datum...)
 - Falls Datenschutzfolgeabschätzung gefordert: Anhang verwenden!
- **Verwendung auch als Mustervorlage für eigene Verarbeitungen**

I. Self-Assessment und Muster Verarbeitungsverzeichnis



- Verarbeitungen
 - standardisiert
 - können als Muster für eigene Verarbeitungen verwendet werden

1. Aktenverwaltung und Datenmanagement (zB Elak, Endarchivierung, CRM/Kundenpflege) im Rahmen der Privatwirtschaftsverwaltung; Förder- und Subventionsvergabe (ehemals SA029)	7
2. Verfahrensabwicklung im Rahmen der Hoheitsverwaltung, insb Bauwesen und angehängte Verfahren	11
3. Teilnahme an genehmigten bzw freigegebenen (Standardanwendungen) Informationsverbundsysteme	14
4. Haushaltsführung, Steuern- und Abgabenverwaltung der Gemeinde und Nebenverfahren	15
5. Staatsbürgerschaftsevidenz (ehemals SA009)	20
6. Personenstandsbücher (alt) und lokales Personenstandsregister (alt, ehemals SA008, SA008a)	24
7. Personalverwaltung (ehemals SA0015), inkl Bewerberdatenverwaltung	29
8. Duale Zustellung	33
9. User Help-Desk (zB auch in Form eines Ticketsystems), Servicedesk	36
10. Informationsportale für Bürger sowie Bürgerservice	39
11. Kinderbetreuungsdatenmanagement, einschließlich Einhebung der Kindergarten- und Hortbeiträge, sowie Einhebung der Schulessensbeiträge	42
12. Schulverwaltung	46
13. Verwaltung von Senioren- und Pflegeheimbewohnerdaten	50
14. Gemeindebetriebe, insb Wirtschaftshof, Freizeiteinrichtungen (zB Freibad)	53
15. Verwaltung von Benutzerkennzeichen, insb Passwörter (ehemals SA007)	57
16. Mietzinsverrechnung – Verwaltung der gemeindeeigenen Häuser und Objekte im Miteigentum bzw Wohnungseigentum	60
17. Abwicklung von Vergabeverfahren (e-Procurement)	63
18. Melderegister und Meldewesen (LMR, ehemals SA010)	67
19. Sitzungsmanagement, Mandatar-Infoportal und Mandatarverzeichnis	72
20. Videoüberwachung	75
21. Wahladministration (Wahlmitarbeiterverzeichnis, Wählerevidenz, Wählerverzeichnisse und Stimmlisten, ehemals SA011)	78
22. Tourismus, einschließlich Gästemeldewesen	83

I. Self-Assessment und Muster Verarbeitungsverzeichnis



2. Verarbeitungsverzeichnis

- Verwendung
 - Seite 5 befüllen

Nachfolgend findet sich das Verarbeitungsverzeichnis, dass die grundlegenden Verarbeitungen von personenbezogenen Daten durch Gemeinden und Städte abbildet.

Verzeichnis von Verarbeitungstätigkeiten gemäß Art 30 Abs 1 DSGVO

Angaben zum Verantwortlichen (Gemeinde/Stadt))

Name:
Straße, Nr.:
PLZ, Ort:
Telefon:
E-Mail:
Internetadresse:

Angaben zum Datenschutzbeauftragten

Name:
Straße, Nr.:
PLZ, Ort:
Telefon:
E-Mail:

Angaben zum Datenschutzkoordinator (verantwortlicher Bediensteter des Verantwortlichen)

Name:
Straße, Nr.:
PLZ, Ort:
Telefon:
E-Mail:

Versionsnummer:

I. Self-Assessment und Muster Verarbeitungsverzeichnis

> Womöglich Datenschutzfolgeabschätzung (DSFA) : Anhang verwenden, 5 Kontrollfragen!

