

# Leitfaden

## Zur rechtskonformen Umsetzung von Informationssicherheit und Datenschutz

### Anleitungen zur Umsetzung nach Art. 32 DSGVO und nach BSI Grundsicherheitsanforderungen

Kapitel	Inhalte	Seiten
1	Übersicht Leitfaden (Inhalte)	2
2	Auszug DSGVO Art. 32 Datensicherheit	3
3	Auszug DSGVO Art. 37 Datenschutzbeauftragte	4
4	BSI IT-Sicherheitsanforderungen	5–6
5	Anwendungshinweise Checkliste & Curriculum	7
6	Mustervorlage Einführung IT-Sicherheit für Mitarbeitende	8–10
7	Mustervorlage Einführung Datenschutz für Mitarbeitende	11–12
8	Mustervorlage Zusatzvereinbarung Arbeitsvertrag	13
9	Mustervorlage Zusatzvereinbarung IT-Dienstleistende	14
10	Mustervorlage Leitlinie Informationssicherheit	15
11	Mustervorlage Verfahrensanweisung Schulung (ISO 9001)	16–17
12	Mustervorlage Verfahrensanweisung IT-Notfall	18
13	Curriculum	19
14	Glossar Informationssicherheit und Datenschutz	20–22
15	Start mit dem MC-ORG (Registrierung/Onboarding)	23–24
16	Start für Mitarbeitende (MC-SMARTLEARN)	25–26

Die Inhalte und Vorlagen des Leitfadens stehen den Kund\*innen nach Abschluss einer Ecclesia Cyber-Versicherung exklusiv zur Verfügung.

Die vollständigen Inhalte können mit dem Autorisierungs-Code über das cloudbasierte Assistenz-System **MC-ORG** online abgerufen und genutzt werden.

(Copyright MCSS AG, Köln)



# Leitfaden für Informationssicherheit und Datenschutz

## Überblick

Informationssicherheit (inkl. Cyberschutz) und Datenschutz in kleinen und mittleren Unternehmen hat durch aktuelle Entwicklungen eine hohe Priorität bekommen. Mit dem Abschluss einer Cyber-Versicherung wurde ein wichtiger Schritt für mehr Sicherheit eingeleitet.

Mit der Datenschutz-Grundverordnung (DSGVO) ist die Einführung von Datensicherheit in Unternehmen und Organisationen verpflichtend geworden.

## Checkliste zu Anforderungen nach BSI

Die IT-Sicherheitsrichtlinie der KBV und des Bundesamts für Sicherheit in der Informationstechnik (BSI) stellt eine gute Basis für notwendige Maßnahmen dar. Die in diesem Leitfaden enthaltene Checkliste erlaubt einen schnellen Überblick über den Ist-Zustand und die zu treffenden Maßnahmen nach Prioritäten.

## Curriculum (Einführungsplan) für 12 Monate

Natürlich sind die Belastungen in allen Unternehmen in diesen Zeiten hoch und Kapazitäten sind begrenzt. Deshalb wurde dieser Leitfaden und das **MCSS Assistenz-System** so zeit- und kostensparend wie möglich entwickelt. Ein Curriculum für einen ersten Einführungszeitraum von 12 Monaten gibt einen realistischen „Fahrplan“ vor. Begleitet wird dieser mit 4 Webinaren für die Verantwortlichen (eine Schulung pro Quartal).

## Cloudsystem MCSS Ökosystem

Der Leitfaden ist als schnelle und einfache Einführung in Informationssicherheit und Datenschutz entwickelt worden. Dahinter steht ein cloudbasiertes Sicherheitsmanagementsystem für Cyberschutz, Informationssicherheit und Datenschutz. Mit Abschluss der Cyber-Versicherung haben die versicherten Einrichtungen Zugang zu dem **MCSS Ökosystem** über das Internet. Dazu nutzt man einen digitalen Zugangs-Code, der per E-Mail bzw. Brief mitgeteilt wurde. Das System kann mit PCs, Laptops, Tablet-Computern und auch Smartphones überall dort genutzt werden, wo ein Internet-Anschluss zur Verfügung steht.

Während dieser analoge Leitfaden nur begrenzte Informationen und Wissens-Module zur Verfügung stellen kann, bietet das cloudbasierte **MCSS Ökosystem** über 2.400 Funktionen und Komponenten:

- **Status-Analysen** erlauben die Bewertung bereits eingesetzter technischer, organisatorischer und rechtlicher Maßnahmen. Die Analysen liefern Messwerte über den „Reifegrad“ der internen Organisation.
- **Wissenstests** mit „Multiple Choice“ Antworten geben den Mitarbeitenden die Möglichkeiten, ihre Kenntnisse zu den wichtigsten Anforderungen für Informationssicherheit und Datenschutz zu prüfen.
- **Checklisten** sind eine praktische Anleitung, um Cyberschutz zusammen mit dem Team in Schulungen nach einem strukturierten Plan (siehe Curriculum) umzusetzen.
- **Verfahrensweisungen** (nach ISO 9001) bilden die Grundlage für ein professionelles Qualitätsmanagement auch für die Sicherheitsmaßnahmen.
- **MC-SMARTLEARN** ist ein speziell für die Mitarbeitenden entwickeltes Trainingsprogramm, das zeitgemäß mit Apps auf dem Smartphone abgerufen werden kann.
- **Berichts-Generierung** zur Erfüllung der gesetzlichen Verpflichtungen nach der DSGVO ist durch entsprechende Vorlagen mit geringem Zeitaufwand möglich.
- **Webinare** können Verantwortliche in den Unternehmen und Organisationen bei der Führung der Teams mit Fachwissen und Unterlagen unterstützen.
- **Schulungsnachweise** können vom **MCSS Kundenservice** digital zur Verfügung gestellt werden (Sicherheit bei Sicherheits-Audits).

## Zugang zum Cloudsystem

Der Zugang zum digitalen Assistenz-System für Cyber-Versicherte ist bereits durch die Versicherungsprämie lizenziert und sehr einfach zu nutzen. **MCSS** stellt den sicheren Zugangs-Code allen Versicherten zur Verfügung. Dazu wird die im Versicherungsvertrag angegebene E-Mail-Adresse für die Kommunikation verwendet.

**Achtung:** Wenn der Code bislang nicht eingegangen ist, bitte auch im SPAM Ordner des Postfachs nachschauen.  
**Ansonsten Nachfrage an:** [anwenderservice@mcss-ag.de](mailto:anwenderservice@mcss-ag.de) mit Angabe der Cyber-Versicherungs-Nr.

## Art. 32 DSGVO Originaltext aus der EU-Datenschutz-Grundverordnung

### Sicherheit der Verarbeitung

- (1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:
- a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
  - b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
  - c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
  - d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.**
- (2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugtem Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.
- (3) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.
- (4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

### Passende Erwägungsgründe

- (75) Risiken für die Rechte und Freiheiten natürlicher Personen (76) Risikobewertung  
(77) Leitlinien zur Risikobewertung **(78) Geeignete technische und organisatorische Maßnahmen**  
**(79) Zuteilung der Verantwortlichkeit (83) Sicherheit der Verarbeitung**

## Art. 37 DSGVO

### Benennung eines Datenschutzbeauftragten

- (1) Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn
  - a) die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, soweit sie im Rahmen ihrer justiziellen Tätigkeit handeln,
  - b) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder
  - c) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht.
- (2) Eine Unternehmensgruppe darf einen gemeinsamen Datenschutzbeauftragten ernennen, sofern von jeder Niederlassung aus der Datenschutzbeauftragten leicht erreicht werden kann.

## § 38 BDSG

### Datenschutzbeauftragte nichtöffentlicher Stellen

- (1) <sup>1</sup>Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. <sup>2</sup> Nehmen der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vor, die einer Datenschutz-Folgenabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 unterliegen, oder verarbeiten sie personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung, haben sie unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen.
- (2) § 6 Absatz 4, 5 Satz 2 und Absatz 6 finden Anwendung, § 6 Absatz 4 jedoch nur, wenn die Benennung einer oder eines Datenschutzbeauftragten verpflichtend ist.

**Anmerkung: In kleineren Organisationen kann der/die Datenschutzbeauftragte (DSB) auch die Aufgaben im Zusammenhang mit der Datensicherheit nach Art. 32 der DSGVO übernehmen. Voraussetzung ist die dokumentierte Qualifikation des internen oder externen DSB.**

