SMCT MANAGEMENT concept

Umsetzung
der europäischen Datenschutz-Grundverordnung EU-DSGVO

Version:	1.0
Datum der Version:	19.11.2022
Erstellt von:	Stefan Stroessenreuther
Genehmigt von:	Stefan Stroessenreuther
Vertraulichkeitsstufe:	Öffentlich

Inhaltsverzeichnis

1. Zweck, Anwendungsbereich und Nutzer

Im Nachfolgenden wird aufgezeigt, welche Dokumente zur Umsetzung der europäischen Datenschutz-Grundverordnung (EU-DSGVO) bei der Einführung in den Mitgliedsunternehmen [**Verband e.V.]** durch **SMCT MANAGEMENT** bereitgestellt werden. Es wird aufgezeigt, welche Rolle durch **SMCT MANAGEMENT** übernommen wird und welche Kosten zu erwarten sind.

2. Referenzdokumente

- EU DSGVO 2016/679 (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG)
- [relevantes nationales Gesetz oder Verordnung bezüglich der DSGVO Umsetzung]
- [andere örtlichen Gesetze und Vorschriften]

3. EU DSGVO Umsetzungsprojekt

3.1. Umsetzungsziel Einführung DSGVO

Umsetzung des EU-DSGVO Managementsystems im Einklang mit der Datenschutz-Grundverordnung (EU DSGVO 2016/679) des Europäischen Parlaments und des Rates.

3.2. Betriebliche Umsetzung der DSGVO

Während des EU DSGVO Umsetzungsprojektes müssen **nachfolgende** Dokumente (von denen einige Anhänge beinhalten, die hier nicht ausdrücklich erwähnt werden) in einem Datenschutz Handbuch dokumentiert werden.

Die hier genannten Richtlinien, Verfahren und sonstigen Dokumente werden durch **SMCT MANAGEMENT** bereitgestellt. Für die Umsetzung bzw. **Überarbeitung** der Dokumente ist das jeweilige Unternehmen zuständig.

- **Politik des Schutzes personenbezogener Daten** – diese Politik bezieht sich auf die Bestimmung der Grundprinzipien des Schutzes personenbezogener Daten, als auch auf den Nachweis, dass sich das Unternehmen diesen Prinzipien verpflichtet;
- **Politik des Schutzes personenbezogener Daten von Arbeitnehmern –** diese Politik legt dar unter welchen Bedingungen das Unternehmen personenbezogene Daten seiner Arbeitnehmer bearbeitet;
- **Datenschutzerklärung –** eine Erklärung, die darlegt unter welchen Bedingungen ein Unternehmen die personenbezogenen Daten seiner Klienten/ Website-Besucher bearbeitet;
- **Verzeichnis der Datenschutzerklärungen** – ein Dokument, in dem Sie alle veröffentlichten Erklärungen aufführen müssen;
- **Politik der Datenspeicherung –** Politik, die den Zeitrahmen darlegt, in dem das Unternehmen personenbezogene Daten aufbewahren darf;