FH OÖ F&E GmbH

Verarbeitungsverzeichnis

V1.1

Anhang – Datenschutz-Folgenabschätzung

ALLGEMEINES ZUR DATENSCHUTZ-FOLGENABSCHÄTZUNG

Die **Datenschutz-Folgenabschätzung (DSFA)** nach Art 35 DSGVO wird als Prozess in 5 Schritten erstellt, um die Verarbeitungstätigkeiten zu beschreiben, die in den Bereichen des Art 35 Abs 3 lit a – c DSGVO **voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen** zur Folge haben. Es geht dabei vor allem um die Verwendung neuer Technologien bei denen aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung derartige Risiken für die betroffenen Personen entstehen. Die DSFA muss vor der Verarbeitung von personenbezogenen Daten stattfinden, wobei der Datenschutzbeauftragte für den Gesamtprozess der Datenschutz-Folgenabschätzung verantwortlich ist, wenn einer bestellt wurde. Die Datenschutz-Folgenabschätzung wird nach folgender Vorgangsweise vorgenommen:

Grundsätzliche Einordnung der Verarbeitung

Die zu bewertende Verarbeitungstätigkeit birgt voraussichtlich ein hohes Risiko für die betroffenen Personen, weil die Verarbeitung insb in folgenden Bereichen liegt:

- a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;
- b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art 9 Abs 1 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder
- c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

Risikobewertung

- a) Systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;
- b) Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
- c) Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen und
- d) Bewältigung der Risiken durch Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

Folgenabschätzung

Bleibt trotz der zur Bewältigung der Risiken geplanten Abhilfemaßnahmen (Schritt 2) ein hohes Risiko für die von der Verarbeitung betroffenen Personen bestehen, so ist die Datenschutzbehörde zu konsultieren, wobei folgende Informationen zur Verfügung gestellt werden müssen:

- Verantwortlichkeiten des Verantwortlichen
- Zweck und Mittel, die für die Verarbeitung verwendet werden

Schritt 1: Ist eine Datenschutzfolgeabschätzung (DSFA) erforderlich?

Erhebt, nutzt, speichert oder teilt Ihre Datenanwendung besondere Datenkategorien (Art 9 DSGVO) oder Daten über strafrechtliche Verurteilungen oder Straftaten (Art 10 DSGVO) von Einwohnern Ihrer Gemeinde/Stadt?	Ja / Nein
Verwendet Ihre Datenanwendung personenbezogene Daten um persönliche Vorlieben, Standorte, Bewegungen von Einzelnen, die finanzielle Situation, Gesundheits- oder Arbeitsleistung Ihrer Einwohner vorherzusagen?	Ja / Nein
Erfolgt eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen aufgrund automatisierter Verarbeitung einschließlich Profiling und dient diese als Grundlage für rechtswirksame Entscheidungen?	Ja / Nein
Erfolgt eine systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche? (zB Videoüberwachung)	Ja / Nein
Fallen Ihnen andere Risiken ein, die in Bezug zum Gebrauch Ihrer Datenanwendung für die Rechte und Freiheiten Einzelner bestehen?	Ja / Nein

Falls eine der Fragen aus dem oa Fragebogen mit „Ja“ beantwortet wird, muss eine DSFA für diese Datenverarbeitungstätigkeit durchgeführt werden.

I. Self-Assessment und Muster Verarbeitungsverzeichnis



- Verwendung auch als Mustervorlage für eigene Verarbeitungen
 - Wenn keine der vorhandenen Musterverarbeitungen passt
 - Ähnlichste Verarbeitung suchen (verarbeitete Datenkategorien), kopieren und adaptieren
 - Zweck beschreiben
 - Korrekte Auswahl der Rechtsgrundlage
 - Verarbeitung besonderer Datenkategorien bearbeiten
 - Löschfristen
 - Datenschutz-Folgeabschätzung erforderlichenfalls durchführen
 - Tabelle Betroffene Personen, Datenarten, Übermittlungsempfänger anpassen, eventuell Übermittlungsempfänger im Anhang ergänzen
 - Korrekte Auswahl der getroffenen Datensicherheitsmaßnahmen
 - ...

II. Betroffenen Rechte



■ Erörterung der Betroffenenrechte, Prozessbeschreibungen, erforderliche Daten

1. RECHTE DER BETROFFENEN PERSON	4
1.1. Allgemeine Grundsätze/Prinzipien	4
2. BETROFFENENRECHTE IM EINZELNEN UND KONKRETER PROZESS	7
2.1. Informationspflicht zu personenbezogenen Daten, Art 13f DSGVO	7
2.2. Auskunftsrecht der betroffenen Person, Art 15 DSGVO	10
2.2.1. Auskunftsprozess	11
2.3. Berichtigung, Art 16 DSGVO	13
2.3.1. Berichtigungsprozess	13
2.4. Löschung, Art 17 DSGVO	14
2.4.1. Lösungsprozess	14
2.5. Recht auf Einschränkung der Verarbeitung, Art 18 DSGVO	17
2.6. Recht auf Datenübertragbarkeit, Art 20 DSGVO	18
2.7. Widerspruchsrecht und automatisierte Entscheidungsfindung im Einzelfall, Art 21f DSGVO	19
2.8. Mitteilungspflicht gegenüber Empfängern, Art 19 DSGVO	20
2.9. Meldung von Verletzungen des Datenschutzrechts an die Datenschutzbehörde/Betroffenen, Art 33f DSGVO („Data Breach Notification“)	21
2.9.1. Prozess zur data breach notification	22