# BSI Sicherheitsanforderungen (Checkliste)

Nr.	Zielobjekt	Anforderung	Priorität			Status (in %)			Verantwortung	Datum
			1	2	3	0	50	100		
<b>Software: Rechner-Programme, mobile Apps und Internet-Anwendungen</b>			1	2	3	0	50	100		
1	Mobile Anwendungen	<b>Sichere Apps nutzen</b> Nur Apps aus den offiziellen Stores runterladen und nutzen. Wenn nicht mehr benötigt, Apps löschen.		x						
2	Mobile Anwendungen	<b>Aktuelle App-Versionen</b> Updates immer zeitnah installieren, um Schwachstellen zu vermeiden.		x						
3	Mobile Anwendungen	<b>Sichere Speicherung lokaler App-Daten</b> Nur Apps nutzen, die Dokumente verschlüsselt und lokal abspeichern.			x					
4	Mobile Anwendungen	<b>Verhinderung von Datenabfluss</b> Keine vertraulichen Daten über Apps versenden.		x						
5	Office-Produkte	<b>Verzicht auf Cloud-Speicherung</b> Keine Nutzung der in Office-Produkte integrierten Cloud-Speicher zur Speicherung personenbezogener Informationen.			x					
6	Office-Produkte	<b>Beseitigung von Rest Informationen vor Weitergabe von Dokumenten</b> Vertrauliches aus Dokumenten löschen vor einer Weitergabe an Dritte.			x					
7	Internet-Anwendungen	<b>Authentisierung bei Webanwendungen</b> Nutzen Sie nur Internet-Anwendungen, die ihre Zugänge (Login-Seite und -Ablauf, Passwort, Benutzerkonto etc.) strikt absichern.		x						
8	Internet-Anwendungen	<b>Schutz vertraulicher Daten</b> Stellen Sie Ihren Internet-Browser gem. Hersteller-Anleitung so ein, dass keine vertraulichen Daten im Browser gespeichert werden.			x					
9	Internet-Anwendungen	<b>Firewall benutzen</b> Verwendung und regelmäßiges Update einer Web App Firewall.	x							
10	Internet-Anwendungen	<b>Kryptografische Sicherung vertraulicher Daten</b> Nur verschlüsselte Internet-Anwendungen nutzen.		x						
11	Internet-Anwendungen	<b>Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen</b> Keine automatisierten Zugriffe bzw. Aufrufe auf Webanwendungen einrichten oder zulassen.			x					
12	Endgeräte	<b>Verhinderung der unautorisierten Nutzung von Rechner-Mikrofonen und Kameras</b> Mikrofon und Kamera am Rechner sollten grundsätzlich deaktiviert sein und nur bei Bedarf temporär direkt am Gerät aktiviert und danach wieder deaktiviert werden.	x							
13	Endgeräte	<b>Abmelden nach Aufgabenerfüllung</b> Nach Ende der Nutzung immer den Zugang zum Gerät sperren oder abmelden.	x							
14	Endgeräte	<b>Regelmäßige Datensicherung</b> Sichern Sie regelmäßig Ihre Daten.	x							
15	Endgeräte	<b>Einsatz von Viren Schutzprogrammen</b> Setzen Sie aktuelle Virenschutzprogramme ein.	x							
16	Endgeräte (Windows)	<b>Konfiguration von Synchronisationsmechanismen</b> Die Synchronisierung von Nutzerdaten mit Microsoft-Cloud-Diensten sollte vollständig deaktiviert werden.		x						
17	Endgeräte (Windows)	<b>Datei- und Freigabeberechtigungen</b> Regeln Sie Berechtigungen und Zugriffe pro Personengruppe und pro Person.	x							
18	Endgeräte (Windows)	<b>Datensparsamkeit</b> Verwenden Sie so wenige persönliche Daten wie möglich.		x						
19	Smartphone und Tablet	<b>Schutz vor Phishing und Schadprogrammen im Browser</b> Nutzen Sie aktuelle Schutzprogramme vor Phishing und Schadprogrammen im Browser.	x							
20	Smartphone und Tablet	<b>Verwendung der SIM-Karten PIN</b> SIM-Karten durch PIN schützen. Super-PIN/PUK nur durch Verantwortliche anzuwenden.		x						
21	Smartphone und Tablet	<b>Sichere Grundkonfiguration für mobile Geräte</b> Auf mobilen Endgeräten sollten die strengsten bzw. sichersten Einstellungen gewählt werden, weil auch auf mobilen Geräte das erforderliche Schutzniveau für die verarbeiteten Daten sichergestellt werden muss.		x						
22	Smartphone und Tablet	<b>Verwendung eines Zugriffsschutzes</b> Schützen Sie Ihre Geräte mit einem komplexen Gerätesperrcode.	x							

23	Smartphone und Tablet	<b>Updates von Betriebssystem und Apps</b> Updates des Betriebssystems und der eingesetzten Apps bei Hinweis auf neue Versionen immer zeitnah installieren, um Schwachstellen zu vermeiden. Legen Sie zusätzlich einen festen Turnus (z.B. monatlich) fest, in dem das Betriebssystem und alle genutzten Apps auf neue Versionen geprüft werden.	x																	
24	Smartphone und Tablet	<b>Datenschutz-Einstellungen</b> Der Zugriff von Apps und Betriebssystem auf Daten und Schnittstellen Ihrer Geräte sollten Sie in den Einstellungen restriktiv auf das Notwendigste einschränken.		x																
25	Mobiltelefon	<b>Sperrmaßnahmen bei Verlust eines Mobiltelefons</b> Bei Verlust eines Mobiltelefons muss die darin verwendete SIM-Karte zeitnah gesperrt werden. Hinterlegen Sie die dafür notwendigen Mobilfunkanbieter-Informationen, um sie bei Bedarf im Zugriff zu haben.			x															
26	Mobiltelefon	<b>Nutzung der Sicherheitsmechanismen von Mobiltelefonen</b> Alle verfügbaren Sicherheitsmechanismen sollten auf den Mobiltelefonen genutzt und als Standard-Einstellung vorkonfiguriert werden.		x																
27	Mobiltelefon	<b>Updates von Mobiltelefonen</b> Es sollte regelmäßig geprüft werden, ob es Softwareupdates für die Mobiltelefone gibt.			x															
28	Wechseldatenträger / Speichermedien	<b>Schutz vor Schadsoftware</b> Wechseldatenträger müssen bei jeder Verwendung mit einem aktuellen Schutzprogramm auf Schadsoftware überprüft werden.	x																	
29	Wechseldatenträger / Speichermedien	<b>Angemessene Kennzeichnung der Datenträger beim Versand</b> Eindeutige Kennzeichnung für Empfänger, aber keine Rückschlüsse für andere ermöglichen.			x															
30	Wechseldatenträger / Speichermedien	<b>Sichere Versandart und Verpackung</b> Versand-Anbieter mit sicherem Nachweis-System, manipulationsichere Versandart und Verpackung.			x															
31	Wechseldatenträger / Speichermedien	<b>Sicheres Löschen der Datenträger vor und nach der Verwendung</b> Datenträger nach Verwendung immer sicher und vollständig Löschen. Ihr Rechner bietet dafür verschiedene Möglichkeiten.		x																
32	Netzwerk-sicherheit	<b>Absicherung der Netzübergangspunkte</b> Der Übergang zu anderen Netzen, insbesondere dem Internet, muss durch eine Firewall geschützt werden.	x																	
33	Netzwerk-sicherheit	<b>Dokumentation des Netzes</b> Das interne Netz ist inklusive eines Netzplanes zu dokumentieren.	x																	
34	Netzwerk-sicherheit	<b>Grundlegende Authentisierung für den Netzmanagement-Zugriff</b> Für den Management-Zugriff auf Netzkomponenten und auf Management-Informationen muss eine geeignete Authentisierung verwendet werden.	x																	

## BSI Checkliste für KMU Datensicherheit

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat die Aufgabe im Namen der Bundesregierung Informationen und Instrumente für Cyberschutz und Informationssicherheit bereitzustellen. Die in diesem Leitfaden angebotene Checkliste stellt eine pragmatische Mindestanforderung für KMU dar.

Über das cloudbasierte **MCSS Ökosystem** können alle weitergehenden Dokumente wie Schulungsunterlagen, Checklisten, Erklärvideos, Wissenstests und Textvorlagen abgerufen werden: Hauptmenü „Coaching“.

**IT-Sicherheitsregelung für die Beauftragten** MC-SMARTLEARN

Die folgende Inhaltsübersicht listet alle für die Beauftragten relevanten Dokumente, Anweisungen und Schulungen. Diese können jederzeit auch mobil aufgerufen werden.



Basis-Schulung IT-Sicherheit



Team-Meetings IT-Sicherheit



Einsatz von Virenschutz



Einsatz von Firewall-Software



Internet Anwendungen



Einsatz mobiler Endgeräte



Anwendung von Passwörtern



Zutritts-, Zugangs- & Zugriffsschutz



Durchführung der Datensicherung



IT-Sicherheit im Qualitätsmanagement



Optimierungsmanagement mit PDCA Anwendung



IT-Notfallmanagement

# Anwendungshinweise zur Sicherheits-Checkliste und der Curriculum-Vorlage zur IT-Sicherheit

## Überblick

Nach **Art. 32** der Datenschutz-Grundverordnung (DSGVO) ist das Unternehmen verpflichtet, die Sicherheit der Datenverarbeitung in der Organisation zu gewährleisten. Das gilt sowohl im Kontext der Informationssicherheit wie auch in Bezug auf den Datenschutz.

## Checkliste zu den BSI Anforderungen zur Informationssicherheit

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) befasst sich mit allen Fragen rund um die IT-Sicherheit in der Informationsgesellschaft. Ziel des BSI ist es, den sicheren Einsatz von Informations- und Kommunikationstechnik in unserer Gesellschaft zu ermöglichen und voranzutreiben. Das BSI wurde am 1. Januar 1991 gegründet und gehört zum Geschäftsbereich des Bundesministeriums des Innern und für Heimat.

### • Wer kann die Checkliste bearbeiten?

- Mitarbeitende mit Grundkenntnissen zum Einsatz von Informationstechnologie können die Checkliste für die Organisation bearbeiten.
- Falls notwendig, kann der externe IT-Partner/die externe IT-Partnerin einbezogen werden.

### • Was wird in die Checkliste eingetragen?

- In den Spalten „Priorität“ sind bereits die Prioritäten 1-3 eingetragen. Bei der Umsetzung wird empfohlen, mit Priorität 1 (sehr wichtig) zu starten. Anschließend können die weiteren Prioritäten bearbeitet werden.
- In den rechten Spalten kann eingetragen werden, wie der Status bei der Umsetzung der einzelnen Anforderung aktuell zum Start des Projekts ist:
  - **0%** = noch nicht begonnen oder nicht relevant
  - **50%** = bereits eingeleitet und in Bearbeitung
  - **100%** = vollständig umgesetzt
- In jeder Organisation ist es wichtig, dass die Zuständigkeit und Verantwortung klar definiert sind. Es wird empfohlen, 2 Mitarbeitende als Koordinierende einzusetzen (inkl. einer Vertretung).
- Als Datum kann man das Datum der ersten Statusanalyse eintragen. Natürlich kann man die Checkliste auch kopieren und den Status regelmäßig (z.B. alle 3 Monate) überprüfen.

### • Welche Informationen stehen zusätzlich zur Verfügung?

- Im Rahmen der Cyber-Versicherung steht das digitale **MCSS Ökosystem** zur Verfügung. Über den individuellen Zugangs-Code (siehe E-Mail) kann das cloudbasierte System genutzt werden. In der Cloud stehen alle relevanten Unterlagen wie Verfahrensanweisungen, Checklisten und Trainingsunterlagen zur Verfügung.
- Die **MCSS AG** als Partnerin der Cyber-Versicherung bietet auch unterstützende Webinare an. Die Termine erfährt man unter [www.mcass-ag.de](http://www.mcass-ag.de).

## Curriculum (Einführungsplan) für 12 Monate

Je nach Reifegrad der eigenen Organisation und der verfügbaren Kapazitäten und Qualifikationen benötigen Unternehmen zwischen 12 und 24 Monate zur vollständigen Umsetzung der Regelung. In diesem Leitfaden-Dokument ist eine Beispiel-Vorlage für 12 Monate enthalten:

### • Wie können die Aufgaben eingeteilt werden?

- Die Aufgaben sind unterteilt nach 3 Rubriken:
  - Informationssicherheit nach Art. 32 DSGVO
  - Datenschutz nach DSGVO/BDSG
  - Qualitätsmanagement (beispielsweise nach der ISO 9001 Norm)
- Je nach interner Organisation können die einzelnen Bereiche parallel bearbeitet werden. Wenn sowohl Datenschutz wie auch QM optimal umgesetzt sind, kann jeweils nur die Aufgabe zur Informationssicherheit (IS) bearbeitet werden.

