Checkliste für die Umsetzung der DSGVO in Verbindung mit Informationssicherheit

Erstelldatum	13.01.2023
Update	16.02.2025

Herausgeber	Teilnehmer der Bewertung zur Selbsteinschätzung	
	Name	Position
SMCT MANAGEMENT concept Stefan Strößenreuther Reuthweg 11 95100 Selb		

Inhaltsverzeichnis

1. Grundlagen und Verantwortung		
1.1 Rechtsgrundlagen klären	Umgesetzt	Zufrieden
Welche Verarbeitungen personenbezogener Daten (PbD) finden statt?	☐	☐
Auf welcher **Rechtsgrundlage** (z. B. Einwilligung, Vertrag, berechtigtes Interesse) basieren die Verarbeitungen?	☐	☐
1.2 Rollen und Zuständigkeiten	Umgesetzt	Zufrieden
Gibt es einen **Datenschutzbeauftragten (DSB)**?	☐	☐
Wer ist für **Informationssicherheit** (ISB-Beauftragter) und **Datenschutz** verantwortlich?	☐	☐
Sind die Rollen klar voneinander abgegrenzt bzw. sinnvoll verzahnt?		
1.3 Geltungsbereich definieren	**Umgesetzt**	**Zufrieden**
Welche **Datenkategorien** und **Systeme** fallen unter DSGVO und müssen mittels Informationssicherheitsmaßnahmen geschützt werden?	☐	☐
Wie sind Außenstellen, Cloud-Dienste und mobile Geräte eingebunden?	☐	☐

2. Dateninventar und Dokumentation		
2.1 Verzeichnis von Verarbeitstätigkeiten (Art. 30 DSGVO)	Umgesetzt	Zufrieden
Für alle Prozesse mit PbD: Verantwortlicher, Zweck, Kategorien von Personen und Daten, Rechtsgrundlage, Speicherort, Weitergabe.	☐	☐
Sind alle relevanten Systeme und Speicherorte (Server, Papierakten, Cloud-Services) erfasst?	☐	☐
2.2 Asset- und System Register	**Umgesetzt**	**Zufrieden**
Haben wir ein **IT-Asset-Register**, in dem die kritischen Informationswerte (inkl. personenbezogener Daten) aufgelistet sind?	☐	☐
Gibt es für jedes Asset einen Eigentümer (Data Owner) und Klassifizierung (z. B. intern, vertraulich)?	☐	☐
2.3 Dokumentenlenkung	**Umgesetzt**	**Zufrieden**
Datenschutzerklärungen, Richtlinien (z. B. Aufbewahrungsfristen, Zugriffsrechte) sind versioniert und leicht auffindbar.	☐	☐
Sind Betriebsvereinbarungen (z. B. E-Mail- und Internetnutzung) in die IS-Dokumentation eingebunden?	☐	☐

3. Risikobasierter Ansatz (Art. 24 DSGVO / ISO 27001		
3.1 Risikoanalyse	Umgesetzt	Zufrieden
Werden personenbezogene Daten gesondert in der **IS-Risikoanalyse** identifiziert?	☐	☐

Klassifizierung der Daten (z. B. besonders schützenswerte Daten / normal): Relevanz für Vertraulichkeit, Integrität, Verfügbarkeit.	☐	☐
3.2 Risiken für die Rechte und Freiheiten	**Umgesetzt**	**Zufrieden**
Werden kritische Verarbeitungen (z. B. Profiling, Überwachung) auf die **Notwendigkeit einer Datenschutz-Folgenabschätzung (DFA)** geprüft?	☐	☐
DFA-Dokumentation gemäß Art. 35 DSGVO bei Bedarf erstellt und regelmäßig überprüft?	☐	☐
3.3 Umgang mit Klimarisiken (ab Nov. 2024 im Kontext)	**Umgesetzt**	**Zufrieden**
Werden mögliche Auswirkungen (z. B. Stromausfälle, Lieferkettenstörungen) auf die Datenverfügbarkeit / Systemsicherheit bedacht?	☐	☐
Notfall- und Wiederanlaufpläne in Bezug auf personenbezogene Daten aktualisiert?	☐	☐