III. DSGVO Maßnahmenkatalog



- Organisatorische und technische Informationssicherheitsmaßnahmen
 - Umsetzung nach Stand der Technik und Best Practice
 - Gliederung nach den Datensicherheitsmaßnahmen des VVZ
 - Bilden Grundlage für angemessenen Schutz jeglicher Informationen (nicht nur personenbezogener Daten)
 - Umsetzung kann abweichen erfolgen, bei „Abschwächung“ MUSS dokumentiert und begründet werden, warum!
 - Formulare/Hilfsmittel im Anhang
 - Weiterführende Literatur: Verweise in Fußnoten, Dokumente im Anhang

- Für Steuerungssysteme (ICS/SCADA) zB im Bereich Wasser, Abwasser, Ortsnahwärme, Photovoltaik: Kapitel 6

- BSI IT-Glossar im Anhang

III. DSGVO Maßnahmenkatalog



1. Vorwort, Hinweise zur Handhabung	5	4.3. Firewall	25
2. Zugangs- und Zugriffskontrolle	6	4.4. Virtual Private Networks (VPN)	26
2.1. Verwalten von Benutzern und Berechtigungsgruppen	6	4.5. Wireless LAN	27
2.1.1. Berechtigungskonzept	6	4.5.1. Internes WLAN	27
2.1.2. Berechtigungsvergabe	8	4.5.2. Gäste-WLAN	28
2.2. Elektronische Zugriffskontrolle - Passwörter	9	4.5.3. Öffentliche Hot-Spots	29
2.3. Physische Zugangskontrolle	10	4.6. Sicheres Drucken	30
2.3.1. Zulässige Schlüssel	10	4.7. Datenübertragung	31
2.3.2. Schlüsselverwaltung	10	4.7.1. Datenübertragung per E-Mail	31
2.4. Endgeräte	11	5. Verfügbarkeit/Belastbarkeit und Integrität	32
2.4.1. Passwortrichtlinie	11	5.1. Datensicherung	32
2.5. Physische Räume	12	5.1.1. Datensicherungskonzept	32
2.5.1. Öffentliche Räumlichkeiten	12	5.1.2. Auswahl des Sicherungsmediums	33
2.5.2. Nicht öffentliche Räumlichkeiten	12	5.1.3. Regelmäßige Überprüfung und Test der Datensicherung	34
2.5.3. Räumlichkeiten mit erhöhtem Schutzbedarf	12	5.1.4. Aufbewahrung der Backup-Datenträger	35
2.5.4. Serverraum/ IT-Raum für kritische IT-Komponenten	13	5.1.5. Aufbewahrungsdauer - gesetzliche Verpflichtungen	36
3. Speicher- und Datenträgerkontrolle	14	5.2. Regelmäßige Software Updates	37
3.1. Umgang mit Informationsträgern	14	5.3. Virenschutz	38
3.1.1. Aufbewahrung von Informationsträgern	14	6. IT-Security von Sondersystemen	39
3.1.2. Entsorgung von Informationsträgern	15	6.1. Industrielle Steuerungssysteme (ICS/SCADA)	39
3.1.3. Verschlüsselung von mobilen Geräten und externen Datenträgern	16	7. Organisatorische Maßnahmen	41
3.1.4. Umgang mit externen Wechseldatenträgern	17	7.1. Regelmäßige Überprüfung der Maßnahmen	41
3.2. Verhindern unbefugter Kenntnisnahme	18	8. Anhang	42
3.2.1. Clean-Desk Policy/ Clear-Screen Policy	18	8.1. Checkliste Eintritt Mitarbeiter	42
3.2.2. Zweckgebundenheit - Reduzierung von unbefugten Verarbeitungsschritten	19	8.2. Checkliste Austritt Mitarbeiter	43
3.2.3. Bring Your Own Device	20	8.3. Formular Vorgehensweise bei Schadsoftwarebefall	44
3.2.4. Cloud-Anbieter	21	8.4. Formular Schlüssel-Empfangsbestätigung	45
3.2.5. Einsatz von Messengern	22	8.5. Formular Schlüssel-Rückgabebestätigung	46
4. Übertragungs- und Eingabekontrolle	23	8.6. Formular Berechtigungsvergabe	47
4.1. Nachvollziehbarkeit	23	8.7. Formular Entsorgung/ Wiederverwendung/ Löschung von Datenträgern	48
4.1.1. Änderungshistorie	23	8.8. Checkliste Softwareupdates	49
4.2. Einsatz von Software	24	8.9. Checkliste Überprüfung und Test der Datensicherung	50
		8.10. Muster-Formular für periodische Überprüfungsarbeiten	51
		8.11. Formular Vertretungsregelung	52
		9. Index	54