### • Welche Unterstützung steht für die Umsetzung nach Curriculum zur Verfügung?

- Die Organisationen werden im Rahmen der Cyber-Versicherung durch Webinare unterstützt. Pro Quartal wird ein Webinar (40 min.) angeboten. Die Inhalte entsprechen den Aufgaben im Curriculum.
- Für alle Aufgaben stehen in der Cloud umfangreiche Vorlagen (wie Verfahrensanweisungen, Wissenstests, Erklärvideos etc.) zur Verfügung: Man wählt im Hauptmenü den Bereich „Coaching“.



# Einführung in die Informationssicherheit (MC-SMARTLEARN)

## 1 IT-Sicherheitsregelungen nach Art. 32 DSGVO

- Mit Inkrafttreten der **Datenschutz-Grundverordnung** gelten auch Regelungen für die Datensicherheit und den Cyberschutz.
- Nach **Art. 32 DSGVO** müssen Maßnahmen zur Sicherheit der Datenverarbeitung umgesetzt werden.
- Wichtig ist, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall zeitnah wiederherzustellen.
- Die wichtigsten verpflichtenden Anforderungen sind:
  - Regelmäßige Datensicherungen
  - Einsatz von Virenschutzprogrammen
- Weitere Anforderungen sind:
  - Regelungen für **Berechtigungen und Zugriffe** zu IT-Systemen
  - **Schutz vor „Phishing“** und Schadprogrammen
- Weitere Standards sind:
  - Einsatz von **Firewalls**
  - Regelungen für die Netzwerk-Administration
- Die entsprechenden Regelungen können im Zusammenhang mit einem **QM-System** etabliert werden.

## 2 Anwendung von Passwörtern

- Es ist bekannt, dass schlecht gewählte Passwörter, wie beispielsweise 123456, viel zu unsicher und leicht zu „hacken“ sind.
- Auch ein und dasselbe Passwort für viele verschiedene Programme oder Zugänge zu nehmen, ist ebenfalls sehr riskant.
- Namen, Geburtsdaten oder dergleichen sind nicht als Passwörter geeignet.
- Das vollständige Passwort sollte möglichst nicht in Wörterbüchern vorkommen, da Hacker-Systeme alle gebräuchlichen Wörter in Sekundenbruchteilen „knacken“ können.
- Ein gutes Passwort sollte mindestens acht Zeichen lang sein und Sonderzeichen, Zahlen sowie Groß- und Kleinbuchstaben enthalten.
- Passwörter sollten nicht offen im System gespeichert werden und natürlich auch nicht auf Zetteln (Post-it) aufgeschrieben werden.
- Ein Passwort sollte nur dann geändert werden, wenn Verdacht auf einen Missbrauch besteht.
- Weitere Informationen erhält man über das **Bundesamt für Sicherheit in der Informationstechnik** ([www.bsi.org](http://www.bsi.org)) unter dem Stichwort „Passwort“.

## 3 Einsatz von Firewalls + Virenschutz

- In der IT-Sicherheit spielt eine Firewall („Feuerwand“/Brandschutzwand) eine wichtige Schutz-Rolle.
- Die Firewall ist ein digitaler „Türsteher“, der ankommende und abgehende Datenpakete im Netzwerk kontrolliert und regelt.
- Die Firewall ist ein Baustein des IT-Sicherheitskonzepts. Diese muss ständig aktualisiert werden.
- Die Koordination der Firewall wird von den IT-Verantwortlichen übernommen. Sie benötigen die Kooperation aller Nutzenden, z.B. bei der Meldung von Vorkommnissen.
- Zusätzlich zur Firewall wird ein „**Virenschutzprogramm**“ von den IT-Verantwortlichen eingesetzt.
- Es kann entweder ein Virenschutz über das Betriebssystem (z.B. MS Windows) oder ein externer Virenschutz eingesetzt werden.
- **Meldungen am Bildschirm** sind aufmerksam zu lesen, Hinweise sind zu beachten und bei Wichtigkeit (zeitnah) weiterzugeben.
- Es ist wichtig, dass alle Mitarbeitenden wissen, an wen relevante **Informationen zu melden** sind und auch dass klar ist, wem man Fragen stellen kann.
- Mehr Informationen zur Firewall und Virenschutz erhält man vom **Bundesamt für Sicherheit in der Informationstechnik (BSI)**. Im Internet erreicht man das Bundesamt über [www.bsi-fuer-buerger.de](http://www.bsi-fuer-buerger.de).



## 4 Prävention Phishing Angriffe

- Als Phishing bezeichnet man den Eingang betrügerischer E-Mails, die zu Handlungen auffordern, die von Kriminellen zu Schädigungen genutzt werden.
- Wichtig ist, dass diese Phishing-Mails erkannt und sofort neutralisiert werden.
- Am besten erkennt man Phishing an gefälschten Absendenden-Adressen.
- Zuerst ist die E-Mail-Adresse der absendenden Person durch **Vergleich mit bekannten Adressen zu prüfen**.
- Die wichtigsten Fragen: Kann die absendende Person den Versand der Mail **telefonisch bestätigen**?
- Werden vertrauliche Daten abgefragt oder fordert die E-Mail zur Eingabe **persönlicher Informationen**?
- Werden Geheimnummern oder Passwörter abgefragt?
- Signalisiert die E-Mail Dringlichkeit oder Handlungsbedarf?
- Enthält die E-Mail Verlinkungen, die auf **andere Webseiten** verweisen?
- Welche Ziel-URL wird bei einem Mouseover angezeigt?
- Ist die Anrede unpersönlich formuliert oder enthält der Text Rechtschreib- oder Zeichenfehler?
- Das Motto für mehr Cybersicherheit: **Besser einmal zu viel prüfen** und richtig reagieren als unkonzentriert einfach „klicken“. Aufmerksamkeit ist Professionalität.

## 5 Private Nutzung Internet/eigene Geräte

- Die Nutzung von Smartphones und Tablets erfordert besondere Sicherheitsmaßnahmen.
- Es müssen immer aktuelle Schutzprogramme vor „**Phishing**“ und Schadprogrammen im Browser genutzt werden.
- SIM-Karten sollten grundsätzlich durch eine **PIN** geschützt werden.
- Die **Super-PIN/PUK** sind grundsätzlich nur durch Verantwortliche anzuwenden.
- Besonders auf mobilen Endgeräten sollten die strengsten & sichersten Einstellungen gewählt werden.
- Alle mobilen Geräte sollten mit einem komplexen Gerätesperrcode geschützt werden.
- Damit Schwachstellen vermieden werden, müssen **Updates** des Betriebssystems und der eingesetzten Apps **zeitnah** installiert werden.
- Es ist sinnvoll, einen festen Turnus (z.B. monatlich) festzulegen, in dem das Betriebssystem und alle genutzten Apps auf neue Versionen geprüft werden.
- Zugriffe von Apps auf Daten und Schnittstellen der mobilen Geräte sollten in den **Einstellungen restriktiv auf das Notwendigste** eingeschränkt werden.

## 6 Zutritts-, Zugangs- und Zugriffsschutz

- Die technischen Maßnahmen zur IT-Sicherheit sind Teil eines einrichtungsinternen QM.
- Alle wichtigen Räumlichkeiten sind durch **Sicherheitsschlösser, Alarmsicherung, Videoüberwachung** und andere Sicherungen zu schützen.
- Die Datensicherungsaufbewahrung ist z.B. durch geeignete **Tresore** zu planen oder über **externe Back-Ups** zu realisieren.
- Wichtiger als die technischen Maßnahmen sind die organisatorischen Umsetzungen des Zutrittsschutzes.
- Zu den organisatorischen Maßnahmen gehören **Schulungen**, verständliche Verfahrensanweisungen, Regelungen für Servicepersonal und ein Protokollbuch für IT-Serviceeinsätze.
- Die wichtigsten Regelungen zur IT-Sicherheit sind **Prozessbeschreibungen** zur Datensicherungserstellung, -aufbewahrung und/oder der externen Archivierung.
- Zum Standard gehören Regelungen zum Gebäudezugang mit einem allgemeinen **Schlüsselmanagement**, inklusive Schlüsselverlust-Regelungen.
- Die Ergebnisse der Evaluierung zum Zutrittsschutz sind in Protokollen für den **Jahres-Sicherheitsbericht** zu dokumentieren.

## 7 Kommunikation im Team

- Mehr als 70% der ungeplanten Vorfälle in der Informationssicherheit sind auf den „**Faktor Mensch**“ zurückzuführen.
- Im Informationssicherheitsmanagement spielt deshalb die **Orientierung, Aufklärung und Schulung** des gesamten Teams eine zentrale Rolle.
- Am Anfang steht die Orientierung über die Regulatorik wie **Gesetze, Verordnungen, Richtlinien etc.**
- Dies kann z.B. über **Merkblätter** oder kurze digitale **Storyboards** erfolgen.
- Außerdem können Aufklärungen zu Cyberschutz und Informationssicherheit in die **Standard-Schulungen** der Mitarbeitenden einbezogen werden.
- In **Teambesprechungen** können die Wissensbereiche Informationssicherheit und Datenschutz in der Einrichtung als regelmäßige Besprechungspunkte aufgenommen werden.
- Bei aktuellen Risiken oder bei bereits eingetretenen Störfällen ist die Unterrichtung des Teams je nach Infrastruktur zu organisieren: z.B. über **Sofort-Meldungen** auf das Mobiltelefon oder per Aushang.
- Die Kommunikation im Team ist so wichtig, dass sie ständig zu **überprüfen** und dann zu **verbessern** ist.

## 8 IT-Notfallmanagement

- Wichtig für das Verhalten bei IT-Notfällen: **Ruhe bewahren** & IT-Notfall melden:  
Besser einmal mehr als einmal zu wenig anrufen!
- Standard ist: **Meldungen an IT-Sicherheitsbeauftragte** und IT-Sicherheitskoordinierende, Einrichtungsleitung sowie bei kritischen Störungen an die IT-Dienstleistenden.
- Nach der Meldung des Notfalls sind unverzüglich die erforderlichen **Sofortmaßnahmen** zu ergreifen.
- Zielsetzung des Notfallmanagements ist es, zu verhindern, dass die Unterbrechung oder Störung von wichtigen Prozessen der Organisation betroffen sind.
- Daher sollten möglichst rasch die vorbereiteten **Kontinuitätspläne** aktiviert werden:
  - Mitarbeitende ausführlich informieren, Aktionsplan einbeziehen, **Reservesystem aktivieren**, Rekonstruktion der Datensicherung mit IT-Verantwortlichen vorbereiten.
  - Mögliche **Terminverschiebung organisieren** und betroffene Personen informieren.
  - Sobald alle Voraussetzungen für einen funktionsfähigen Normalbetrieb erfüllt sind, kann er wieder mit Protokoll aufgenommen werden.
  - **Aus Krisen kann gelernt werden:** Wie kam es dazu? Welche Auswirkungen hat es? Festgestellte Mängel und **Verbesserungsmöglichkeiten** werden offen kommuniziert und zeitnah umgesetzt.