4. Technische und organisatorische Maßnahmen (TOM)		
4.1 Zugriffs- und Berechtigungskonzept	Umgesetzt	Zufrieden
Striktes **Need-to-Know-Prinzip**: Zugriff auf PbD nur für autorisierte Rollen	☐	☐
Regelmäßige **Rezertifizierung** von Berechtigungen (Joiner, Mover, Leaver-Prozesse).	☐	☐
4.2 Verschlüsselung und Pseudonymisierung	**Umgesetzt**	**Zufrieden**
Welche **Datenbanken** / Speicherorte enthalten PbD und sind sie verschlüsselt?	☐	☐
Ist eine **Pseudonymisierung** (Ersatz von direkt identifizierenden Merkmalen) bei bestimmten Prozessen sinnvoll / vorgeschrieben?	☐	☐
4.3 Netzwerk- und Endgerätesicherheit	**Umgesetzt**	**Zufrieden**
Firewalls, Segmentierung, Intrusion Detection/Prevention, Patch-Management bei Systemen mit PbD.	☐	☐
Mobile Devices (z. B. BYOD) mit MDM (Mobile Device Management) abgesichert, verschlüsselte Datenübertragung.	☐	☐
4.4 Protokollierung und Monitoring	**Umgesetzt**	**Zufrieden**
Logging von **Zugriffen** auf PbD: Wer, wann, auf welche Daten?	☐	☐
Zentralisiertes Monitoring (z. B. SIEM), um Anomalien in PbD-Beständen zu erkennen.	☐	☐

5. Rechte der Betroffenen und Datenschutzprinzipien		
5.1 Betroffenenrechte	Umgesetzt	Zufrieden
Verfahren für Auskunft, Berichtigung, Löschung, Einschränkung (z. B. standardisiertes Anfrage-Portal oder E-Mail-Prozess).	☐	☐
Reaktion innerhalb der **gesetzlichen Fristen** (i. d. R. ein Monat), Nachweis über Erfüllung/Ablehnung	☐	☐

5.2 Data Protection by Design and Default (Art. 25 DSGVO)	Umgesetzt	Zufrieden
Werden bei neuen Systemen und Prozessen die PbD- und DS-by-Default-Prinzipien beachtet (Minimaldatenerhebung, Standards als „Privacy-friendly“)?	☐	☐
Dokumentierte **Freigabe** / Prüfung neuer Projekte (z. B. IT-Change-Request mit DS-Check)?	☐	☐
5.3 Protokollierung / Nachweisführung	**Umgesetzt**	**Zufrieden**
Nachweis, wie die **Grundsätze** (z. B. Zweckbindung, Datensparsamkeit, Richtigkeit) praktisch umgesetzt werden.	☐	☐
Kontinuierliche **Überwachung** von Löschfristen und Archivierung.	☐	☐

6. Auftragsverarbeitung und Datenübermittlung		
6.1 Auftragsverarbeitungsverträge (AVV)	Umgesetzt	Zufrieden
Bestehen Verträge nach Art. 28 DSGVO mit allen Dienstleistern, die PbD in unserem Auftrag verarbeiten?	☐	☐
Enthalten sie Vorgaben zu Sicherheitsstandards, Subunternehmern und Reporting-Pflichten bei Vorfällen?	☐	☐
6.2 Drittstaatentransfers	**Umgesetzt**	**Zufrieden**
Wenn Daten außerhalb der EU/EWR fließen: Prüfen von **Transfermechanismen** (SCC, Angemessenheitsbeschluss, Binding Corporate Rules).	☐	☐
Dokumentation, ob ggf. zusätzliche Sicherheitsmaßnahmen (z. B. Verschlüsselung) erforderlich sind.	☐	☐
6.3 Kontrollmöglichkeiten	**Umgesetzt**	**Zufrieden**
Audit- oder Prüfungsrechte gegenüber Dienstleistern (**ISO 27001**, SOC2-Reports etc.)?	☐	☐
Regelmäßige Überprüfung, ob Auftragsverarbeiter ihren vertraglichen Verpflichtungen nachkommen.	☐	☐

7. Incident Management und Meldepflichten		
7.1 Incident-Response	Umgesetzt	Zufrieden
Interner Prozess für Security Incidents, die **personenbezogene Daten** betreffen (z. B. Datenschutzvorfälle) klar dokumentiert.	☐	☐
Krisenstab oder Incident Response Team, Eskalation an Datenschutzbeauftragten?	☐	☐
7.2 Meldepflichten	**Umgesetzt**	**Zufrieden**
Verfahren für **Meldungen** an die Aufsichtsbehörde (Art. 33 DSGVO) bei Datenpannen binnen 72 Stunden?	☐	☐
Vorgehensweise bei **Informationspflicht** an Betroffene (Art. 34 DSGVO) dokumentiert?	☐	☐
7.3 Forensik und Lessons Learnedd	**Umgesetzt**	**Zufrieden**

Protokollierung, forensische Untersuchung von Datenschutzvorfällen, Ableitung von Korrekturmaßnahmen.	☐	☐
Ergebnisse in den **KVP** (Kontinuierlichen Verbesserungsprozess) einfließen lassen.	☐	☐