III. DSGVO Maßnahmenkatalog

FH OÖ F&E

DSGVO-Maßnahmenkatalog

V1.1



4.5. Wireless LAN

4.5.1. Internes WLAN

Zuständig: IT-Leiter

Angriffe auf die IT-Infrastruktur über Wireless LAN dürfen nicht unterschätzt werden. So wäre es einem Angreifer bei einem ungesicherten WLAN möglich, Firmendaten auszuspionieren und somit den Datenschutz zu gefährden.

Bei der Planung und Installation eines WLANs ist darauf zu achten, dass dieses dem aktuellen Stand der Technik hinsichtlich der Security Implementierung (WPA2-PSK oder WPA2-Enterprise) entspricht. Bei der Positionierung der WLAN-Komponenten sollte darauf geachtet werden, dass diese vor unautorisiertem physischem Zugriff geschützt sind (manipulationssichere Montage, Schutzgehäuse).

Die Zugangsdaten zum Webinterface bzw. zu dem Konfigurationsmenü sind bei der Ersteinrichtung zu ändern (der Zugang zum Access-Point darf nicht über Standardpasswörter möglich sein).

Wenn ein Pre-Shared-Key (WPA2-PSK) verwendet wird, so muss das Passwort für den Pre-Shared-Key folgende Anforderungen erfüllen:

- Mindestens 20 Zeichen lang.
- Muss jeweils mindestens einen Großbuchstaben, einen Kleinbuchstaben, sowie aus einem Sonderzeichen oder einer Zahl bestehen.
- Wird das Passwort geändert, so darf das bereits verwendete Passwort niemals erneut verwendet werden.

Sollte der Access-Point die Möglichkeit bieten, über WPS eine Verbindung aufzubauen, so ist das Verwenden von WPS untersagt und diese Funktion zu deaktivieren.

Da sich auch im WLAN-Bereich ständig neue Sicherheitslücken ergeben, ist dafür Sorge zu tragen, dass die WLAN-Komponenten regelmäßige Firmware-/Software-Updates erhalten (Wartungsvertrag).