# Einführung in den gesetzlichen Datenschutz (MC-SMARTLEARN)

## 1 Kenntnisse der rechtlichen Verpflichtungen wie DSGVO/BDSG

- In Organisationen mit Verarbeitung von **Personendaten** hat Datenschutz eine hohe rechtliche und wirtschaftliche Bedeutung.
- Für viele Organisationen gilt eine berufliche Schweigepflicht aber in jedem Fall die **Datenschutz-Grundverordnung (DSGVO)** und das **Bundesdatenschutzgesetz (BDSG)**.
- Die Datenschutz-Grundverordnung ist eine verpflichtende Europa-Vorschrift.
- Sie besteht aus insgesamt 99 Artikeln in 11 Kapiteln und definiert konkrete Verpflichtungen, die in den Organisationen umzusetzen sind.
- Weitergehende Verpflichtungen ergeben sich aus dem nationalen Bundesdatenschutzgesetz (BDSG).
- Alle Mitarbeitenden sind in **dokumentierten Schulungen** auf alle diese Datenschutz-Rahmenbedingungen zu verpflichten.

## 2 Datenschutzleitlinien

- Datenschutz ist Teamarbeit und macht regelmäßige Kommunikation und Aktualisierung erforderlich.
- Alle Mitarbeitenden müssen Ziele, Bedingungen und die Maßnahmen kennen.
- Die zentralen Elemente werden in der **Datenschutzleitlinie** definiert.
- Ergänzt wird die Leitlinie durch **Datenschutzrichtlinien** für spezielle Situationen und Abläufe.
- Die Datenschutzleitlinie ist ein Dokument für die interne und möglicherweise externe Kommunikation (z.B. als Datenschutzerklärung).
- Es wird empfohlen, die **Datenschutzleitlinie als Bestandteil in die Verträge mit allen Mitarbeitenden aufzunehmen**.

## 3 AV-Verträge

- Datenschutz ist auch in der Kooperation mit Partner\*innen eine zentrale Anforderung.
- In der DSGVO ist die Zusammenarbeit mit den sogenannten **Auftragsverarbeitenden** genau geregelt.
- Auftragsverarbeitende sind Dienstleistende, die im Rahmen einer Vereinbarung Zugriff auf Informationen und auch Personendaten erhalten können.
- Dazu gehören z.B. **IT-Dienstleistende und Berater\*innen**. Ausgenommen sind Steuerberater\*innen und andere Berufe, die einer Geheimhaltungspflicht unterliegen.
- In AV-Verträgen werden alle datenschutzrechtlichen Verpflichtungen mit den externen Partnerunternehmen dokumentiert.

## 4 Zustimmungen zur Datenverarbeitung

- Die Verarbeitung personenbezogener Daten ist generell verboten, solange sie nicht durch ein Gesetz ausdrücklich erlaubt ist oder die Betroffenen in die Verarbeitung eingewilligt haben.
- Die grundsätzlichen Anforderungen an die Wirksamkeit einer **rechtsgültigen Einwilligung** sind in Art. 7 DSGVO festgehalten.
- Die Einwilligung sollte durch eine eindeutige bestätigende Handlung erfolgen, mit der freiwillig, für den konkreten Fall, unmissverständlich die Einwilligung bekundet wird.
- Es ist sinnvoll, dass überall dort, wo Einwilligungen eingeholt werden müssen, entsprechende **Vorlagen analog oder digital** vorhanden sind.
- Beruht die Verarbeitung auf einer Einwilligung, muss der oder die Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.
- Da eine Aufbewahrungspflicht nicht gesetzlich festgelegt ist, richtet sich die **Dauer der Speicherung der Einwilligung** nach den individuellen Anforderungen der Verarbeitung.
- Es empfiehlt sich, dass die Regelungen in **Zusammenarbeit mit dem oder der DSB** festgelegt werden.

## 5 Weitergabe von Personendaten

- Die Weitergabe personenbezogener Daten an Dritte ist grundsätzlich ohne Zustimmung der betroffenen Personen nach DSGVO und BDSG **nicht** zulässig.
- Beispiele für Standarddaten sind etwa all jene Informationen, die sich auf **Anschrift, Alter und Geburtsort einer natürlichen Person** beziehen.
- Besondere Daten nach Art. 9 DSGVO sind speziell auch medizinische und soziale Daten, die berufsmäßig verarbeitet werden.
- Für solche Datenverarbeitungen gelten zusätzlich zu der DSGVO und dem BDSG auch berufliche Geheimhaltungspflichten im Gesundheits- und Sozialbereich.
- Wird die Datenweitergabe in Ausnahmefällen gestattet, darf die Datenübermittlung nur **verschlüsselt** und in getrennter Form erfolgen.
- Auch das Anonymisieren personenbezogener Daten ist eine Option für eine rechtskonforme Datenweitergabe.
- Die regelmäßige Weitergabe von Personendaten wird in Zusammenarbeit mit den DSB geregelt und in Prozessbeschreibungen dokumentiert.
- Mögliche Datenpannen im Zusammenhang mit der Weitergabe von Personendaten sind umgehend den Verantwortlichen zu melden und zu dokumentieren.
- In kritischen Fällen ist die zuständige Kontrollbehörde über eine Datenpanne zu informieren.

## 6 Geheimhaltung & berufliche Schweigepflicht

- Eine besondere **Schweigepflicht** gilt für Berufsgruppen, die aufgrund ihrer Tätigkeiten Personendaten regelmäßig verarbeiten.
- Zu diesen Berufsgruppen zählen Ärzt\*innen, Zahnärzt\*innen, Apotheker\*innen, Berufspsycholog\*innen und andere Heilberufe, deren Befähigung auf einer staatlichen Ausbildung basiert.
- Ebenfalls einer beruflichen Geheimhaltung unterliegen Rechtsanwält\*innen, Steuerberater\*innen, Wirtschaftsprüfer\*innen und vergleichbare Berufsgruppen mit staatlicher Ausbildung.
- Alle **Mitarbeitenden**, die den Berufsgruppen **mit Schweigepflicht** direkt oder indirekt zuarbeiten, unterliegen ebenfalls der gesetzlichen Schweigepflicht.
- Mit den Gruppen mit berufsbedingter Schweigepflicht können ohne AV-Vertrag und ohne besondere Vereinbarung auch personenbezogene Daten ausgetauscht werden.

## 7 Einzelregelungen der DSGVO

- Die Datenschutz-Grundverordnung besteht aus insgesamt 99 Artikeln in 11 Kapiteln.
- Eine wichtige Einrichtung der DSGVO ist die Benennung eines **Datenschutzbeauftragten/einer Datenschutzbeauftragten, DSB** genannt.
- Für größere Organisationseinheiten mit **20 und mehr Mitarbeitenden** sind DSB Benennungen verpflichtend.
- Der Umfang technischer und organisatorischer Maßnahmen, auch **TOM** genannt, ist abhängig von der Verarbeitung der Personendaten in einer Organisation.
- Für medizinische und soziale Einrichtungen gelten besondere Anforderungen nach Art. 9 der DSGVO.
- Aber auch im Gastgewerbe und in der Touristik können besondere Vorschriften gelten, wenn sensible Personendaten verarbeitet werden, z.B. bei Behinderungen von Personen.
- Die wichtigsten Regelungen der DSGVO werden in **internen Richtlinien** dokumentiert.
- Die Richtlinien beschreiben technische und organisatorische Maßnahmen (TOM) in allen Arbeitsbereichen.
- Die Datenschutzrichtlinien können organisatorisch als Prozessbeschreibungen/Verfahrensanweisungen oder Checklisten im **Qualitätsmanagement** umgesetzt werden.

## 8 Verhalten bei Datenpannen

- Auch der professionellste Datenschutz kann Störfälle nicht vollständig vermeiden.
- Kommt es zu Datenschutzverstößen und -störungen, muss ein **Notfallplan** abgerufen werden.
- Der Notfallplan beginnt mit der **Klassifizierung des Datenschutzverstoßes** nach der Dimension: Wie viele Personendaten sind betroffen?
- In kritischen Fällen gilt eine Pflicht zur **Meldung** an die zuständige Aufsichtsbehörde.
- Bei meldepflichtigen Datenpannen sind Fristen einzuhalten. In der DSGVO ist eine **Meldefrist von maximal 72 Stunden** definiert.
- Unabhängig von ihrer Klassifizierung sind alle **Unregelmäßigkeiten** im Zusammenhang mit dem Datenschutz **zu dokumentieren**.

**Anlage zum Vertrag mit (Name)**

**vom (Datum)**

## **Generelle Orientierung**

Cyberschutz, Informationssicherheit, Datenschutz und auch Personensicherheit stellen besondere verpflichtende Anforderungen an alle Mitarbeitenden. Die folgenden Anforderungen stellen die wichtigsten gesetzlichen Regelungen, die zu befolgen sind, global zusammen:

### **Informationssicherheit und Cyberschutz**

Die Gefahren für die Informationssicherheit, Cyber- und Datenschutz sind in den vergangenen Monaten und Jahren erheblich gestiegen. Die Statistiken zeigen, dass über 70% der Schadensfälle auf den „Faktor Mensch“ zurückzuführen sind. Deshalb ist die verantwortliche Mitwirkung der Mitarbeitenden bei allen technischen, organisatorischen und rechtlichen Maßnahmen von elementarer Bedeutung. Dazu werden den Mitarbeitenden angemessene Orientierungen und Schulungen angeboten.

### **Datenschutz (z.B. DSGVO, BDSG)**

Der Datenschutz und die Datensicherung sind auf EU-Ebene und nationaler Ebene geregelt. Es gelten insbesondere die europäische Datenschutz-Grundverordnung (DSGVO) und das Bundesdatenschutzgesetz (BDSG).

### **Personensicherheit**

Die Sicherheit aller Personen in der Organisation hat höchste Priorität. Dazu gelten z.B. die Anforderungen nach dem Infektionsschutzgesetz (IfSG), die Unfallverhütungs-Bestimmungen und die Vorschriften der Berufsgenossenschaften (BGV).

### **Notfallmanagement (z.B. BG Vorschriften)**

In allen Organisationseinheiten mit Mitarbeitenden und Kund\*innen, Gästen und Partner\*innen müssen Vorkehrungen für Notfälle getroffen werden. Diese sind sowohl gegen Personenschäden wie auch Eigentumsschäden einzuführen.

