🙂

Checkliste zum nDSG

Projektplanung

☐ Informiere dich umfassend über das neue Datenschutzgesetz.

☐ Lege klare Verantwortlichkeiten und Funktionen für die Planung und Durchführung des Projektes fest.

☐ Weise die erforderlichen finanziellen und personellen Ressourcen zu.

☐ Identifiziere die datenschutzrelevanten Bereiche in deinem Unternehmen, also die Bereiche, in denen personenbezogene Daten verarbeitet werden.

☐ Identifiziere die nötigen technischen und organisatorischen Massnahmen, um Konformität mit dem nDSG zu erreichen.

☐ Kläre den Projektablauf und plane die einzelnen Schritte.

☐ Setze eine realistische Zeitplanung fest.

Bearbeitungsverzeichnis

☐ Erstelle eine entsprechende Datei und prüfe, ob die Pflichtfelder für dein Unternehmen ausreichen oder ergänzt werden müssen.

☐ Identifiziere die Abteilungen, in denen Personendaten erfasst werden.

☐ Schule die Mitarbeiter:innen, wie sie die Excel-Tabelle richtig ausfüllen und welche Informationen erfasst werden müssen.

☐ Lasse die Abteilungen alle Bearbeitungstätigkeiten erfassen.

☐ Überprüfe die gesammelten Inventare auf Richtigkeit und Vollständigkeit.

☐ Stelle die Ergebnisse in einer gemeinsamen Tabelle zusammen: Sammle alle Informationen aus den verschiedenen Abteilungen und füge sie in einer zentralen Tabelle zusammen.

☐ Implementiere einen Prozess zur Aktualisierung: Lege fest, in welchen Zeitabständen die Tabelle aktualisiert wird, um sicherzustellen, dass Änderungen in der Datenbearbeitung regelmässig aufgenommen werden. Das muss mindestens jährlich geschehen.

Datenschutzerklärung

☐ Sammle und erfasse alle Bearbeitungstätigkeiten in deinem Unternehmen.

☐ Gruppiere die Bearbeitungstätigkeiten nach Datenkategorien, Bearbeitungszwecken, Auftragsverarbeitern und Aufbewahrungskriterien.

☐ Überarbeite deine Datenschutzerklärung. Du kannst auch die betroffenen Abteilungen einbeziehen.

☐ Platziere Hinweise auf deine Datenschutzerklärung auf deiner Webseite, in E-Mails und in Apps.

☐ Implementiere einen Prozess zur Aktualisierung. Lege fest, in welchen Zeitabständen deine Datenschutzerklärung aktualisiert wird, um sicherzustellen, dass Änderungen regelmässig eingearbeitet werden. Mindestens jährliche Aktualisierungen sind empfehlenswert.

Auftragsbearbeitung

☐ Verschaffe dir eine Übersicht aller Auftragsbearbeiter, mit denen du personenbezogene Daten teilst.

☐ Verwende Muster-Verträge und passe sie entsprechend deinen Bedürfnissen an, oder frage bei den Auftragsbearbeitern nach, ob sie einen eigenen Muster-Vertrag anbieten

☐ Handle den genauen Vertragsinhalt mit jedem Auftragsbearbeiter individuell aus.

☐ Schliesse die Verträge ab und bewahre sie auf: Nachdem alle Details geklärt sind, unterzeichne die Auftragsverarbeitungsverträge (AVVs bzw ABVs) und bewahre sie sicher auf, um deine Rechtskonformität nachweisen zu können.

Auslandtransfers

☐ Erstelle eine Übersicht aller deiner Datenverarbeiter im Ausland.

☐ Erstelle eine Vereinbarung mit jedem Datenbearbeiter und füge die SCC ein.

☐ Lies die SCC sorgfältig durch und passe sie nur dort, wo es ausdrücklich nötig ist, an deinen Kontext an.

☐ Schliesse die Verträge ab und bewahre sie auf, um deine Rechtskonformität nachweisen zu können.

Betroffenenrechte

☐ Identifiziere alle Orte im Unternehmen, an denen personenbezogene Daten gespeichert werden. Das sollte aus dem Bearbeitungsverzeichnis ersichtlich sein, wenn du ein solches erstellt hast.

☐ Stelle sicher, dass es eine Möglichkeit gibt, diese Daten strukturiert zu exportieren.

☐ Entwickle und implementiere interne Prozesse, nach denen Anfragen bearbeitet werden (je ein eigener Prozess für Anfragen nach Auskunft, Datenweitergabe, Korrektur oder Löschung der Daten sowie Widerruf von Einwilligungen)

☐ Erstelle Musterschreiben für die verschiedenen Anfragen.

☐ Lege die Zuständigkeiten für die Beantwortung von Anfragen fest und schule die involvierten Mitarbeiter:innen.

Datensicherheit durch TOMs

☐ Bestimme eine Person in deinem Unternehmen, die den Prozess der Massnahmenumsetzung koordiniert. Das kann dein:e Datenschutzberater:in sein, wenn dein Unternehmen eine solche ernannt hat.

☐ Identifiziere aufgrund der Massnahmenliste potenzielle Schwachstellen und Risiken in Bezug auf die Datenverarbeitung in deinem Unternehmen. Prüfe auch, ob das Prinzip Privacy by Default eingehalten wird.

☐ Kläre mit den entsprechenden Abteilungen und IT-Spezialisten ab, welche Massnahmen ergriffen werden können, um die Datensicherheit zu erhöhen. Auf der technischen Seite können das verbesserte Zugangskontrollen, Verschlüsselungen, Backups, Datenlöschungen und Systemupdates sein; auf der organisatorischen Seite Bearbeitungsreglemente, Schulungen, Notfallpläne und Dokumentationen.

☐ Erstelle eine Prioritätenliste und überwache die Umsetzung.

☐ Implementiere einen Prozess, nach dem die TOMs regelmässig überprüft und aktualisiert werden, um sicherzustellen, dass sie auch in Zukunft den aktuellen Bedrohungslagen und Anforderungen entsprechen.

Extra: E-Mail-Versand

☐ Stelle sicher, dass dein CRM die Möglichkeit enthält, Einwilligungen für Marketingnachrichten festzuhalten.

☐ Ergänze wo nötig deine Datenformulare um die Einwilligung für den Erhalt von Marketingnachrichten.

☐ Richte das Double-Opt-In-Verfahren bei allen E-Mail-Anmeldungen ein.

☐ Stelle sicher, dass bei jeder Datenerhebung auf die Datenschutzerklärung hingewiesen wird.

☐ Vergewissere dich, dass deine E-Mails von einer anschreibbaren Absenderadresse gesendet werden und dass alle Werbenachrichten Absender- und Kontaktangaben sowie eine Abmeldemöglichkeit enthalten.

☐ Schliesse einen Auftragsverarbeitungsvertrag mit deinem E-Mail-Dienstleister ab.

Fazit

☐ Führe Mitarbeiterschulungen durch, damit alle Beteiligten die erforderlichen Kenntnisse und Fähigkeiten haben, um den Datenschutz in der Praxis zu gewährleisten.

☐ Plane regelmässige Überprüfungen und Aktualisierungen der Datenschutz-Compliance, um auf Veränderungen sowohl in deinem Unternehmen als auch in der technischen Entwicklung zeitnah einzugehen.