III. DSGVO Maßnahmenkatalog



■ Checkliste zur Abarbeitung, Umsetzungskontrolle, Dokumentation

Nr.	Maßnahme	Relevant für die Umsetzung?		Verantwortlicher	Status der Umsetzung?	Beschreibung der bisherigen Umsetzung	Umsetzung bis	Prüfung der Umsetzung		
		JA / NEIN	Begründung					Verantwortlicher	geprüft am	Anmerkungen
2	Zugangs- und Zugriffskontrolle									
2.1	Verwalten von Benutzern und Berechtigungsgruppen									
2.1.1	Berechtigungskonzept									
2.1.2	Berechtigungsergänzung									
2.2	Elektronische Zugriffskontrolle - Passwörter									
2.3	Physische Zugangskontrolle									
2.3.1	Zulässige Schlüssel									
2.3.2	Schlüsselverwaltung									
2.4	Endgeräte									
2.4.1	Passwortrichtlinie									
2.5	Physische Räume									
2.5.1	Öffentliche Räumlichkeiten									
2.5.2	Nicht öffentliche Räumlichkeiten									
2.5.3	Räumlichkeiten mit erhöhtem Schutzbedarf									
2.5.4	Serverraum/ IT-Raum für kritische IT-Komponenten									
3	Speicher- und Datenträgerkontrolle									
3.1	Umgang mit Informationsträgern									
3.1.1	Aufbewahrung von Informationsträgern									
3.1.2	Entsorgung von Informationsträgern									
3.1.3	Verschlüsselung von mobilen Geräten und externen Datenträgern									
3.1.4	Umgang mit externen Wechseldatenträgern									
3.2	Verhindern unbefugter Kenntnisnahme									
3.2.1	Clean-Desk Policy/ Clear-Screen Policy									
3.2.2	Zweckgebundenheit - Reduzierung von unbefugten Verarbeitungsschritten									
3.2.3	Bring Your Own Device									
3.2.4	Cloud-Anbieter									
3.2.5	Einsatz von Messengern									
4	Übertragungs- und Eingabekontrolle									
4.1	Nachvollziehbarkeit									
4.1.1	Änderungshistorie									
4.2	Einsatz von Software									
4.3	Firewall									
4.4	Virtual Private Networks (VPN)									
4.5	Wireless LAN									
4.5.1	Internes WLAN									
4.5.2	Gäste-WLAN									
4.5.3	Öffentliche Hot-Spots									
4.6	Sicheres Drucken									
4.7	Datenübertragung									
4.7.1	Datenübertragung per E-Mail									
5	Verfügbarkeit/ Belastbarkeit und Integrität									
5.1	Datensicherung									
5.1.1	Datensicherungskonzept									
5.1.2	Auswahl des Sicherungsmediums									
5.1.3	Regelmäßige Überprüfung und Test der Datensicherung									
5.1.4	Aufbewahrung der Backup-Datenträger									
5.1.5	Aufbewahrungsdauer - gesetzliche Verpflichtungen									
5.2	Regelmäßige Software Updates									
5.3	Virenschutz									
6	IT-Security von Sondersystemen									
6.1	Industrielle Steuerungssysteme (ICS/SCADA)									
7	Organisatorische Maßnahmen									
7.1	Regelmäßige Überprüfung der Maßnahmen									

III. DSGVO Maßnahmenkatalog



Checkliste zur Abarbeitung, Umsetzungskontrolle, Dokumentation

Nr.	Maßnahme	Relevant für die Umsetzung?		Verantwortlicher	Status der Umsetzung?	Beschreibung der bisherigen Umsetzung	Umsetzung bis	Verantwortlicher
		JA / NEIN	Begründung					
4.5	Wireless LAN							
4.5.1	Internes WLAN	JA		Max Mustermann	TEILWEISE	WLAN Passwörter zu kurz	01.04.2018	
4.5.2	Gäste-WLAN							
4.5.3	Öffentliche Hot-Spots							
4.6	Sicheres Drucken							
4.7	Datenübertragung							
4.7.1	Datenübertragung per E-Mail							

Dokumentenhistorie/Deckblatt, Ausfüllhilfe!

DSGVO Maßnahmenkatalog Checkliste			
Ausfüllhilfe			
Fragen/Checks			
Relevant für die Umsetzung? JA/NEIN, Begründung		Erläuterung	
Gemeinde/Stadt: <Gemeinde/Stadt Name>		Die Umsetzung der Maßnahme ist in der vorgeschlagenen Art nicht erforderlich, da beispielsweise die Umsetzung der Maßnahme durch einen externen Dienstleister erfolgt, andere Maßnahmen implementiert wurden (welche nicht im Maßnahmenkatalog aufgeführt sind, aber vergleichbare Ergebnisse liefern) oder weil die Maßnahme im jeweiligen Kontext nicht relevant ist (z.B. weil darin adressierte Dienste nicht aktiviert wurden).	
Version: 1.1		Wurde eine Maßnahme mit "NEIN", dh als nicht relevant markiert, ist eine Begründung anzugeben, warum die Umsetzung nicht erforderlich ist.	
Datum: DD.MM.JJJJ		Sind die Maßnahmenempfehlungen relevant, ist ein Verantwortlicher für die Umsetzung zu benennen.	
Klassifikation: streng vertraulich		Status der Umsetzung	
Zuständig: <Name>		Als Antworten bezüglich des Umsetzungsstatus der einzelnen Maßnahmen kommen folgende Aussagen in Betracht:	
Freigabe:		JA NEIN TEILWEISE	
Beschreibung der bisherigen Umsetzung		Alle Empfehlungen in der Maßnahme sind vollständig, wirksam und angemessen umgesetzt.	
Umsetzung bis		Die Empfehlungen der Maßnahme sind größtenteils noch nicht umgesetzt.	
Versionshistorie		Einige der Empfehlungen sind umgesetzt, andere noch nicht oder nur teilweise.	
Datum	Autor	Wird beim Umsetzungsstatus der Maßnahme "TEILWEISE" angegeben, sind die bereits implementierten Maßnahmen zu beschreiben.	
0.1	<Name>	Wird der Umsetzungsstatus der Maßnahme mit "NEIN" oder mit "TEILWEISE" beantwortet, ist ein Datum festzulegen, bis wann die Umsetzung aller Empfehlungen der Maßnahme erfolgt.	
	Tätigkeit	Hier ist zu dokumentieren, wie die Prüfung der Umsetzung erfolgte.	
	Initialbearbeitung	Farbgebung	
		keine Eingabe bei der Maßnahme erforderlich	
		Begründung, Beschreibung und/oder Datum bei der Maßnahme erforderlich	