Für Notfälle werden betriebliche Versicherungen abgeschlossen, um Schäden zu begrenzen. Versicherungen sind zur Schadensregulierung nur verpflichtet, wenn die vereinbarten Schutzmaßnahmen eingehalten werden (sogenannte Obliegenheiten).

### **Weiterbildungsverpflichtung**

Die Mitarbeitenden haben Zugang zu den wesentlichen und relevanten Wissensinhalten durch analoge und durch digitale Schulungsangebote. Dazu steht ein gedruckter Leitfaden (analoge Schulung) und ein Trainingsprogramm über Smartphone-Nutzung zur Verfügung.

Die Mitarbeitenden sind verpflichtet, diese Schulungs- und Weiterbildungsangebote regelmäßig zu nutzen und dies als Nachweis zu dokumentieren.

Datum/Unterschrift

## Zusatzvereinbarung zum IT-Service- und Lizenzvertrag vom (Datum)

Nach den Bestimmungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) sind Unternehmen verpflichtet, die angemessene Datensicherheit zu gewährleisten (Art. 32 DSGVO „Datensicherheit“)

Zu den Maßnahmen und Anforderungen gehören insbesondere nach der aktuell beschlossenen Fassung:

- Passwort-Management nach dem Stand der Technik
- Schutz und Protokollierung des Zugriffs auf Arbeitsplatzrechner
- Einsatz von Virenschutz-Programmen und IT-Firewalls
- Datensicherung, Archivierung und Datenrekonstruktion (intern und extern)
- Austausch, Entsorgung und Reparatur von IT-Systemen und Datenträgern
- Rollen- und Rechtevergabe inkl. Administrationsmanagement
- Jährliche Überprüfung und Anpassung der Sicherheitsmaßnahmen

Hiermit wird bestätigt, dass mit dem bestehenden o.g. Vertragsverhältnis die o.g. Funktionen und Maßnahmen der Datensicherheit erfüllt werden.

Soweit die konkret verpflichtenden Anforderungen nicht zu den vereinbarten Leistungen gehören, werden sie im Folgenden aufgelistet:

Liste der nicht durch das Vertragsverhältnis geregelten IT-Sicherheitsfunktionen und -maßnahmen:

- 1
- 2
- 3
- 4

(Evtl. genauere Spezifikation in einem mitgeltenden Dokument der Vertragspartner\*innen)

Mitgeltende Dokumente:

- Original Dienstleistungs- und Wartungsvertrag
- Dokumentation der IT-Infrastruktur der Auftraggebenden

Datum/Unterschrift

Datum/Unterschrift

Auftraggebende/r

Auftragnehmende/r

## **Leitlinie zur Informationssicherheit**

Im Interesse von Kund\*innen, Mitarbeitenden und Partner\*innen des Unternehmens müssen Daten und IT-Prozesse durchgängig und wirksam vor Missbrauch und dem Verlust der Integrität, Vertraulichkeit und Verfügbarkeit bewahrt werden.

Informationsverarbeitung und -sicherheit spielt damit eine Schlüsselrolle für unsere Aufgabenerfüllung. Alle wesentlichen strategischen und operativen Funktionen und Aufgaben werden durch Informationstechnik (IT) maßgeblich unterstützt. Ein Ausfall von IT-Systemen muss insgesamt kurzfristig kompensiert werden können. Auch in Teilbereichen muss unser Unternehmen immer funktionsfähig bleiben.

Die Informationssicherheit hat für alle Verantwortlichen durch die rechtliche Verankerung der Schweigepflicht in Gesetzen und Verordnungen eine besonders hohe Priorität. Deshalb haben aktuelle Schulungen aller Personen einen hohen Stellenwert.

### **Übergeordnete Ziele**

Angemessene Informationssicherheit ist integraler Bestandteil der Politik des Unternehmens und leistet einen unverzichtbaren Beitrag zum Erfolg der Versorgung. Informationssicherheit ist an den Geschäftszielen ausgerichtet und wird von der Leitung verantwortet. Unsere Daten und unsere IT-Systeme in allen technikabhängigen Bereichen werden in ihrer Verfügbarkeit so gesichert, dass die zu erwartenden Stillstandzeiten toleriert werden können. Fehlfunktionen und Unregelmäßigkeiten in Daten und IT-Systemen sind nur in geringem Umfang und nur in Ausnahmefällen akzeptabel (Integrität).

Die Standard-Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der schützenswerten Informationen und IT-Systeme stehen. Schadensfälle mit hohen finanziellen Auswirkungen müssen verhindert werden. Alle Mitarbeitenden der Organisation halten die einschlägigen Gesetze und Verordnungen (z.B. DSGVO Datenschutz-Grundverordnung, Strafgesetzbuch und Vorschriften zur beruflichen Schweigepflicht) und vertraglichen Regelungen ein. Dazu gehören auch die Verpflichtungen aus Versicherungsverträgen (z.B. Obliegenheiten aus Cyber-Versicherungen). Dazu werden auch die Zusatzvereinbarungen zu Arbeitsverträgen rechtskonform angepasst.

Negative finanzielle und immaterielle Folgen für das Unternehmen sowie für die Mitarbeitenden durch Gesetzesverstöße sind zu vermeiden. Alle Mitarbeitenden und die Leitung sind sich ihrer Verantwortung beim Umgang mit IT bewusst und unterstützen die Sicherheitsstrategie nach besten Kräften. Alle Personen sind zur Einhaltung der IT-Sicherheitsmaßnahmen verpflichtet. Externe Vertragspartner\*innen sind in rechtskonformen Verträgen ebenso zu verpflichten.

Die Leitlinie wird bei Bedarf den technischen, organisatorischen und rechtlichen Anforderungen angepasst.



# Verfahrensanweisung (VA) „Schulung zur IT-Sicherheit in kleinen und mittleren Unternehmen“ (KMU)“

## Übersicht

Diese VA dient der internen Unterstützung der Informationssicherheitskoordinierenden (ISK) in kleinen und mittleren Unternehmen/Organisationen, speziell bei der rechtskonformen Umsetzung der Cyberschutz-, Informationssicherheit und Datenschutz-Rahmenbedingungen.

## Ziel und Zweck

Die Verfahrensanweisung hat das Ziel, die Abläufe und allgemeinen Regelungen zu Informationssicherheit und Datenschutz in strukturierten Prozessen und Verfahren transparent umzusetzen und gut verständlich darzustellen. Ziel dieser Beschreibung ist die Vereinheitlichung der Abläufe und der Sicherstellung der Vollständigkeit und Qualität.

## Anwendungsbereich

Diese Anweisung gilt für die Durchführung von Schulungen zur konformen Anwendung der rechtlichen Rahmenbedingungen und insbesondere der Datenschutz-Grundverordnung (DSGVO). Die Schulungen beziehen sich auf Anwendungen der IT-Sicherheit im Bereich der Verwaltung und der Informationstechnologie (z.B. Kund\*innendaten-Verwaltung). Der Anwendungsbereich ist unabhängig von den Standorten der Einheiten und ist definiert für alle Bereiche, in denen personenbezogene Daten erfasst, verarbeitet, übertragen und gespeichert werden.

## Verantwortung

Verantwortlich für die einzelnen Segmente des Verfahrens sind dazu beauftragte Personen, insbesondere:

- Leitung / Mitglieder der Geschäftsleitung
- Informationssicherheitsbeauftragte (ISB)
- Externe Dienstleistende, soweit rechtlich geregelt (externe IT-Sicherheitsberatende)

Die individuellen Verantwortungsbereiche sind in Protokollen, falls vorgesehen, zu dokumentieren.

## Prozesse

Die Schulungen können nach 4 Alternativen durchgeführt werden:

- Schulung im Selbststudium
- Schulung in Team Meetings
- Videoschulungen
- Schulung in Webinaren durch externe Dienstleistende

Die Schulungen bestehen aus unterschiedlichen Schulungsmodulen, **MC-SMARTLEARN**:

- Erklärvideos zu Informationssicherheit (IS) und Datenschutz (DS)
- Checklisten zu IS und DS
- „Multiple Choice“ Fragen zur Überprüfung des Wissensstatus (Wissenstests)

## Schulung im Selbststudium (Schulungsvideos)

Unabhängig von Terminen können Teammitglieder zeitgünstig die Schulungsfragen mit den Antworten durcharbeiten. Dabei kann man pro Frage und Antwort ca. 3 Minuten planen (bei 20 Fragen und Antworten ca. eine Stunde). Es empfiehlt sich, ein Protokoll anzufertigen, das als Nachweisdokument für die Geschäftsleitung dienen kann.

Auf dem Protokoll werden vermerkt:

- Name des Teammitglieds
- Rolle / Funktion im Unternehmen
- Inhalt der Schulung (Hauptthema und Stufe)
- Erst- oder Folgeschulung zum Thema
- Datum des Selbststudiums
- Uhrzeit von - bis der Selbstschulung
- Offene Fragen für DSB oder Unternehmensleitung
- Antworten zu den Fragen

Die Nachweisprotokolle werden im Ordner „Mitgeltende Dokumente“ abgelegt.

## Schulung in Team Meetings

Eine effektive Schulung der Mitarbeitenden kann integriert in Team Meetings durchgeführt werden. Die Koordinierenden können IT-Sicherheitsbeauftragte, Datenschutzbeauftragte oder externe Dienstleistende (z.B. **MCSS AG**) sein.

Die Schulungseinheiten richten sich nach dem Status der Datenschutz-Ausbildung. Eine Einheit soll maximal 90 Minuten dauern (ca. 20-30 Fragen und Antworten).

Als Nachweisdokument fertigt die Schulungsleitung ein Protokoll mit folgenden Angaben an:

- Titel und Thema der Schulung
- Referent\*in / Schulungs-Koordinator\*in
- Ort der Schulung
- Datum der Schulung
- Uhrzeit von - bis
- Teammitglieder
  - Namen
  - Rollen/Funktionen
  - Ersts Schulung/Folgeschulung

Die Nachweisprotokolle werden im Ordner „Mitgeltende Dokumente“ abgelegt.

## Schulung in Webinaren

Webinare sind Online-Schulungen, die von verschiedenen Organisationen und kommerziellen Anbieter\*innen veranstaltet werden. Es wird von den Verantwortlichen geprüft, welche Webinar-Angebote eine Rechtskonformität gewährleisten.

Im Regelfall bieten Anbieter\*innen von Schulungs-Webinaren auch Teilnahmenachweise. Ist dies nicht der Fall, dokumentieren die Mitarbeitenden ihre Teilnahme intern mit folgenden Angaben:

Name des Teammitglieds:

- Rolle/Funktion im Unternehmen
- Inhalt der Schulung (Hauptthema und Stufe)
- Veranstalter\*in des Webinars
- Erst- oder Folgeschulung zum Thema
- Datum des Webinars
- Uhrzeit von - bis des Webinars

Die Nachweisprotokolle werden im Ordner „Mitgeltende Dokumente“ abgelegt.

