CHECKLISTE DSGVO

Weniger ist mehr – oder: nicht zuviel statt viel zuwenig

Vorbereitung:

Die GF muss es wollen; Statt Belastung Nutzen bedenken: Bessere Unternehmenssteuerung, Marktchancen, Reduktion von Haftungsrisiken

Was ist zu tun:

Entscheidung zu treffen, Das Wollen ins Tun bringen, Mitarbeiter einbinden

SINNVOLLES DSMGMT FÜR KMUs

Inhaltsverzeichnis

Die Checkliste in 3 Teilen

Phase 1 Vorbereitung

1.1. Management Awareness bilden und Management Commitment festlegen

1.2. Projektauftrag für Umsetzungsprojekt einholen

1.3. Ressourcen bereitstellen

1.4. Schlüsselpersonal schulen

1.5. Prüfen ob Datenschutzbeauftragter notwendig ist (Artikel 9,10,37 DSGVO)

Phase 2 Umsetzung

2.1. Verarbeitungstätigkeiten identifizieren

2.2. Verfahrungsverzeichnis erstellen

2.3. Risikoanalyse durchführen

2.4. Einhaltung der Datenschutzgrundsätze sicherstellen

2.5. Datensicherheitsmaßnahmen
(TOMs = technische und organisatorische Maßnahmen durchsetzen)

2.6. Betroffenenrechte wahren

2.7. Einwilligungsprozess einführen

2.8. Informationspflichten einführen

2.9. Auftragsverarbeiter-Rahmenbedingungen sicherstellen

Phase 2 Umsetzung (Fortsetzung)

2.10. Privacy by Design und Privacy by Default sicherstellen

2.11. Data breach Prozess einführen

2.12. Die Aufgaben des Datenschutzbeauftragten (DSB)

2.13 Datenschutz Policy erstellen

2.14. Mitarbeiter schulen

2.15. Datenübermittlung (EU / International)

Phase 3 Laufende Tätigkeiten

3.1. Verfahrensverzeichnis aktualisieren

3.2. Audits durchführen

3.3. Kontakt mit Behörden und betroffenen Personen pflegen

3.4. KVP des Datenschutzs- Managementsystems (DSMS) sicherstellen

Kompakte Checkliste zur Umsetzung der Datenschutzsgrundverordnung.

Zusätzliche Materialien zur Powerpoint Präsentation

Urheber der Checkliste und der daraus erfließenden Beschreibungen ist die Vereinigung der Datenschutzsbeauftragten im Verein Privacy Officers. Die Daten sind öffentlich im Netz zur Verfügung gestellt, der Link lautet:

https://www.privacyofficers.at/Privacyofficers_Checkliste_Umsetzung_DSGVO_v1.0_24052017_FINAL.pdf

Zielsetzung ist es allen Unternehmen aber insbesondere auch kleineren und mittleren Betrieben, die im voraus kein Spezialpersonal wie Datenschutzofficer Datenschutzbeauftragten, CIO bestellen können mit dieser Checkliste ein Bild der möglichen, vorgeschriebenen, aber vor allem sinnvollen und zumutbaren Maßnahmen (hier differenziert der Gesetzgeber sehr zum Vorteil der kleineren Unternehmen) zur Verfügung zu stellen.

Phase 1 Vorbereitung

1.1. Management Awareness bilden und Management Commitment einholen

Das Datenschutzmanagement ist auch in kleinen Unternehmen wesentlich. Stellen Sie sicher, dass es zumindest eine Einsicht zur Notwendigkeit des Datenschutzes gibt. Die Umsetzung der Datenschutzgrundverordnung erfolgt durch vom Management ausgehend durch Selbstverpflichtung und Schulung von Awareness.

Phase 1 Vorbereitung

1.2. Projektauftrag für Umsetzungsprojekt einholen

Im Projektauftrag ist es wesentlich, dass Sie das Datenschutzmanagement als eigenes Projekt begreifen. Alle Betroffenen einbinden, Ziel des Projekts festlegen, was soll/was darf nicht passieren, Budget festlegen, Rahmenbedingungen identifizieren und eine Verbindlichkeit herstellen.

Phase 1 Vorbereitung

1.3. Ressourcen bereitstellen

Je nach Größe des Unternehmens sind finanzielle und / oder personelle Ressourcen für die Datenschutzorganisation bereit zu stellen. Zum Beispiel: Datenschutzbeauftragter, Datenschutzkoordinatoren, etc.

Phase 1 Vorbereitung

1.4. Schlüsselpersonal schulen

In jedem Unternehmen gibt es Personen, die mit Daten zu tun haben. Diese sind zu schulen. Die Datenverarbeitung i.e. ermitteln, registrieren, verändern, ergänzen, etc. – setzt immer voraus, dass es einen Impuls von einer Person gibt. Diese Personen sind zu schulen.