DSGVO Maßnahmenkatalog Checkliste	
Ausfüllhilfe	
Fragen/Checks	
Relevant für die Umsetzung? JA/NEIN, Begründung	Erläuterung
Gemeinde/Stadt: <Gemeinde/Stadt Name>	Die Umsetzung der Maßnahme ist in der vorgeschlagenen Art nicht erforderlich, da beispielsweise die Umsetzung der Maßnahme durch einen externen Dienstleister erfolgt, andere Maßnahmen implementiert wurden (welche nicht im Maßnahmenkatalog aufgeführt sind, aber vergleichbare Ergebnisse liefern) oder weil die Maßnahme im jeweiligen Kontext nicht relevant ist (z.B. weil darin adressierte Dienste nicht aktiviert wurden).
Version: 1.1	Wurde eine Maßnahme mit "NEIN", dh als nicht relevant markiert, ist eine Begründung anzugeben, warum die Umsetzung nicht erforderlich ist.
Datum: DD.MM.JJJJ	Sind die Maßnahmenempfehlungen relevant, ist ein Verantwortlicher für die Umsetzung zu benennen.
Klassifikation: streng vertraulich	Status der Umsetzung
Zuständig: <Name>	Als Antworten bezüglich des Umsetzungsstatus der einzelnen Maßnahmen kommen folgende Aussagen in Betracht:
Freigabe:	JA NEIN TEILWEISE
Beschreibung der bisherigen Umsetzung	Alle Empfehlungen in der Maßnahme sind vollständig, wirksam und angemessen umgesetzt.
Umsetzung bis	Die Empfehlungen der Maßnahme sind größtenteils noch nicht umgesetzt.
Versionshistorie	Einige der Empfehlungen sind umgesetzt, andere noch nicht oder nur teilweise.
Datum	Wird beim Umsetzungsstatus der Maßnahme "TEILWEISE" angegeben, sind die bereits implementierten Maßnahmen zu beschreiben.
Autor	Wird der Umsetzungsstatus der Maßnahme mit "NEIN" oder mit "TEILWEISE" beantwortet, ist ein Datum festzulegen, bis wann die Umsetzung aller Empfehlungen der Maßnahme erfolgt.
Tätigkeit	Hier ist zu dokumentieren, wie die Prüfung der Umsetzung erfolgte.
Initialbearbeitung	Farbgebung
	keine Eingabe bei der Maßnahme erforderlich
	Begründung, Beschreibung und/oder Datum bei der Maßnahme erforderlich

III. DSGVO Maßnahmenkatalog



- Ergänzende Dokumente
 - Referenzierte Dokumente von BSI, EU, ...
 - BSI - Glossar – IT-Grundschutz-Kataloge
 - AKTUELLE VERSIONEN ONLINE!

4 Glossar und Begriffsdefinitionen



In diesem Glossar werden einige wichtige Begriffe rund um Informationssicherheit und IT-Grundschutz erläutert.

Administrator

Ein Administrator verwaltet und betreut Rechner sowie Computernetze. Er installiert Betriebssysteme und Anwendungsprogramme, richtet neue Benutzerkennungen ein und verteilt die für die Arbeit notwendigen Rechte. Dabei hat er im Allgemeinen weitreichende oder sogar uneingeschränkte Zugriffsrechte auf die betreuten Rechner oder Netze.

Angriff

Ein Angriff ist eine vorsätzliche Form der Gefährdung, nämlich eine unerwünschte oder unberechtigte Handlung mit dem Ziel, sich Vorteile zu verschaffen bzw. einen Dritten zu schädigen. Angreifer können auch im Auftrag von Dritten handeln, die sich Vorteile verschaffen wollen.

