Checkliste: EU-DSGVO

Prüfen Sie in wenigen Schritten, ob Ihr Unternehmen den neuen Datenschutz-vorschriften der EU gerecht wird.

Die EU-Datenschutzgrundverordnung (DSGVO) mit Anwendung ab dem 25. Mai 2018 wird eine weitgehende Vereinheitlichung des europäischen Datenschutzrechts bewirken. Sie hat zum Ziel, die Grundrechte und -freiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten abzusichern. Für Unternehmen hat die Vorschrift eine Anpassung der Geschäftsprozesse zur Folge.

Dieses Ziel der neuen Verordnung soll durch umfangreiche Grundsätze zur Verarbeitung personenbezogener Daten erreicht werden, insbesondere Rechtmäßigkeit, Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit sowie Rechenschaftspflicht.

Die CINTELLIC Consulting Group hat eine Checkliste zur DSGVO erstellt, mit der Sie sich einen Überblick zum Thema verschaffen können. Anhand der Liste können Sie prüfen, ob Ihr Unternehmen bereit für die DSGVO ist – oder aber welche Maßnahmen Sie gegebenenfalls noch ergreifen müssen, um den neuen Vorschriften gerecht zu werden. Eine gewissenhafte Prüfung lohnt sich, denn bei Verstößen gegen die EU-Verordnung drohen Strafen von bis zu 20 Mio. € bzw. 4% des weltweiten Unternehmensumsatzes. Dabei stellt die Checkliste Prüfungskriterien aus fachlicher Sicht dar und ersetzt keine rechtliche Prüfung.

Checkliste Teil 1

☐ **1. Erstellung einer Planung/ Projekt-Setup**
☐ 1.1. Verantwortlichkeiten definieren, Projektteam aufsetzen
☐ 1.2. Verständnis schaffen und juristische Beratung involvieren
☐ 1.3. Meilensteinplan aufsetzen, Arbeitspakete verteilen Ressourcen- & Budgetplanung aufsetzen

☐ **2. Aufbau & Verzahnung eines formellen Datenschutz-Managementsystems**
☐ 2.1. Datenschutz-Management:
☐ • Datenschutzkonzept ausarbeiten inkl. Projektplan, Umsetzungsplanung, Aufgabenpriorisierung
☐ • Internes Audit planen (Revision, Datenschutz-Beauftragter)
☐ • Unternehmensinterne Kommunikation anstoßen
☐ 2.2. Klassifizierung von Dokumenten/ Informationen bezüglich Vertraulichkeit & Schutzzielen
☐ • Identifikation von personenbezogenen Daten und Vergabe von Bearbeitungsrechten
☐ 2.3. Datenschutzorganisation: Einbindung in Compliance- & Risiko-Monitoringsysteme

☐ **3. Erstellung von Dokumentationen & Vereinbarungen** zur Anlage von Verzeichnis- und Verarbeitungstätigkeiten der Unternehmen und Auftragsverarbeiter
☐ 3.1. Update des heutigen Verfahrensverzeichnisses
☐ 3.2. Umfassende Dokumentation der Datenflüsse
☐ • wie werden Daten über welchen Kanal erfasst
☐ • wo werden Daten gespeichert, wo liegen Metadaten
☐ • wie werden Daten zu welchem Zweck und wo verarbeitet
☐ • wann werden Daten gelöscht
☐ • wann muss die Speicherung der Daten erfolgen
☐ 3.3. Anpassung der ADV‘s an neue Anforderungen & Haftungsklauseln
☐ 3.4. Update interner Dokumente (Betriebsvereinbarungen, Policies, Arbeitsanweisungen etc.)
☐ • neue Prozesse auf Fach- und IT Seite definieren, betreffend Auskunftserteilung, Portabilität von Daten bei Anbieterwechsel
☐ • Anträge auf Löschung und Korrektur von Daten etablieren
☐ 3.5. Update der Datenschutzerklärungen/ Informationen an betroffene Personen; Integration der Informationspflichten (Art. 12-15)
☐ • Neue Formulierungen aufsetzen, inkl. transparenter Darlegung der Datenschutz-Erklärung
☐ • Nachträgliches Einholen der neuen Datenschutzerklärungen/ Opt-Ins von den betroffenen Personen

