Anlage technisch-organisatorische Maßnahmen

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

basierend auf Information Security Assessment based on ISO 27001:2013
https://www.vda.de/de/services/Publikationen/information-security-assessment.html

Unternehmen **Comp- Pro GmbH, Nienburg**

Datum 01.10.2020 Ersteller Elke Mach / Robin Mach

DSGVO-Ziele gem. Art. 5 Abs. 1, lit. f DSGVO

Vertraulichkeit	**Integrität**	**Verfügbarkeit**	**Level** Reifegrad Level: 0-5; na	
				Ausfüllhilfe finden Sie in dem Dokument: **Merkblatt zu Anlage zu AV-Vertrag toMs DSGVO VDA-ISA_DE_4-0** Trifft eine Frage nicht zu, so ist na (not applicable) einzutragen.
				6. Organisation der Informationssicherheit
X	X		1	6.1 Inwieweit sind die Verantwortlichkeiten für Informationssicherheit definiert und zugewiesen? (Referenz zu ISO 27001: Control A6.1.1)
X			1	6.2 Inwieweit werden in Projekten, unabhängig von ihrer Art, Anforderungen an die Informationssicherheit berücksichtigt? (Referenz zu ISO 27001: Control A6.1.5)
X	X	X	2	6.3 Inwieweit gibt es eine Richtlinie zur Nutzung von mobilen Endgeräten und deren Remote Zugriff auf Daten der Organisation? (Referenz zu ISO 27001: Control A6.2.1 und A6.2.2)
X			1	6.4 Inwieweit sind die gemeinsamen Rollen und Verantwortlichkeiten zwischen IT-Dienstanbietern (insbes. Cloud Providern) und der eigenen Organisation definiert? (Referenz zu ISO 27017: Control CLD.6.3.1)
				7. Personalsicherheit
X	X	X	1	7.1 Inwieweit werden Mitarbeiter vertraglich zur Einhaltung der Richtlinien zur Informationssicherheit verpflichtet? (Referenz zu ISO 27001: Control A7.1.2 und A7.3.1)
X	X	X	1	7.2 Inwieweit werden Mitarbeiter über die Risiken beim Umgang mit Informationen und deren Verarbeitung geschult und sensibilisiert? (Referenz zu ISO 27002: Control 7.2.1 und 7.2.2)

8 Verwaltung der Werte

X	X	X	1

8.1 Inwieweit gibt es Verzeichnisse für Werte (Assets), die Informationen in verschiedenen Ausprägungen enthalten?
(Referenz zu ISO 27001: Control A8.1.1, A8.1.2, A8.1.3 und A8.1.4)

X	X	X	1

8.2 Inwieweit werden Informationen hinsichtlich ihres Schutzbedarfs eingestuft und gibt es Regeln für Kennzeichnung, Handhabung, Transport, Speicherung, Lagerung, Löschung und Entsorgung?
(Referenz zu ISO 27001: Control A8.2.1, A8.2.2 und A8.2.3)

X	X	X	2

8.3 Inwieweit ist ein angemessener Umgang mit gespeicherten Informationen auf mobilen Datenträgern geregelt?
(Referenz zu ISO 27001: Control A8.3.1, A8.3.2 und A8.3.3)

X			NA

8.4 Inwieweit wird das sichere Entfernen von Information-Assets aus den IT-Diensten (insbes. Cloud) gewährleistet?
(Referenz zu ISO 27017: Control CLD.8.1.5)

9. Zugangssteuerung

X	X		1

9.1 Inwieweit sind Regelungen und Verfahren bezüglich dem Zugang zu IT-Systemen vorhanden?
(Referenz zu ISO 27001: Control A9.1.2)

X	X		1

9.2 Inwieweit sind Verfahren zur Registrierung, Änderung und Löschung von Benutzern mit den zugehörigen Zugriffsrechten umgesetzt und erfolgt dabei insbesondere ein vertraulicher Umgang mit den Anmeldeinformationen?
(Referenz zu ISO 27001: Control A9.2.1, A9.2.2, A9.2.4 und A9.2.5)

X	X		1

9.3 Inwieweit ist die Zuweisung sowie die Nutzung von privilegierten Benutzer- und technischen Konten geregelt und wird diese überprüft?
(Referenz zu ISO 27001: Control A9.2.3)

X	X		2

9.4 Inwieweit gibt es verbindliche Regeln für den Anwender zur Erstellung und im Umgang mit vertraulichen Anmeldeinformationen?
(Referenz zu ISO 27001: Control A9.3.1 und A9.4.3)