Application-Level-Gateway (ALG)

Die Funktionen eines Sicherheitsgateways auf Anwendungsebene werden von den so genannten Application-Level-Gateways (ALG) übernommen. Implizit nehmen ALGs auch Funktionen auf den ISO-/OSI-Schichten 1 bis 3 wahr. ALGs, auch Sicherheitsproxies genannt, unterbrechen den direkten Datenstrom zwischen Quelle und Ziel. Bei einer Kommunikationsbeziehung zwischen Client und Server über einen Proxy hinweg nimmt der Proxy die Anfragen des Clients entgegen und leitet sie an den Server weiter. Bei einem Verbindungsaufbau in umgekehrter Richtung, also vom Server zum Client, verfährt der Proxy analog.

Sämtliche Kommunikationsbeziehungen zwischen den beiden Rechnern verlaufen in diesem Fall also mittelbar über den Proxy. Diese Kommunikationsform ermöglicht es einem Proxy beispielsweise bestimmte Protokollbefehle zu filtern.

Authentisierung (englisch "authentication")

Authentisierung bezeichnet den Nachweis eines Kommunikationspartners, dass er tatsächlich derjenige ist, der er vorgibt zu sein. Dies kann unter anderem durch Passwort-Eingabe, Chipkarte oder Biometrie erfolgen.

Einige Autoren unterscheiden im Deutschen zwischen den Begriffen Authentisierung, Authentifizierung und Authentikation. Mit Authentisierung wird dann die Vorlage eines Nachweises zur Identifikation bezeichnet, mit Authentifizierung die Überprüfung dieses Nachweises. Um den Text verständlich zu halten, verzichtet der IT-Grundschutz auf diese Unterscheidung.

IV. Schulungskonzept



- Für Schulungsanbieter und/oder Gemeinden/Städte, die selbst Schulungsprogramme erstellen wollen
- Beschreibt
 - Empfohlene Gliederung
 - Empfohlene Teilnehmerkreise
 - Mindestinhalte

IV. Schulungskonzept



- Für Schulungsanbieter und/oder Gemeinden/Städte, die selbst Schulungsprogramme erstellen wollen

- Beschreibt

- Empfohlene Teilnehmerkreise
 - Behördenleiter, GF, Bgmst
 - IT-Leiter
 - Mitarbeiter Gemeinde/Stadt
 - Mitarbeiter Dienstleister
- Empfohlene Gliederung in Module
- Empfohlene Inhalte je Modul