☐ **4. Erstellung einer Risikoanalyse & Folgenabschätzung**, im Bedarfsfall frühzeitige Einbindung der Aufsicht
☐ 4.1. Prüfung bisheriger Bewertungen auf Basis neuer Begriffsbedeutungen
☐ 4.2. Risikoanalyse analog ISO 27005 oder 29134
☐ 4.3. Konzeption und Implementierung eines Meldeprozesses bei Verletzung an Aufsichtsbehörde innerhalb von 72 Stunden (Art. 33)
☐ 4.4. Schulung betroffener Mitarbeiter zur korrekten und fristgerechten Vorgehensweise bei Datenschutz-Verletzungen
☐ 4.5. Datenschutz-Folgenabschätzung (Art. 35)
☐ • Anhand separater Checklisten die prüfungsrelevanten Fälle identifizieren
☐ • Planung der Prüfungsdurchführung und Einbindung der Aufsicht
☐ 4.6. Output: Überblick über erforderliche rechtliche und technisch-organisatorische Anpassungen

☐ **5. Bestellung eines unternehmensinternen Datenschutzbeauftragten**

Checkliste Teil 2

☐ **6. Technische Umsetzung der Datenschutzregeln** zur Sicherheit der Verarbeitung (Art. 32)
☐ 6.1. „Verfremdung“ von Daten durch Krypto-Konzept, Pseudonymisierung oder Anonymisierung
☐ 6.2. Aufbau von Sicherheitsmaßnahmen um Datenverlust zu vermeiden
☐ 6.3. Aufbau eines Systems das die Sicherheitsmaßnahmen auf Funktionalität überprüft
☐ 6.4. Entwicklung eines obligatorischen Notfallkonzeptes
☐ 6.5. Prüfung, ob Privacy by Design bzw. by Default im Unternehmen umgesetzt sind
☐ • Prävention statt nachgelagerter Abhilfe
☐ • Einbettung von Datenschutz und -sicherheit im Design
☐ • Sichtbarkeit und Transparenz
☐ • Respektieren der Privatsphäre der Benutzer
☐ • Datenschutz per „Default“

☐ **7. Planung & Durchführung von Mitarbeiterschulungen**
☐ • insbesondere betreffend Fristen bei Betroffenenrechten & Incident-Management
☐ • betroffene Mitarbeiter wie beispielsweise Juristen, Datenschutzbeauftragte und Revision, Analysten aus Database Marketing, Finance oder BI, IT-Mitarbeiter die Datenhandling verantworten, Sachbearbeiter in direktem und indirektem Kundenkontakt, Abteilungsleiter (operativ & strategisch)

☐ **8. Prüfung konkreter Löschmaßnahmen**
☐ 8.1. Feststellung der Aufbewahrungspflichten inklusive der Prüfung, wann die DSGVO keine Anwendung findet (beispielsweise im Gesundheitswesen)
☐ 8.2. Klassifikation der Daten, die nicht gelöscht werden dürfen und die gelöscht werden müssen (nach Zweckerledigung, Widerruf der Einwilligung, Widerspruch gegen weitere Verarbeitung, Daten von Kindern)
☐ 8.3. wirksame Löschung an allen Speicherorten gewährleisten
☐ 8.4. Vorgehensweise für durchführende Mitarbeiter dokumentieren, Formulare und Prozesse für Lösch- und Widerrufsanträge vorbereiten
☐ 8.5. Mögliches Outsourcing planen

☐ **9. Etablierung von Prozessen & Maßnahmen zur fristgerechten Wahrung der Rechte Betroffener** (binnen eines Monats)
☐ 9.1. Informationspflichten (Art. 13 & 14):
☐ • Überblick, in welchen Prozessen Daten erhoben werden
☐ • Zuordnung der Daten zu Löschfristen
☐ • Ausspielen der Informationen an die Betroffenen
☐ 9.2. Auskunftsrecht (Art. 15):
☐ • Prozesse für Anfragen einrichten
☐ • vollständige Übersicht über gespeicherte Daten
☐ • Formular für Auskunft erstellen
☐ 9.3. Löschpflichten & Recht auf Vergessenwerden (Art. 17):
☐ • Formulare und Prozesse für Lösch- und Widerrufsanträge erstellen
☐ • Löschkonzept erstellen & implementieren
☐ • Analysieren, welche Daten nicht gelöscht werden dürfen / müssen
☐ • Wirksames Löschen an allen Speicherorten gewährleisten
☐ • Dokumentation der Weitergabe an Dritte
☐ • Prozesse zur regelmäßigen Prüfung aufsetzen
☐ 9.4. Eingeschränkte Verarbeitung (Art. 18):
☐ • Formulare und Prozesse einrichten
☐ • Information der betroffenen Person vor Aufhebung der Einschränkung
☐ 9.5. Datenübertragbarkeit (Art. 20):
☐ • Antrag und Prozess zur Datenübertragung einrichten
☐ • Sicheren Kanal zur Datenübermittlung aufbauen
☐ 9.6. Widerspruchsrecht (Art. 21):
☐ • Prozesse zur Prüfung der Rechtmäßigkeit inklusive Datenschutzfolgeabschätzung einrichten
☐ • Prozesse zur Pseudonymisierung oder Anonymisierung einrichten