Phase 1 Vorbereitung

1.5. Prüfen ob Datenschutzbeauftragter notwendig ist (Artikel 9,10,37 DSGVO)

Prüfen ob Datenschutzbeauftragter notwendig ist. Siehe Auflagen zu einem Datenschutzbeauftragten (Unternehmen über 250 Mitarbeiter, Verarbeiter von kritischen Daten, Datenverarbeitung als zentrales Geschäftsmodell). Gesetzgeber ist hier sehr großzügig in puncto Zumutbarkeit und Umsetzungsmöglichkeit für kleinere und mittlere Betriebe. Details bitte klären.

(Gesetzgeber ist aber hier auch sehr ungenau!)

Phase 2 Umsetzung

2.1. Verarbeitungstätigkeiten identifizieren

Was sind Verarbeitungstätigkeiten? Diese sind zu identifizieren und zu dokumentieren.

Daten ermitteln, Daten speichern, verändern, verschicken, ablegen, ergänzen, verändern, löschen etc. Verarbeitungstätigkeit bewusst weitfassen, immer wenn sie Daten anschauen, benützen, erfolgt schon eine Verarbeitungstätigkeit. Welche personenbezogenen Daten, welcher betroffenen Personen werden verarbeitet, zu welchem Zweck werden sie verarbeitet, was ist die Rechtsgrundlage zB. Vertragserfüllung, Einwilligungserklärung, wo kommen die Daten her, wo gehen sie hin, wie lange warden sie benötigt, wie umfangreich sind sie, was wird nicht mehr benötigt, was kann gelöscht werden.

Phase 2 Umsetzung

2.2. Verfahrensverzeichnis erstellen

Diese Verpflichtung trifft auch auf kleinere Unternehmen zu. Was tun wir mit den Daten. Wie tun wir es. Kategorien von Empfängern gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offen gelegt werden (Sozialversicherung, Finanzamt, Steuerberater etc.) Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien festhalten.

Vor allem wichtig sind Namen und Kontaktdaten z.B. eines Auftrags für Arbeiter bzw. Auch des Datenschutzbeauftragten. Auch hier müssen schriftliche Dokumentationen dieser Verfahren erfolgen.

Phase 2 Umsetzung

2.2. Verfahrensverzeichnis erstellen

Achtung auch hier sind die Bestimmungen unscharf, das Verfahrensverzeichnis hat keine bestimmte zentrale Formvorschrift, jedoch soll die Unterlage alle wesentlichen Informationen enthalten. Kontaktdaten des Verantworklichen, Zweck der Verarbeitungstätigkeit, Kategorien betroffener Personen und Kategorieren pb Daten (z.B. Mitarbeiter, Kunden, Lieferanten, Rechnungsdaten, Adressdaten etc.)

Phase 2 Umsetzung

2.3. Risikoanalyse durchführen……nicht verpflichtend für KMUs, aber…

(z.B. Datenschutz – Folgenabschätzung: Reputationsschaden, finanzieller Schaden, Strafen etc.)

Risikoanalyse erfolgt durch eine Vorprüfungsphase (welche Technologie wird angewandt, welche Personen sind involviert, was wird getan um die Sicherheit der Verarbeitungstätigkeit zu erhöhen (zB. Passwörter, Raumsperren, Zugangsdifferenzierungen, Videoüberwachungen) und um das Risiko zu verringern.

Phase 2 Umsetzung

2.4. Einhaltung der Datenschutzgrundsätze sicherstellen

Rechtmäßigkeit der Verarbeitung, Datenminimierung und Zweckbindung, Speicherbegrenzung, Richtigkeit, Integrität, Vertraulichkeit, Verfügbarkeit, Rechenschaftspflicht und vor allem auch die Frage der Dokumentation, was haben wir getan, wie ist es dokumentiert.

Phase 2 Umsetzung

2.5. Datensicherheitsmaßnahmen

(TOMs = technische und organisatorische Maßnahmen durchsetzen)

Datensicherheitsmaßnahmen angehen: Technische, organisatorische Maßnahmen setzen, Stand der Technik nach national anerkannten Normen sicherstellen, z.B. ISO, IEC 27001 und vor allem hier wiederum die Personalsicherheit beachten, Prozesse, Teamwechsel, Austritt, etc.

Checklisten erstellen, was hat zu passieren wenn, hier fallen auch die Bereiche hinein, Verschlüsselung, Klärung von Lieferantenbeziehungen (zB. ganz speziell Fernwartungen und Vorort-Services, Dienstleisterbeziehungen etc.

Hier können Sie auch Details wie zB Länge des Passworts etc. festlegen.