- **Arbeitsbeschreibung des Datenschutzbeauftragten –** ein Dokument, in dem die Verantwortlichkeiten des Datenschutzbeauftragten beschrieben ist;
- **Richtlinien für das Datenverzeichnis und die Zuordnung von Verarbeitungstätigkeiten –** ein Dokument, welches erklärt, wie alle Datenverarbeitungstätigkeiten aufgeführt werden;
- **Verzeichnis von Verarbeitungstätigkeiten –** ein Dokument, das vom Unternehmen genutzt werden sollte, um die Übereinstimmung mit den Anforderungen von Artikel 30 der DSGVO nachzuweisen;
- **Einverständniserklärung betroffener Personen -** ein Dokument, das vom Unternehmen genutzt wird, um das Einverständnis betroffener Personen zu erlangen personenbezogene Daten für einen bestimmten Zweck zu verarbeiten;
- **Widerrufung der Einverständniserklärung betroffener Personen –** ein Dokument, das von betroffenen Personen genutzt wird, um ihr Einverständnis zu widerrufen;
- **Elterliche Einverständniserklärung –** ein Dokument, das vom Unternehmen genutzt wird, um das Einverständnis von Eltern/Erziehungsberechtigten/Vertretern eines Minderjährigen zu erlangen, personenbezogene Daten für einen bestimmten Zweck zu verarbeiten;
- **Widerrufung der elterlichen Einverständniserklärung** – ein Dokument, das von Eltern/Erziehungsberechtigten/Vertretern eines Minderjährigen genutzt wird, um ihr Einverständnis zu widerrufen, personenbezogene Daten für einen bestimmten Zweck verarbeiten zu dürfen;
- **Verfahren des Zugangsersuchens betroffener Personen –** ein Dokument, das einen Prozess erstellt anhand dem das Unternehmen auf Ersuchen betroffener Personen antwortet;
- **Methodik der Datenschutz-Folgenabschätzung** – ein Dokument, in dem beschrieben wird, wie die Notwendigkeit und Verhältnismäßigkeit einer bestimmten Verarbeitungstätigkeit abgeschätzt wird und in den Maßnahmen bereitgestellt werden, die möglichen Risiken für die Rechte und Freiheiten betroffener Personen zu mindern;
- **Verzeichnis der DSFA –** ein Dokument, das vom Unternehmen genutzt wird, um den DSFA-Prozess zu dokumentieren. Es umfasst den Schwellenfragebogen und den Datenschutz- Folgenabschätzungsfragebogen;
- **Verfahren der grenzüberschreitenden personenbezogenen Datenübertragung –** ein Dokument, in dem die Bedingungen festgelegt sind, unter denen die grenzüberschreitende Datenübertragung ausgeführt werden darf;
- **Standardvertragsklauseln –** Modellklauseln, herausgegeben von der EU-Kommission, um angemessene Schutzmaßnahmen bereitzustellen hinsichtlich des Schutzes der Privatsphäre und der Grundrechte und Freiheiten des Einzelnen und der Ausübung der dazugehörigen Rechte;
- **DSGVO Einhaltungsfragebogen für den Auftragsverarbeiter –** ein Fragebogen zur Bewertung der Übereinstimmung des Zulieferers mit EU DSGVO;
- **Vereinbarung über die Datenverarbeitung mit Lieferanten –** ein Vertragsdokument, das die Grenzen und Bedingungen festlegt, unter denen der Zulieferer (Auftragsverarbeiter) personenbezogene Daten für das Unternehmen (Verantwortliche) verarbeiten darf;

3.3. Ergänzende DSGVO Dokumentation

Der Schutz von personenbezogenen Daten umfasst neben der Dokumentation auch die Einhaltung und Gewährleistung von Richtlinien, die den Schutz von personenbezogenen Daten sicherstellen und das Risiko durch unbefugte Einsichtnahme in sensiblen Daten minimiert.

Die hier genannten Richtlinien, Verfahren und sonstige Dokumente werden durch **SMCT MANAGEMENT** bereitgestellt. Für die Umsetzung bzw. Überarbeitung der Dokumente ist das jeweilige Unternehmen zuständig.

- **IT-Sicherheitspolitik** – beschreibt die Grundsicherheitsvorschriften für alle Arbeitnehmer;
- **Zugangssteuerungsrichtlinie** – definiert auf welche Weise das Management Zugangsrechte bestimmten Nutzern des Informationssystems genehmigt;
- **Sicherheitsverfahren für die IT-Abteilung** – beschreibt Sicherheitsregeln, die in der IT-Infrastruktur befolgt werden müssen;
- **Bring Your Own Device (BYOD) Richtlinie** – beschreibt die Regeln für Nutzung von Handys und anderer firmenfremder Geräte zu Geschäftszwecken;
- **Richtlinie zu Mobilgeräten und Telearbeit** – beschreibt die Sicherheitsregeln für den Gebrauch von Laptops, Handys und anderer Geräte außerhalb des Firmengeländes;
- **Richtlinie zum aufgeräumten Arbeitsplatz und leeren Bildschirm** – definiert wie Informationen am Arbeitsplatz und auf Computerbildschirmen geschützt werden;
- **Richtlinie zur Klassifizierung von Informationen** – definiert, wie Daten in Bezug zu Vertraulichkeit zu klassifizieren sind und wie Daten entsprechend geschützt werden;
- **Richtlinie der Anonymisierung und Pseudonymisierung** – definiert wie diese Techniken angewendet werden, um die personenbezogene Datenverarbeitung zu schützen;
- **Richtlinie des Einsatzes von Verschlüsselung** – definiert, wie kryptografische Kontrollen und Schlüssel zu benutzen sind, um die Vertraulichkeit und Integrität der Daten zu schützen;
- **Notfallwiederherstellungsplan** – definiert, wie die Infrastruktur und Daten nach einem Störfall wiederherzustellen sind;
- **Verfahren für interne Audits** – definiert, wie die organisatorischen und technischen Sicherungsvorkehrungen in einem Unternehmen zu testen, zu beurteilen und zu evaluieren sind;
- **Reaktion auf eine Datenschutzverletzung und Meldeverfahren –** ein Verfahren, das, im Falle einer Datenschutzverletzung, die Verpflichtungen des Unternehmens festlegt;
- **Verzeichnis der Datenschutzverletzung** – internes Register der Datenschutzverletzungen des Unternehmens;
- **Meldungsformular der Datenschutzverletzung an die Aufsichtsbehörde** – Dokument, das im Falle einer Datenschutzverletzung genutzt wird;
- **Meldungsformular der Datenschutzverletzung an betroffene Personen –** Dokument, das im Falle einer Datenschutzverletzung genutzt wird.