X	X		NA

9.5 Inwieweit wird der Zugriff auf Informationen und Applikationen auf berechtigte Personen eingeschränkt?
(Referenz zu ISO 27001: Control A9.4.1 und A9.4.2)

X	X		NA

9.6 Inwieweit ist eine Trennung der Daten innerhalb einer, mit fremden Organisationen gemeinsam genutzter Umgebungen gewährleistet?
(Referenz zu ISO 27017: Control CLD.9.5.1 und CLD.9.5.2)

10 Kryptographie

X	X		1

10.1 Inwieweit gibt es Regeln zur Verschlüsselung inkl. der Verwaltung des Schlüsselmaterials (kompletter Lifecycle) zum Schutz von Informationen bei Speicherung und Transport und sind diese umgesetzt worden?
(Referenz zu ISO 27001: Control A10.1.1)

11. Physische und umgebungsbezogene Sicherheit

X	X	X	2

11.1 Inwieweit sind Sicherheitszonen für den Schutz von schutzbedürftigen oder kritischen Informationen sowie informationsverarbeitenden Einrichtungen definiert, abgesichert und überwacht (Zutrittssicherungen)?
(Referenz zu ISO 27001: Control A11.1.1 und A11.1.2)

		X	2

11.2 Inwieweit hat das Unternehmen Maßnahmen gegen die Auswirkungen von Naturkatastrophen, vorsätzlichen Angriffen oder Unfällen getroffen?
(Referenz zu ISO 27001: Control A11.1.4)

X	X	X	1

11.3 Inwieweit werden Schutzmaßnahmen in Anlieferungs- und Versandbereichen bzgl. des Zutritts unbefugter Personen getroffen?
(Referenz zu ISO 27001: Control A11.1.6)

X	X	X	1

11.4 Inwieweit sind Richtlinien und Verfahren für den Gebrauch von Assets, einschließlich ihrer Mitnahme, Entsorgung und Wiederverwendung vorhanden und umgesetzt?
(Referenz zu ISO 27001: Control A11.2.5, A11.2.6 und A11.2.7)

12. Betriebssicherheit

X	X	X	1

12.1 Inwieweit werden Änderungen von Organisation, Geschäftsprozessen, informationsverarbeitenden Einrichtungen und Systemen bzgl. ihrer Sicherheitsrelevanz gesteuert und umgesetzt?
(Referenz zu ISO 27001: Control A12.1.2)

X	X	X	1

12.2 Inwieweit sind die Entwicklungs- und Testumgebungen von den Produktivumgebungen getrennt?
(Referenz zu ISO 27001: Control A12.1.4)

	X	X	2

12.3 Inwieweit ist der Schutz (z.B. "end-point security") vor Schadsoftware (Viren, Würmer, Trojaner, Spyware, …) in Verbindung mit der Sensibilisierung von Benutzern ausgeprägt?
(Referenz zu ISO 27001: Control A12.2.1)

	X	X	1

12.4 Inwieweit werden Datensicherungen unter Berücksichtigung einer entsprechenden Regelung erstellt und regelmäßig getestet?
(Referenz zu ISO 27001: Control A12.3.1)

X	X	X	1	12.5 Inwieweit werden Ereignis-Logs, die z.B. Benutzeraktivitäten, Ausnahmen, Fehler und Sicherheitsereignisse beinhalten können, erzeugt, aufbewahrt, überprüft und gegen Veränderungen abgesichert? (Referenz zu ISO 27001: Control A12.4.1 und A12.4.2)
X	X	X	NA	12.6 Inwieweit werden die Aktivitäten von Systemadministratoren und -operatoren protokolliert, die Ablage der Protokolle gegen Veränderungen abgesichert und regelmäßig überprüft? (Referenz zu ISO 27001: Control A12.4.3)
	X		1	12.7 Inwieweit werden Informationen über technische Schwachstellen der IT-Systeme zeitnah beschafft, beurteilt und geeignete Maßnahmen ergriffen (z.B. Patch-Management)? (Referenz zu ISO 27001: Control A12.6.1 und A12.6.2)
		X	1	12.8 Inwieweit werden Auditanforderungen und -aktivitäten, die zur Überprüfung von IT-Systemen dienen, geplant, abgestimmt, und die IT-Systeme in der Folge technisch überprüft (Systemaudit)? (Referenz zu ISO 27001: Control A12.7.1, A18.2.3)
X			1	12.9 Inwieweit wurden Auswirkungen kritischer administrativer Funktionen von externen IT-Diensten (insbes. Cloud-Dienste) berücksichtigt? (Referenz zu ISO 27017: Control CLD.12.1.5)