8. Schulungen und Awareness		
8.1 Datenschutz-Schulungen	Umgesetzt	Zufrieden
Regelmäßige **Schulungen** für Mitarbeitende (Pflichtmodule, E-Learning, Workshops) zu DSGVO-Basics, Umgang mit PbD.	☐	☐
Rollenspezifische **Schulungen** für HR, Marketing, IT, Führungskräfte etc.?	☐	☐
8.2 Security-Awareness	**Umgesetzt**	**Zufrieden**
Phishing-**Simulationen**, Übungen für Passwortsicherheit, Sensibilisierung für Social Engineering.	☐	☐
Feedback- und **Meldesysteme** für potenzielle Datenschutzverstöße (Whistleblowing-Kanal, interne Hotline).	☐	☐
8.3 Dokumentation von Schulungen	**Umgesetzt**	**Zufrieden**
Aufbewahrung von Teilnehmerlisten, Schulungsinhalten und Terminen.	☐	☐
Regelmäßige Aktualisierung, wenn sich Gesetzeslage oder interne Verfahren ändern.	☐	☐

9. Interne Audits und Managementreview		
9.1 Auditplanung	Umgesetzt	Zufrieden
DSGVO-relevante Prozesse in den Plan für **ISMS-Audits** (nach ISO 27001) einbeziehen.	☐	☐
Auditoren sollten sowohl **Datenschutz-** als auch **IT-Security-Aspekte** prüfen.	☐	☐
9.2 Auditdurchführung	**Umgesetzt**	**Zufrieden**
Prüfen von **Verfahrensverzeichnissen**, Auftragsverarbeitungsverträgen, Datenschutz-Folgenabschätzungen, Sicherheitsrichtlinien etc.	☐	☐
Auditfeststellungen priorisieren und Korrekturmaßnahmen ableiten.	☐	☐
9.3 Managementbewertung	**Umgesetzt**	**Zufrieden**
Ergebnisse der Audits, Vorfälle (Incidents), Änderungen in Gesetzen oder Branchen-standards auf Managementebene diskutieren.	☐	☐
Beschlüsse (z. B. Budget für neue IT-Sicherheitstools, Prozessverfeinerung) doku-mentieren und umsetzen.	☐	☐

10. Kontinuierliche Verbesserung		
10.1 Aktualisierung von Verfahren und Dokumenten	Umgesetzt	Zufrieden

Bei **Prozessänderungen**, neuen Tools oder Partnerschaften: Datenschutz- und Sicherheitsaspekte neu bewerten.	☐	☐
Versionskontrolle, wer die Änderungen wann freigegeben hat.	☐	☐
10.2 Lessons Learned	Umgesetzt	Zufrieden
Nach Incidents, Audits und Übungen: Was lief gut, wo gab es **Schwachstellen**?	☐	☐
Maßnahmen in den KVP einfließen lassen, Best Practices an alle relevanten Abteilungen weitergeben.	☐	☐
10.3 Re-Evaluierung	Umgesetzt	Zufrieden
Periodische komplette **Neubewertung** der GDPR-Compliance und IS-Sicherheit; ggf. externe Unterstützung, Penetrationstests, Scans.	☐	☐
Umsetzung neuer **Anforderungen** (z. B. Aktualisierungen in EU-Verordnungen, Vorgaben von Kunden oder Partnern).	☐	☐

SMCT MANAGEMENT übernimmt als externer Datenschutzbeauftragter die professionelle Beratung und tägliche Betreuung aller Themen rund um die DSGVO und weitere datenschutzrelevante Vorschriften. Wir unterstützen Sie bei der Analyse und Dokumentation Ihrer Datenverarbeitungen, erstellen ein Verzeichnis der Verarbeitungstätigkeitenund etablieren praxisnahe Verfahrensanweisungen.

Dabei prüfen wir auch technische und organisatorische Maßnahmen (TOM), stimmen uns mit den zuständigen Fachabteilungen ab und kümmern uns um das Datenschutz-Risikomanagement – einschließlich Datenschutzaudits und möglicher Folgenabschätzungen (DFA).

Als externer Datenschutzbeauftragter sind wir Ihr neutraler Ansprechpartner für datenschutzrechtliche Fragestellungen: Wir beraten Führungskräfte und Mitarbeitende in alltäglichen Situationen, geben bei neuen Projekten frühzeitig Hinweise zu „Privacy by Design“ und schützen Ihr Unternehmen vor möglichen Sanktionen durch Behörden oder Reputationsschäden.

Sollte es zu Anfragen von Betroffenen oder Meldungen von Datenschutzverletzungen kommen, kümmern wir uns um eine fristgerechte und rechtskonforme Bearbeitung. Damit sorgen wir für Rechtssicherheit, entlasten Ihre internen Ressourcen und stellen sicher, dass das Thema Datenschutz nachhaltig in Ihre Organisationskultur eingebettet ist.