Hinweis: Webinare können „Live“ oder auch als „Konserven“ (Videoschulungen) angeboten werden.

## Dokumentation der Schulungen

Die Schulungen werden sowohl durch die Mitarbeitenden wie auch durch die Verwaltung dokumentiert.

Die Mitarbeitenden sammeln Kopien ihrer Schulungen in ihrem Qualifikations-Ordner für Audits und für Nachweise bei Wechsel des Arbeitsplatzes.

### **Mitgeltende Dokumente:**

- Curriculum ISMS/DSMS zur Umsetzung von IT-Sicherheit und Datenschutz
- Einführung in die Informationssicherheit für Mitarbeitende
- Einführung in den Datenschutz für Mitarbeitende

# Verfahrensweisung (VA) „Notfallmanagement im Rahmen der IT-Sicherheitsregelung in kleinen und mittleren Unternehmen (KMU)“

## Übersicht

In Art. 32 der Datenschutz-Grundverordnung (DSGVO) werden die Verpflichtungen zur Datensicherheit (insbesondere personenbezogen) geregelt.

Durch die Datensicherheit sollen alle Daten eines Unternehmens/einer Organisation in jeglicher Hinsicht geschützt werden. Damit ist ein Schutz vor Verlust, Verfälschung, Beschädigung oder auch Löschung gemeint. Die Ziele der Datensicherheit sind somit Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität.

## Ziel und Zweck

Die Verfahrensweisung hat das Ziel, die Abläufe und allgemeinen Regelungen zum Notfallmanagement in der Datensicherheit in strukturierten Prozessen und Verfahren transparent umzusetzen und gut verständlich darzustellen. Ziel dieser Beschreibung ist die Vereinheitlichung der Abläufe und die Sicherstellung des Prozesses, der geregelt wird und die Gewährleistung der Vollständigkeit sowie der geplanten Ergebnisqualität. Die Informationstechnologie ist heute wesentlicher Bestandteil jeder Organisation/jeden Unternehmens.

Es werden wesentliche sicherheitsrelevante Informationen zu Personen (z. B. Kund\*innen) und Prozessen benötigt. Fällt das IT-Netzwerk aus, so können beispielsweise wichtige Informationen fehlen und zu falschen Entscheidungen führen. Ziel dieser VA ist deshalb die transparente Regelung für Notfälle in der IT-Sicherheit.

## Anwendungsbereich

Diese Anweisung gilt für die Durchführung von Schulungen zur konformen Anwendung der rechtlichen Rahmenbedingungen und insbesondere der Datenschutz-Grundverordnung (DSGVO).

Die Schulungen beziehen sich auf Anwendungen der IT-Sicherheit im Bereich der Verwaltung und der Informationstechnologie (z.B. Kund\*innendaten-Verwaltung).

Der Anwendungsbereich ist unabhängig von den Standorten der Einheiten und ist definiert für alle Bereiche, in denen personenbezogene Daten erfasst, verarbeitet, übertragen und gespeichert werden.

## Verantwortung

Verantwortlich für die einzelnen Segmente des Verfahrens sind dazu beauftragte Personen, insbesondere:

- Leitung / Mitglieder der Geschäftsleitung
- Informationssicherheitsbeauftragte (ISB)
- Datenschutzbeauftragte (DSB) und Datenschutzkoordinierende (DSK)
- Externe Dienstleistende, soweit rechtlich geregelt (externe IT-Sicherheitsberatende)

Die individuellen Verantwortungsbereiche sind in Protokollen, falls vorgesehen, zu dokumentieren.

## Prozesse

Zur Gewährleistung der Datensicherheit muss ein professionelles Notfallmanagement etabliert sein. Die Verpflichtungen für die Notfallversorgung sind in verschiedenen Gesetzen, Verordnungen und Richtlinien dokumentiert.

Zu dem IT-Notfallmanagement gehört im ersten Schritt die Definition und Beschreibung eines IT-Notfalls.

Diese Festlegungen hängen von der einzelnen Organisation und dem Computerisierungsgrad ab.

So kann definiert werden, dass ein Notfall dann vorliegt, wenn wichtige Arbeitsplätze für einen längeren Zeitraum (z.B. länger als 15 Minuten) ausfallen. Für diesen Fall müssen Notfallpläne vorliegen, z.B. für unterbrochene oder abgebrochene Untersuchungen oder Therapien.

Konkrete Fragestellung: Wurde überprüft, ob es sich um einen tatsächlichen IT-Notfall handelt, erfolgt die Meldung an den oder die IT-Verantwortliche\*n? Dies erfolgt im Regelfall über ein Mobiltelefon, das immer unabhängig vom Computer- und Stromnetzwerk funktionieren muss. Dazu müssen die Notfallnummern wie auch die Telefonnummern der Feuerwehr, des notärztlichen Dienstes und der Polizei bekannt und deutlich sichtbar ausgehängt sein.

Für die praktische Nothilfe muss ein Aushang vorhanden sein, der die IT-Notfallbeauftragten und ihre Telefonnummern enthält. Weiterhin müssen Verfahrensweisungen oder interne Regelungen im Rahmen des Qualitätsmanagements vorliegen.

Danach sind die verschiedenen IT-Notfälle zu klassifizieren:

- Ausfall eines einzelnen IT-Arbeitsplatzes
- Ausfall aller IT-Arbeitsplätze einer Abteilung
- Ausfall des gesamten IT-Netzwerks

Im Rahmen des Qualitätsmanagements werden Checklisten und Verfahrensweisungen/interne Regelungen für die möglichen Schweregrade eines IT-Notfalls angeboten.

## Mitgeltende Dokumente:

- Curriculum ISMS/DSMS zur Umsetzung von IT-Sicherheit und Datenschutz
- Einführung in die Informationssicherheit für Mitarbeitende
- Einführung in den Datenschutz für Mitarbeitende

## Leitfaden Curriculum Informationssicherheit und Datenschutz (Planungszeitraum 12 Monate)

Quartal	Themenblöcke	Referenz
Q 01	Informationssicherheit: Kenntnisse der Rechtsnormen	Informationssicherheit
	Datenschutz: Kenntnisse der rechtlichen Verpflichtungen	Datenschutz
	<i>(kann mit Qualitätsmanagement Maßnahmen ergänzt werden)</i>	<i>Qualitätsmanagement</i>
	Anwendung von sicheren Passwörtern	Informationssicherheit
	Datenschutzleitlinie & -richtlinien	Datenschutz
		<i>Qualitätsmanagement</i>
Q 02	Einsatz von Firewalls & Virenschutz	Informationssicherheit
	AV-Verträge (Auftragsverarbeitungs-Verträge)	Datenschutz
		<i>Qualitätsmanagement</i>
	Prävention für Phishing-Angriffe	Informationssicherheit
	Zustimmungen für Datenverarbeitung	Datenschutz
		<i>Qualitätsmanagement</i>
Q 03	Private Nutzung des Internets/eigene Geräte	Informationssicherheit
	Weitergabe von Personendaten	Datenschutz
		<i>Qualitätsmanagement</i>
	Zutrittskontrolle, Zugangskontrolle, Zugriffs- und Weitergabekontrolle	Informationssicherheit
	Geheimhaltung & berufliche Schweigepflicht	Datenschutz
		<i>Qualitätsmanagement</i>
Q 04	Kommunikation und Information im Team zur Informationssicherheit	Informationssicherheit
	Verbale Kommunikation und Datenschutz	Datenschutz
		<i>Qualitätsmanagement</i>
	Notfallmanagement in der IT-Sicherheit	Informationssicherheit
	Verhalten bei Datenpannen	Datenschutz
		<i>Qualitätsmanagement</i>

# Glossar für Informationssicherheit und Datenschutz (MCSS Ökosystem)

## **Anti-Virus SW**

Spezial-Software, die Rechner vor dem Befall von Computer-Viren schützt (Forderung der Datensicherheit).

## **Art. 32 DSGVO**

Gesetzliche Verpflichtung für Datensicherheit nach der Datenschutz-Grundverordnung.

## **BSI**

Bundesamt für Sicherheit in der Informationstechnik, zuständige Behörde für Cyberschutz und IT-Sicherheit in Deutschland.

## **Cloudbasierte Systeme**

Der Vorteil von cloudbasierten Computer-Systemen besteht vor allem darin, dass sie standardisierte Leistungen schneller und zu einem günstigeren Preis anbieten als die Anwendenden selbst dies mit ihrer internen IT können. Cloudbasierte Anwendungen können durch alle mobilen und stationären Endgeräte über das Internet abgerufen werden.

## **Curriculum**

Unter einem Curriculum (lateinisch) versteht man einen Lehrplan, in dem die Lerninhalte und Lernziele über einen längeren Zeitraum definiert sind (beispielsweise für die Einführung von QM- und Datenschutzmanagementsystemen).

## **Cyber-Sicherheit**

Der Cyber-Sicherheit befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik. Das Aktionsfeld der Informationssicherheit wird dabei auf den gesamten Cyber-Raum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationstechnik mit ein.

## **Cyber-Versicherung**

Eine Cyber-Versicherung ist eine fakultative Zusatzversicherung für Organisationen, die Schäden im Zusammenhang mit Hacker-Angriffen oder sonstigen Akten von Cyberkriminalität absichert.

## **Datenschutz**

Unter Datenschutz versteht man den Schutz personenbezogener Daten vor Missbrauch, oft im Zusammenhang auch mit dem Schutz der Privatsphäre. Zweck und Ziel des Datenschutzes ist die Sicherung des Grundrechts auf informationelle Selbstbestimmung der Einzelperson. Jede Person soll selbst bestimmen können, wem er wann welche seiner Daten und zu welchem Zweck zugänglich macht.

## **Datenschutzbeauftragte**

Eine/ein Datenschutzbeauftragte\*r (DSB) wirkt in einem Unternehmen auf die Einhaltung des Datenschutzes hin. Die Person kann Mitarbeitende dieser Organisation sein oder als externe\*r DSB bestellt werden. Der/die DSB muss die notwendige Fachkunde für die Ausübung besitzen und darf nicht in einen Konflikt oder in die Gefahr der Selbstkontrolle geraten. Die Berufung eines/einer DSB wird beispielsweise im DSGVO geregelt.

## **Datenschutzmanagementsystem (DSMS)**

Das Managementsystem organisiert den Datenschutz in der Organisationseinheit, insbesondere gemäß DSGVO und BDSG-neu. Es orientiert sich im Regelfall an der Norm ISO 9001:2015.