FH OÖ F&E	DSGVO Schulungskonzept	V1.1	FH OÖ F&E	DSGVO Schulungskonzept	V1.1
Inhaltsverzeichnis					
Inhaltsverzeichnis		2			
1. Vorwort, Verwendungshinweise		5			
2. Schulungsplanübersicht		6			
2.1. Rolle: Behördenleiter (auch: Geschäftsführer oder Datenschutzbeauftragter von Dienstleister), Bürgermeister		6	4.4.2. Situation in Büroräumen, Besprechungsräumen		10
2.2. Rolle: IT-Leiter		6	4.4.3. Korrekte Entsorgung von Datenträgern		10
2.3. Rolle: Mitarbeiter Gemeinde/Stadt		7	4.4.4. Social Media		10
2.4. Rolle: Mitarbeiter Dienstleister		7	4.4.5. Social Engineering Angriffe / Fake President Fraud		10
3. Modul Datenschutzgrundlagen		8	4.4.6. Umgang mit Bürgern, Gästen – Besucherregelungen		11
3.1. Rechtliche Grundlagen (was sind personenbezogene Daten, warum schützen wir die, gesetzliche Rahmenbedingungen, DSG, DSGVO)		8	4.5. Besondere Regeln für den Notfall		11
3.2. Verarbeitungsgrundsätze		8	4.5.1. Datenverlust - Data Breach Notification		11
3.3. Betroffenenrechte		8	4.5.2. Schadsoftwarebefall		11
3.4. Meldepflichten und Verantwortlichkeiten		8	4.5.3. Fehlverhalten von Mitarbeitern		11
4. Modul Überblick über die Maßnahmen für Datenschutz und Informationssicherheit		8	5. Modul Grundlegende Verhaltensregeln bei Datenschutzanliegen von Betroffenen		11
4.1. Warum werden Schutzmaßnahmen getroffen		9	5.1. Beschwerden		11
4.1.1. Grundsätze der Informationssicherheit		9	5.2. Informationsrecht		11
4.1.2. Vertraulichkeit		9	5.3. Auskunftsrecht		11
4.1.3. Integrität		9	6. Modul Self-Assessment		12
4.1.4. Verfügbarkeit		9	7. Modul Verarbeitungsverzeichnis		12
4.1.5. Least-Privilege Prinzip (warum sieht nicht jeder alles, warum sind nicht alle Admins?)		9	7.1. Sinn und Zweck		12
4.1.6. Need-To-Know-Prinzip (warum Zugriffsbeschränkungen)		9	7.2. Musterverarbeitungsverzeichnis		12
4.1.7. Nachvollziehbarkeit, Dokumentation		9	7.3. Erweiterungen des VVZ		12
4.1.8. Korrektes Verhalten im Notfall		9	7.4. Risikobetrachtung und Datenschutz-Folgenabschätzung		12
4.2. Physische Schutzmaßnahmen		9	8. Modul Maßnahmenumsetzung		13
4.2.1. Anlagen/Objektschutz		9	8.1. Festlegung von Zuständigkeiten/ Verantwortlichkeiten (DSB, Auskunfts-/Meldestelle, ...)		13
4.2.2. Zusperrern		9	8.2. Wahrung der Betroffenenrechte im Außenverhältnis		13
4.2.3. Clean-Desk-Policy		9	8.3. Verträge mit Auftragsdatenverarbeitern		13
4.3. Informationssicherheits-/IT-Schutzmaßnahmen		9	8.4. Umsetzung organisatorische und technische Maßnahmen		13
4.4. Verhaltensregeln, DOs and DON'Ts		10	8.4.1. Zugriffskontrolle (Passwörter, Zutritt, Clean-Desk)		14
4.4.1. Weitergabe von Informationen, Umgang mit Datenträgern		10	8.4.2. Schutz vor unautorisierter Datennutzung und Datenverlust (Rollen/Rechte, Verwahrung/Transport/Vernichtung)		14
			8.4.3. Endgerätesicherheit (Zugriffsregelung, Benutzerrechte, Virens Scanner, ...)		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. Ausfallsicherheit: 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

Wie geht es weiter?



- Alle Dokumente, Muster, Hilfsmittel sind mit Stand Februar 2018 erstellt!

- DSG tritt am 25.5.2018 in Kraft
 - > White-/Blackliste wegen DSFA fehlt
 - > Sichtweise der Behörde fehlt
 - > ...

- NISG / kritische Infrastrukturen
 - > Gesetz ab 9.5.2018
 - > Liste der BwD bis 18.11.2018
 - > Gesetz selbst, Verordnungen, ... fehlen
 - > ...

- Es gibt KEINE Support-/Wartungs-/Aktualisierungsvereinbarung mit FH!

Weiterführende Ausbildung



Informationssicherheitsmanagement

- Kompetent ausgebildete Mitarbeiter (CISO/DSB: wir machen die in Hagenberg ;)
- Zuständigkeiten, Ressourcen, Regelungen/Richtlinien, NOTFALLPLÄNE
- Sicherheitsüberprüfungen von neuen Anwendungen, regelmäßige Sicherheitschecks
- Erfüllung der DSVO/DSG Verpflichtungen – auch durch Outsourcing
- Check von (Cloud-)Providern, Sublieferanten, Verträgen/Nutzungsbedingungen
- Benutzerschulungen

Ausbildung

- FH Hagenberg, Department Sichere Informationssysteme
 - **Information Security Management Master**
 - berufsbegleitend, 8 Präsenzwochen in 2 Jahren
 - Bewerbungsverfahren für 2018 läuft!
 - Sichere Informationssysteme Bachelor/Master



INFORMATION SECURITY MANAGEMENT
BERUFSBEGLEITENDES MASTERSTUDIUM

FH OÖ Fakultät für Informatik, Kommunikation und Medien
Campus Hagenberg

Der sichere Weg in eine sichere Zukunft

www.fh-ooe.at/ism





Danke für die Aufmerksamkeit

SV FH-Prof. DI Robert Kolmhofer

Leiter des Departments Sichere Informationssysteme
FH Oö Fakultät für Informatik/Kommunikation/Medien, Campus Hagenberg
robert.kolmhofer@fh-hagenberg.at



Allgemein beeideter und gerichtlich zertifizierter Sachverständiger (Informatik/Nachrichtentechnik)
Geschäftsführer UNINET it-consulting GmbH