13. Kommunikationssicherheit

X	X	X	1	13.1 Inwieweit werden Netzwerke verwaltet und gesteuert, um Informationen in IT-Systemen und Anwendungen zu schützen? (Referenz zu ISO 27001: Control A13.1.1)
X	X	X	1	13.2 Inwieweit werden Anforderungen an Sicherheitsmechanismen sowie Service Levels und Managementanforderungen an Netzwerkdienste identifiziert und in Service-Level-Agreements dokumentiert? (Referenz zu ISO 27001: Control A13.1.2)
X	X		1	13.3 Inwieweit werden Gruppen von Informationsdiensten, Benutzer und Informationssysteme innerhalb des Netzwerks segmentiert? (Referenz zu ISO 27001: Control A13.1.3)
X	X	X	2	13.4 Inwieweit werden Informationen während des Austauschs oder der Übermittlung geschützt? (Referenz zu ISO 27001: Control A13.2.1 und A13.2.3)
X			1	13.5 Inwieweit werden vor dem Austausch von Informationen Geheimhaltungsvereinbarungen abgeschlossen und werden die Anforderungen bzw. Erfordernisse zum Schutz der Informationen dokumentiert und regelmäßig überprüft?

(Referenz zu ISO 27001: Control A13.2.4)

14. Anschaffung, Entwicklung und Instandhalten von Systemen

X	X	X	1

14.1 Inwieweit werden sicherheitsspezifische Anforderungen bei neuen IT-Systemen (einschließlich öffentlich zugänglicher IT-Systeme) und bei Erweiterungen für bestehende IT-Systeme berücksichtigt?
(Referenz zu ISO 27001: Control A14.1.1, A14.1.2 und A14.1.3))

X	X	X	NA

14.2 Inwieweit werden sicherheitsrelevante Aspekte im Software-Entwicklungsprozess (inkl. Change Management) berücksichtigt?
(Referenz zu ISO 27001: Control A14.2.1 - A14.2.9)

	X		NA

14.3 Inwieweit wird sichergestellt, dass Testdaten sorgfältig erstellt, geschützt und kontrolliert eingesetzt werden?
(Referenz zu ISO 27001: Control A14.3.1)

X	X	X	1

14.4 Inwieweit wird sichergestellt, dass nur evaluierte und freigegebene externe IT-Dienste (insbes. Cloud-Dienste) zum Verarbeiten von Unternehmensdaten eingesetzt werden?
-

15. Lieferantenbeziehungen

X	X	X	2

15.1 Inwieweit werden Anforderungen an die Informationssicherheit bei einem Lieferanten zur Risikoreduzierung vertraglich vereinbart, wenn dieser Zugriff auf Unternehmenswerte erhält (insbesondere Informations- und Kommunikationsdienste sowie beim Einsatz von Unterauftragnehmern)?
(Referenz zu ISO 27001: Control A15.1.1 - A15.1.3)

X	X	X	1

15.2 Inwieweit werden die erbrachten Leistungen eines Lieferanten bzw. beim Unterauftragnehmer regelmäßig überwacht, überprüft und auditiert?
(Referenz zu ISO 27001: Control A15.2.1)

16. Handhabung von Informationssicherheitsvorfällen

X	X	X	1

16.1 Inwieweit sind Verantwortlichkeiten, Verfahren, Meldewege und Kritikalitäts-Stufen im Umgang mit Informationssicherheitsereignissen oder -schwachstellen festgelegt?
(Referenz zu ISO 27001: Control A16.1.1 - A16.1.3)

X	X	X	1

16.2 Inwieweit erfolgt eine Bearbeitung von Informationssicherheitsereignissen?
(Referenz zu ISO 27001: Control A16.1.4 - A16.1.7)

17. Informationssicherheitsaspekte beim Business Continuity Management

		X	1

17.1 Inwieweit werden die Anforderungen an Informationssicherheit (inkl. Redundanz entsprechender Einrichtungen) und die Weiterführung eines ISMS in Krisensituationen definiert, umgesetzt, überprüft und beurteilt?
(Referenz zu ISO 27001: Control A17.1.1 - A17.1.3 und A17.2.1)