## **Datensicherung (englisch „Backup“):**

Bei einer Datensicherung werden zum Schutz vor Datenverlust Sicherungskopien von vorhandenen Datenbeständen erstellt. Datensicherung umfasst alle technischen und organisatorischen Maßnahmen zur Sicherstellung der Verfügbarkeit, Integrität und Konsistenz der Systeme einschließlich der auf diesen Systemen gespeicherten und für Verarbeitungszwecke genutzten Daten, Programme und Prozeduren.

## **DIN EN ISO 9001**

Im Qualitätsmanagement repräsentiert diese Norm ein Qualitätsmanagementsystem als Grundlage auch zur möglichen freiwilligen Zertifizierung. Über die reine Qualitätssicherung hinaus werden unter ISO 9001 umfangreiche Maßnahmen, die alle Abläufe innerhalb von Unternehmen eindeutig festlegen, definiert, dokumentiert und kontrolliert.

## **DSB**

Siehe Datenschutzbeauftragte.

## **DSGVO**

Die Datenschutz-Grundverordnung (DSGVO) ist eine Verordnung der Europäischen Union, mit der die Regeln zur Verarbeitung personenbezogener Daten durch Datenverarbeitende, sowohl private wie öffentliche, EU-weit vereinheitlicht werden. Dadurch soll der Schutz personenbezogener Daten innerhalb der Europäischen Union sichergestellt werden.

## **Firewall**

Eine Firewall (oft auch als Sicherheitsgateway bezeichnet) ist ein System aus soft- und hardwaretechnischen Komponenten, um IP-Netze gegen Angriffe zu sichern.

## **ISB**

Informationssicherheitsbeauftragte\*r, Verantwortliche\*r für Informationssicherheit und Cyberschutz in Organisationen.

## **Informationssicherheitsmanagementsystem (ISMS)**

Das ISMS ist die Sammlung von Dokumenten zur Umsetzung der Informationssicherheit in der Organisation. Es basiert im Regelfall auf der Norm ISO 27001.

## **Leitlinien**

Unter Leitlinien versteht man Empfehlungen, die Handlungsvorgaben enthalten. Sie sollten dann übernommen werden, wenn keine qualifizierten Gründe dagegensprechen.

## **MCSS AG**

Anbietende von cloudbasierten Assistenz-Service-Systemen, speziell für Cyber-Versicherungen:  
[www.mcass-ag.de](http://www.mcass-ag.de)

## **Mobiler Datenträger**

Datenträger, dessen Einsatzzweck durch Mobilität gekennzeichnet ist. Typische mobile Datenträger sind z.B. Speichersticks und -karten sowie externe Festplatten.

## **Notbetrieb**

Auf ein Minimum reduzierte Funktionstüchtigkeit, mit der ein Prozess aufrechterhalten werden kann. Grundlage dafür ist ein internes Notfall-Management.

## **Passwort**

Mit der Eingabe eines Passwortes weist der/die Nutzende nach, dass er/sie zu dem geschlossenen System eine Zugangsberechtigung hat.

Dies kann zum Beispiel die Anmeldung an einem Client oder die Eingabe der Geheimzahl am Geldautomaten sein. „Passwort“ stellt dabei einen Oberbegriff dar und beinhaltet Passwörter, PINs oder auch Passphrasen (Folge von aneinandergereihten Wörtern).

## **Qualitätsmanagement (QM)**

Unter QM versteht man alle Maßnahmen zur Verbesserung und Erhaltung der Qualität als legitime Erwartung der Patient\*innen und der Volkswirtschaft insgesamt. Qualitätsmanagement umfasst die Dokumentation, die Analyse, das Controlling und auch alle Maßnahmen zur Qualitätssicherung.

## **Ransomware**

Ransomware hat innerhalb eines Bereiches der Cyberkriminalität gefährlich an Bedeutung gewonnen. Mit ihr verschlüsseln Angreifende die Daten der Opfer und verlangen ein Lösegeld für den privaten Schlüssel. Ransomware wird unter anderem via E-Mail-Anhängen, infizierten Programmen und kompromittierten Websites verteilt. Security-Experten bezeichnen diese Form der Malware je nach Verbreitungsart, auch als Kryptovirus, Kryptotrojaner oder Kryptowurm.

## **Risiko**

Risiko wird häufig definiert als die Kombination (also dem Produkt) aus der Häufigkeit, mit der ein Schaden auftritt und dem Ausmaß dieses Schadens. Der Schaden wird häufig als Differenz zwischen einem geplanten und ungeplanten Ergebnis dargestellt. Risiko ist eine spezielle Form der Unsicherheit bzw. Unwägbarkeit.

## **Spamfilter**

Software, die Computer vor unerwünschten Informationen (Spam) schützen, werden als Spamfilter bezeichnet.

## **TOM**

Technische und organisatorische Maßnahmen nach DSGVO Artikel 32 für Datenschutz und Informationssicherheit.

## **Virus**

In der Computersprache eine Schadsoftware, die IT-Systeme stören oder zerstören kann.

## **Webinar**

Schulungsangebote im Internet, die auch für die Bereiche Datenschutz und Informationssicherheit in Unternehmen angeboten werden. Sie erfüllen die Anforderung nach ISO Standards (z.B. 9001).

## **Wissenstests**

Das Wissen aller Mitarbeitenden zur Informationssicherheit und zum Datenschutz ist die Grundlage einer rechtskonformen Organisation. Um die Kenntnisse eines Teams zu evaluieren, können digitale Wissenstests genutzt werden.



# Registrierung/Onboarding

## Beschreibung des Prozesses für den Administratorzugang und den Zugang zu MC-SMARTLEARN

Der Zugang zum digitalen Assistenz-System für Cyber-Versicherte ist durch die Versicherungsprämie lizenziert.

**MCSS** stellt den sicheren Zugangs-Code den Versicherten unter der im Versicherungsvertrag angegebene E-Mail-Adresse zur Verfügung.

**Achtung:** Wenn der Code bislang nicht eingegangen ist, bitte auch im SPAM Ordner des Postfachs nachschauen.

**Ansonsten Nachfrage an:** [anwenderservice@mcss-ag.de](mailto:anwenderservice@mcss-ag.de) mit Angabe von Cyber-Versicherungs-Nr. und Adressdaten.



Die Registrierung beginnt unter der Webadresse [mcss-ag.de/kunden-login-ecclesia/](https://mcss-ag.de/kunden-login-ecclesia/)

**1**

### Onboarding Kunden der Ecclesia

#### Willkommen zum digitalen Sicherheitsmanagementsystem

Zur professionellen Umsetzung von Cyberschutz, IT-Sicherheit und Datenschutz haben die Ecclesia und die MCSS AG eine Sicherheitsallianz geschlossen.


Als Leistung dieser Kooperation haben Sie nun Zugang zu Ihrem persönlichen Sicherheitsmanagementsystem. Das cloudbasierte System ergänzt die Ihnen zugestellten Informationen und unterstützt Ihre technischen, organisatorischen und rechtlichen Maßnahmen. Damit können Sie Ihre Mitwirkungspflichten und Obliegenheiten im Rahmen Ihrer Cyber-Versicherung zeitsparend und professionell erfüllen.

Bitte registrieren Sie sich auf dieser Seite, um Ihren Online-Zugang freizuschalten.

Weitere Informationen zur Nutzung von MC-ORG / MC-ORG ÖR:



Rechtliche Rahmenbedingungen




IT-Sicherheit



Nutzung der Cloud



Datenschutz




Innovationskriterien

#### Registrierung

Bitte geben Sie den Authentifizierungscode ein, den Sie per Anschreiben erhalten haben.

**Weiter**



**2**

### Registrierung

Bitte geben Sie den Authentifizierungscode ein, den Sie per Anschreiben erhalten haben.

**Weiter**

In dem Feld „**Registrierung**“ wird der Authentifizierungscode eingegeben und anschließend mit einem Klick auf das Feld „**Weiter**“ bestätigt.

**3**

### Registrierung

Bitte geben Sie die E-Mailadresse des/der Hauptanwender\*in ein. Der/die Hauptanwender\*in wird den Zugang verwalten und kann weitere Anwender\*innen einladen.

**Akzeptieren und weiter**

Nun kann in dem Feld „Registrierung“ die E-Mailadresse des Hauptverantwortlichen (Administratorzugang, der/die für das Projekt Verantwortliche) eingegeben werden. Anschließend wird diese Eingabe mit dem Feld „**Akzeptieren und weiter**“ bestätigt.

**4**

### Registrierung

**Einladung an 'user@testmail.de' gemailt.**

Zum Abschließen der Registrierung klickt der/die Hauptanwender\*in bitte den Link in der E-Mail von 'Anwenderservice MCSS AG' in seinem/ihrer Posteingang oder Spamverzeichnis. Nach der Fertigstellung der Registrierung kann sich der/die Hauptanwender\*in in der MCSS Anwendung anmelden (Link wird angezeigt) und kann weitere Anwender\*innen einladen.

Sie können dieses Browserfenster jetzt schließen.

Es folgt die Bestätigung, dass eine Einladung zur finalen Registrierung an die eingegebene E-Mail-Adresse versendet worden ist.


Diese E-Mail ist im Mailaccount abrufbar und wurde von [anwenderservice@mcss-ag.de](mailto:anwenderservice@mcss-ag.de) versendet.

**Bitte diese Adresse freischalten, damit wichtige Informationen nicht im Spamfilter verloren gehen.**

In der erhaltenen E-Mail ist der entsprechende [Link](#) anzuklicken, um das Onlineregistrierungsformular aufzurufen.

**5**

Test Office 220311-09 hat Sie eingeladen MC-ORG zu nutzen.

 **MCSS Anwenderservice** <anwenderservice@mcss-ag.de>  
16:40

An: user@testmail.de

Sehr geehrte Damen und Herren,

mit dieser E-Mail erhalten Sie die Einladung zur Registrierung Ihres digitalen Assistenz-Systems, zur Eingabe Ihrer Benutzerdaten und anschließenden Nutzung des Systems.

Bitte klicken Sie den nachstehenden Link an, um das Online-Formular aufzurufen und den Registrierungsprozess durchzuführen:  
<https://mcss-ag.net/registration/?Param=GxYAi-KRCvPTH4POT6K0%2b%2f%2fe6FedlZ2rjmWuYpGPm5tnzEkH6%2f8UiOm2DuFFQ6W3lu%2brruZ8%2bcd1CqZ4z%2b7ygjS%2bBxCkAAND34Zq6phqwxO3JmFhaDx3BwyCEP-EJYGGwNLAJrU3003oxKEPfyGHIWID9dmc7lC2ALnTu3rEN2OnEI04Ejvdr8KUEd6E27%2fgM%2fYupx%2fmyj2LkETLEdFHDw%3d%3d>

Wichtig: Aus Sicherheitsgründen ist dieser Link nur 96 Stunden aktiv. Sollten Sie diesen Zeitraum nicht einhalten können, dann mailen Sie Ihren gewünschten Zeitraum für das Onboarding an [anwenderservice@mcss-ag.de](mailto:anwenderservice@mcss-ag.de). Die MCSS AG schaltet dann den Aktivierungslink erneut für 96 Stunden frei.