Phase 2 Umsetzung

2.6. Betroffenenrechte wahren

Siehe Artikel 15 bis 23 Datenschutzgrundverordnung und Erwägungsgründe 60 bis 73

Phase 2 Umsetzung

2.7. Einwilligungsprozesse definieren und umsetzen

Einwilligungsprozess beachten, Rechtmäßigkeit der Verarbeitung personenbezogener Daten (z.B. Erfüllung eines Vertrages oder einer rechtlichen Verpflichtung) müssen registriert und nachweisbar sein. Achtung hier nicht „link“ handeln, also bei einem Kästchen, dass die Person anklicken kann wenn hier bereits ein vorausgefüllte, angekreuztes Kästchen da ist, gilt dies nicht als Zustimmung. Schweigen ist hier ebenfalls keine Zustimmung.

Phase 2 Umsetzung

2.8. Informationspflichten definieren und fixieren

Hier wäre eine sehr umfangreiche Vorgabenliste zu beachten. Zwecke für die die Daten verarbeitet werden, Rechtsgrundlage, welches Interesse liegt der Datenverarbeitung zugrunde, wer empfängt die Daten, wie lange werden sie gespeichert, gibt es ein Beschwerderecht bei einer Aufsichtsbehörde (verändern, löschen, ergänzen)

Phase 2 Umsetzung

2.9. Auftragsverarbeiter-Rahmenbedingungen sicherstellen

Verpflichtende Vorgaben für Dienstleister (zB Clouddienste-Anbieter, Hosting-Anbieter, Software-Provider, ausgelagerte Lohnverrechnungen, Dienstleister innerhalb eines Konzerns etc.)

Phase 2 Umsetzung

2.10. Privacy by Design und Privacy by Default sicherstellen

Heisst, dass technische Anforderungen zB Software, die vornherein so konzipiert ist, dass diese Privacy gewahrt bleibt. Privacy by Default bedeutet, dass Produkte oder Dienstleistungen standardmäßig datenschutzfreundlich vorkonfiguriert sind, um eine zufällige, fahrlässige oder vorsätzliche Verletzung des Datenschutzes zu unterbinden.

Phase 2 Umsetzung

2.11. Data breach Prozess einführen

Vor allem ist sicherzustellen, dass bei einer Datenschutzverletzung bestimmte Schritte definiert sind. Wer macht was wann? Wer muss welche Entscheidungen treffen? Aus welchen Rollen setzt sich z.B. ein CERT (Computer Emergency Response Team) zusammen.

Wann sind Betroffene und die Datenschutzbehörde zu informieren?

Phase 2 Umsetzung

2.12. Die Aufgaben des Datenschutzbeauftragten (DSB)

Datenschutzbeauftragte hat eine kontrollierende und unterstützende Funktion. Einhaltung der Datenschutzgrundverordnung, Sicherstellung eines funktionierenden Datenschutzmanagementsystems (durch Unterstützung) und Rechenschaftspflicht gegenüber der Behörde. (Haftung)

Phase 2 Umsetzung

2.13 Datenschutz Policy erstellen

Was tun wir wie?

Phase 2 Umsetzung

2.14. Mitarbeiter schulen

Phase 2 Umsetzung

2.15. Datenübermittlung (EU / International)

Ist besonders heikel bei internationaler Datenübermittlung.

Phase 3 Laufende Tätigkeiten

3.1. Verfahrensverzeichnis aktualisieren

Einmal jährliche Aktualisierung des Verfahrensverzeichnisses, Überprüfung der Zuständigkeit, Ergänzungen und Korrekturen. Bsp: weitere andere Daten, weitere andere Betroffene, Zweckänderung, Hinzutreten von Empfängern, Veränderte Speicher/Löschfristen, Änderungen von verantwortlichen Rollen, z.B DSB Anpassung der TOMs oder erweiterte Garantien und Vereinbarungen mit Dienstleistern, Anpassung zugrunde liegender Dokumente (Einwilligungserklärung, Verträge, Betriebsvereinbarungen etc.), Überprüfung der Aktualität der Risikobewertung usw.

Phase 3 Laufende Tätigkeiten

3.2. Audits durchführen

Interne und externe Audits (KVPs), Berichtsanfertigung, Berichte an das Management bzw. Handlungsanleitungen für zukünftige Datenschutz Struktur und Verhalten. Hier hilft der DSB.

Phase 3 Laufende Tätigkeiten

3.3. Kontakt mit Behörden und betroffenen Personen pflegen, DSB ins Unternehmen holen

Phase 3 Laufende Tätigkeiten

3.4. KVP des Datenschutzs- Managementsystems (DSMS) sicherstellen

Erkennen und Behebung von Nichtkonformitäten. Fortlaufende Evaluierung und Verbesserung von TOMs i.e. z.B. Stand der Technik, Bedrohungslage, Mitarbeiterawareness, Datenschutzpolicy, datenschutzrelevante Prozesse (Auskunft, Einwilligung etc.), Verträge mit Auftragsverarbeitern, Standardvertragsklauseln, interne bzw. externe Audits organisieren = datenschutztechnisch und –organisatorisch verordnungskonform sein und bleiben.