3.4. Tools für die Umsetzung, Berichterstattung

Ein Cloud Ordner, der alle während der Umsetzung erzeugten Dokumente umfasst, wird auf der Cloud „**Unser-Kundenportal.de**“ für alle teilnehmenden Unternehmen erstellt. Alle Unternehmen haben Zugriff auf diese Dokumente. Diese können jederzeit vom jeweiligen Unternehmen heruntergeladen werden und lokal gespeichert werden. Jedes Unternehmen erhält einen Zugriff mit den nur für das Unternehmen gültigen Zugangsdaten.

3.5. Schulung

Alle Unternehmen haben Zugriff auf unsere **E-Learning Plattform** für eine Basis Schulung der EU-DSGVO. Die Schulung beinhaltet einen multiple-choice Prüfung am Ende der Schulung. Nach bestandener Prüfung erhalten alle Teilnehmer ein Zertifikat.

3.6. Interne Audits

Jährlich wiederkehrendes Datenschutz Audit zur Überprüfung, dass alle Forderungen wirksam umgesetzt wurden. Werden dabei Abweichungen festgestellt, die die Konformität der DSGVO beeinträch-

tigen, sind durch die teilnehmenden Unternehmen geeignete Maßnahmen zur Risikominimierung umzusetzen.

3.7. Technisch organisatorische Maßnahmen (TOM)

Unternehmen müssen sicherstellen, dass personenbezogene Daten geschützt werden. Dies geschieht durch Umsetzung geeigneter technisch organisatorische Maßnahmen (**TOM mittels der in Pkt. 3.2 + 3.3 aufgeführten Dokumente**). Die Umsetzung erfolgt im Datenschutz durch unterschiedliche Vorkehrungen, die von den Verantwortlichen im Unternehmen getroffen werden müssen, um die Sicherheit der erhobenen und verarbeitenden personenbezogenen Daten zu gewährleisten. Die **Ermittlung** der TOM und **daraus resultierenden Maßnahmen** erfolgt anhand einer Risikobewertung bzw. Auditliste durch **SMCT MANAGEMENT**. Für die Umsetzung der Maßnahmen aus der TOM sind die teilnehmenden Unternehmen verantwortlich.

4. Kostenaufstellung

4.1. Einmalige Kosten

Referenz	Beschreibung	Kosten
3.5	Schulung der Mitarbeiter zur EU-DSGVO (Anforderungen, Mindeststandards) über E-Learning Plattform mit multiple-choice Prüfung und Zertifikat	120,00 €
3.2 + 3.3	Datenschutz Handbuch mit allen erforderlichen Dokumenten gemäß Pkt. 3.2 + 3.3	650,00 €
3.7	Ermittlung der technisch organisatorischen Maßnahmen (TOM) Remote über MS TEAMS®)	450,00 €
Kosten sind jeweils pro Unternehmen		

4.2. Jährliche Kosten

Referenz	Beschreibung	Kosten
3.6	Datenschutzaudit (jährlich wiederkehrend) zur Überprüfung auf wirksame Umsetzung der Forderungen aus der DSGVO (Remote über MS TEAMS®)	380,00 €
	Pauschale Kosten als Aufwandsentschädigung, Anfragenbeantwortung etc.	240,00 €
Kosten sind jeweils pro Unternehmen		

4.3. Optionale Kosten

Referenz	Beschreibung	Kosten
	Unterstützung bei der Bearbeitung und Umsetzung der Standards, z.B. technisch organisatorische Maßnahmen (Remote über MS TEAMS®)	680,00 pro AT
	Unterstützung bei der Bearbeitung und Umsetzung der Standards vor-Ort (Aufwand AT zzgl. Reisekosten)	880,00 pro AT
	Unterstützung bei der Bearbeitung von Datenschutzfolge-Abschätzungen	680,00 pro AT
	Software Online Datenschutz – über Webbrowser ausführbar	9,99 mtl.
Kosten sind jeweils pro Unternehmen		