☐ **10. Erstellung von Nachweisen** über die Etablierung notwendiger Prozesse, Tools für Dokumentation und Protokollierung gegenüber Aufsichtsbehörde

Schlussendlich sollten Sie sich die Frage stellen, ob Sie mit Ihren Planungen und Maßnahmen alle Schwerpunkte der DSGVO abdecken.

Verfügbarkeit	Möglichkeiten der Information darüber, welche Daten über wen gespeichert werden. Auskunft in ausgedruckter Form nur an berechtigte Personen.
Nachvollziehbarkeit	Möglichkeiten der Nachweiserstellung, wie personenbezogene Daten verarbeitet werden (auch, wer die Informationen gesehen hat und wer Zugriff darauf hat und hatte, wo sie wann über welchen Kanal erhoben wurden und wo dafür die Zustimmung gegeben wurde, wie sie von wem und wo in welchem Zustand verarbeitet und wie lange sie gespeichert werden).
Einwilligung	Opt-In-/ Opt-Out-Prozesse einrichten und neue Einwilligungen einholen, falls die aktuellen nicht den neuen Standards entsprechen (klare und transparente Kommunikation, nicht an Dienstleistung oder Produkt gekoppelt).
Transparenz	Klare und verständliche Formulierung, wie personenbezogene Daten verarbeitet und verwendet werden (auch, wo sie seit wann liegen und an wen sie weitergegeben werden und zu welchem Zweck sie verarbeitet werden).
Übertragbarkeit an Dritte	Auf Verlangen der betroffenen Person beispielsweise zur Erleichterung des Anbieterwechsels (verschlüsselte Übermittlung der Daten an die betreffende Person oder an ein Unternehmen seiner Wahl in digitaler Form, inklusive entsprechender Prozesse zum Empfangen und Speichern personenbezogener Daten).
Korrektur	Möglichkeiten der Korrektur falscher Daten.
Löschung	Möglichkeiten der Löschung von Daten, auch nach Einwilligung zur Datenspeicherung.

Wenn Sie einen Großteil der Punkte abhaken können, haben Sie bereits einen großen Schritt in Richtung DSGVO getan. Falls nicht, haben Sie anhand der Checkliste einen Anhaltspunkt, in welchen Aspekten und Themen Sie noch nachschärfen sollten, um dem Inkrafttreten der DSGVO Ende Mai entspannt entgegenblicken zu können.

von Melanie Klein, CINTELLIC Consulting Group

#jointheteam

Wir sind weiterhin auf Wachstumskurs. Vielleicht mit Ihnen!? Starten Sie Ihre Karriere bei CINTELLIC!
https://www.cintellic.com/stellenangebote/

Ansprechpartner

Dr. Jörg Reinnarth
Geschäftsführer
CINTELLIC Consulting Group
joerg.reinnarth@cintellic.com

Stephan Klöckner
Senior Manager
CINTELLIC Consulting Group
stephan.kloeckner@cintellic.com

Über CINTELLIC

Die CINTELLIC Consulting Group ist eine der führenden Unternehmensberatungen für die digitale Transformation von Kundenmanagement und CRM. Der Fokus dabei liegt auf dem integrierten Management in den Schnittstellen der Themenfelder BUSINESS, DATA und TECHNOLOGY.

Ihre Mitarbeiter verfügen über langjährige Erfahrungen in den Bereichen Customer Relationship Management, Customer Experience Management, Marketing Operations Management, Kampagnenmanagement und Business Intelligence.

CINTELLIC verbindet strategisches Know-how mit Kompetenz im Bereich der Datenanalyse und Business Intelligence und bietet Konzeptentwicklung und Umsetzung aus einer Hand.

Cintellic GmbH
Remigiusstraße 16
53111 Bonn
t +49 228 92 18 20
f +49 228 92 18 299
info@cintellic.com
www.cintellic.com

CINTELLIC
CONSULTING GROUP