Wenn Sie zu dem Registrierungsprozess weitere Fragen oder Informationen wünschen, dann melden Sie sich bitte bei dem Administrator in Ihrer Organisation.

Vielen Dank

Mit freundlichen Grüßen

Ihr MCSS - Anwenderservice

**6**

  
Registrierung - Administratorzugang einrichten

MC-ORG

Organisation: MCSS Test 220311-09

Emailadresse: user@testmail.de

Vornamen eingeben\*

Nachnamen eingeben\*

Anzeigename eingeben\*

Passwort eingeben\*

Passwort bestätigen\*


Weiter

MCSS User Service Web App  
V1.61.6.0313  
© 2020-2022 by MCSS AG

Bitte die Administratordaten eintragen mit Vorname, Nachname, Anzeigename und Kennwort/Passwort.

Danach mit dem Feld „Weiter“ bestätigen.

**7**

  
Registrierung - MC-SMARTLEARN Zugang einrichten

MC-ORG

Organisation: MCSS Test 220311-09

Loginnamen eingeben\*

Passwort eingeben\*

Passwort bestätigen\*

Registrierung abschließen

MCSS User Service Web App  
V1.61.6.0313  
© 2020-2022 by MCSS AG

Der **MC-SMARTLEARN** Zugang (siehe Seite 23) wird mit Eingabe eines Loginnamens und eines Kennwort/Passworts eingerichtet. Anschließend die Eingabe mit „Registrierung abschließen“ beenden.

**8**

  
Registrierung erfolgreich abgeschlossen

**MC-ORG Anmeldung**

MCSS User Service Web App  
V1.61.6.0313  
© 2020-2022 by MCSS AG

**Die Registrierung ist damit erfolgreich abgeschlossen.**

Jetzt kann mit dem System sofort gearbeitet oder über die Admin-Verwaltung weitere Zugänge angelegt werden.

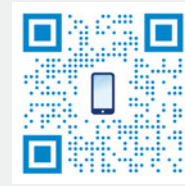
Hierzu ist eine Anleitung im Admin-Zugang verfügbar.

# Einführung MC-SMARTLEARN

## Beschreibung des Prozesses für den MC-SMARTLEARN Zugang und Anwendungshinweise

MC-SMARTLEARN ist eine Schulungsplattform für alle Mitarbeitenden, die sich ortsungebunden und flexibel zu den Themen Informationssicherheit, Datenschutz und Cybersicherheit schulen möchten. Dazu stehen Erklär- und Schulungsvideos, Wissenstests und Checklisten zur Verfügung. Nach erfolgreicher Schulung sind Nachweisdokumente abrufbar. Alle Inhalte sind für Smartphones optimiert.

So ist es möglich, die vielfältigen Inhalte überall zu nutzen, auch unterwegs im Bus, Zug, der Straßenbahn oder als Mitfahrende im Auto.



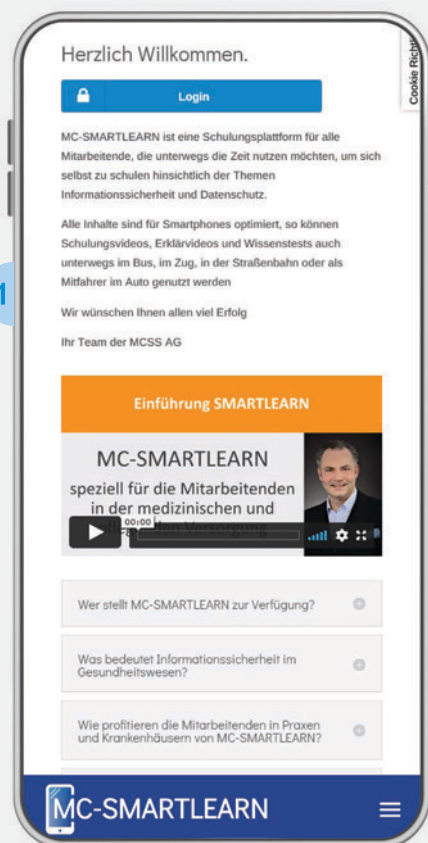
Anmelden können Sie sich unter der Webadresse [mc-smartlearn.de](https://mc-smartlearn.de)

MC-SMARTLEARN ist für Cyber-Versicherte durch die Versicherungsprämie lizenziert.

Den für den Zugang erforderlichen Benutzernamen und das Passwort legt der Administrator (der/die Verantwortliche für das Assistenz-System) fest und stellt dies allen verantwortlichen Mitarbeitenden zur Verfügung.

**Achtung:** MC-SMARTLEARN ist für SMARTPHONES entwickelt.

Auf anderen Computern ist eine Ansicht nur mit angepasstem Bildschirmausschnitt möglich, z.B. durch Verringern der Breite des Browserfensters.



Nach Eingabe der Domain <https://mc-smartlearn.de> in einem beliebigen Browser eines Smartphones erscheint der „Willkommens-Bildschirm“.

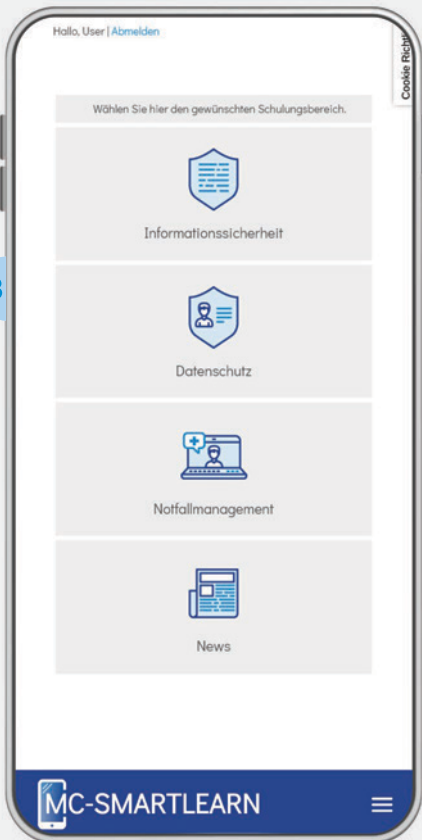
Dort stehen viele Informationen und ein Erklärvideo zur Einführung zur Verfügung.

Mit einem Klick auf den Button „Login“ geht es zur Anmelde-Maske von MC-SMARTLEARN.

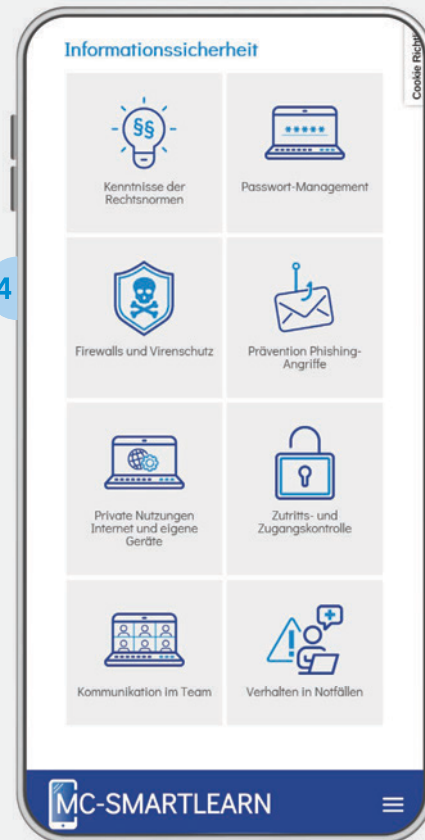
In dem Anmeldebildschirm wird der Benutzername in das Feld „Benutzername“ und das Kennwort in das Feld „Kennwort/Passwort“ eingetragen.

Anschließend mit dem Button „Anmelden“ bestätigen und schon geht es los.

**Typ:** Bitte auf Groß- und Kleinschreibung achten.

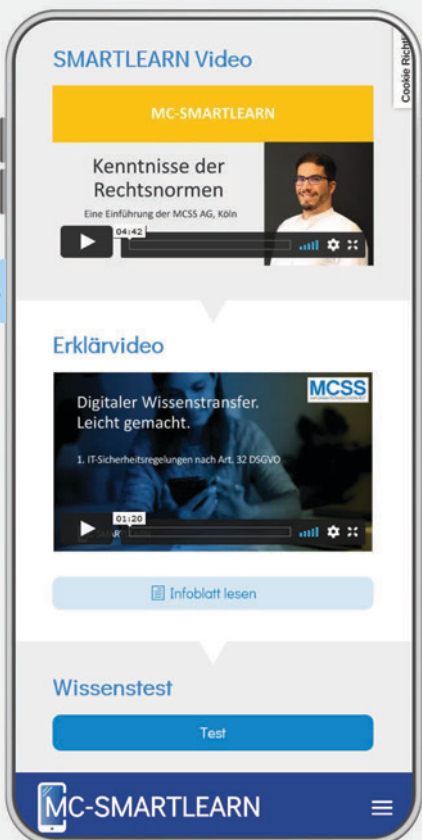


Nach der Anmeldung in **MC-SMARTLEARN** ist die Auswahl zu den Schulungsbereichen Informationssicherheit, Datenschutz und Notfallmanagement möglich, sowie der Aufruf von News aus den genannten Fachbereichen.



In den Schulungsbereichen gibt es unterschiedliche Schulungsblöcke, wie z.B. „**Kenntnisse der Rechtsnormen**“, die die Mitarbeitenden Schritt für Schritt abarbeiten können.

Mit einem „Klick“ auf den Schulungsbereich kann die Fortbildung beginnen.



In jedem Schulungsblock sind zu dem jeweiligen Thema ein **SMARTLEARN-** und ein **Erklärvideo** verfügbar, in denen die ausgesuchten Themen erklärt werden.

Zusätzlich bietet ein **Informationsblatt** weitere Inhalte.

Mit dem **Wissenstest** prüfen Mitarbeitende, ob das jeweilige Thema inhaltlich verstanden wurde. Nach erfolgreich absolviertem Wissenstest kann ein **Schulungsnachweise** angefordert werden.

Alle Bausteine sind mit einem „Klick“ ansteuerbar.

**Tipp:** Zur besseren Konzentration und für unterwegs empfehlen sich Kopfhörer.



