10 Punkte-Plan für eine effektive Umsetzung der Europäischen Datenschutz-Grundverordnung

Dieser „Fahrplan“ setzt voraus, dass Ihre bisherige Datenschutz-Organisation Up-to-date ist und Sie die Datenschutznovellen von 2001 und (insbesondere) 2009 umgesetzt haben. Die nachfolgenden 10 Punkte basieren auf Empfehlungen der Datenschutzaufsichtsbehörden des Bundes und der Länder. Einen Anspruch auf Vollständigkeit erhebt dieser „10 Punkte-Plan“ selbstverständlich nicht.

1. Sensibilisierung durchführen

Geschäftsführungen, Datenschutzbeauftragte und andere für das Thema Datenschutz Zuständige sollten innerhalb des Unternehmens dafür sensibilisieren, dass sich ab dem 25.05.2018 nicht nur der Name einer europäischen Datenschutzregelung ändern wird. Die DS-GVO wird direkte Auswirkungen auf Unternehmen als datenverarbeitende Stellen haben. Anders als eine EU-Richtlinie ist eine EU-Verordnung direkt in den Mitgliedstaaten der Europäischen Union anwendbar, also auch in Deutsch-land. Neben der DS-GVO wird es weiterhin ein – neues – Bundesdatenschutzgesetz und sektorales Fachrecht (UWG, TKG, TMG, SGBr, BetrVG usw.) mit ausführenden Regelungen zur DS-GVO geben. Bitte beachten Sie: bis zum 24.05.2018 (einschließlich) gilt das JETZIGE Bundesdatenschutz-gesetz!

-> Entwurf grober Zeitplan und Umsetzungsfristen, Ressourcen / Budget

2. Bestandsaufnahme durchführen

Um Änderungsbedarf identifizieren zu können, sollte in einem ersten Schritt eine Bestandsaufnahme der Prozesse durchgeführt werden, in denen personenbezogene Daten verarbeitet werden. Das Verfahrensverzeichnis nach § 4d Bundesdatenschutz-gesetz (BDSG) ist ein Ausgangspunkt zur Identifizierung von Verarbeitungsverfahren. Im Folgenden haben wir beispielhaft einige Themen zusammengestellt, bei denen sich für Unternehmen Änderungsbedarf ergeben kann.

-> Aufbau formelles Datenschutz-Managementsystem und Verzahnung im Unternehmen

- *Etablierung eines "Management-Systems“*
- *Etablierung einer Datenschutz-Policy bzw. eines -Prozesses (Datenschutzkonzept) Achtung: vermutlich mitbestimmungspflichtig (Betriebsrat)*
- *Datenschutz-Risikoabschätzung (s.u.)*
- *Plan für internes Audit (PDCA-Zyklus) = Lernen und verbessern*
- *Kommunikation im Unternehmen*
- *Einbindung von Datenschutzaspekten in Klassifizierung von Dokumenten/ Informationen in Bezug auf Vertraulichkeit / Schutzziele*
- *Einbindung der Datenschutzorganisation in Compliance- und Risiko-Monitoring-Systeme, Prüfung, ob DSB (noch) bestellt werden muss (und wer es sonst machen soll)*

3. Rechtsgrundlage(n) prüfen

Auch unter der DS-GVO ist für die Verarbeitung personenbezogener Daten eine Rechtsgrundlage erforderlich (Artikel 6 bis 11 DS-GVO). Es ist zu prüfen, ob das neue Recht für alle Prozesse Rechtsgrundlagen bereitstellt.

4. Personenbezogene Daten von Kindern besonders prüfen

Besondere Anforderungen bestehen für den Umgang mit personenbezogenen Daten von Kindern, wenn es um die Einwilligung in Bezug auf Dienste der Informationsgesellschaft geht (Artikel 8 DS-GVO -> Einwilligung von Kindern unter 16 Jahren ohne Einverständnis der Eltern = unwirksam

-> bei Einwilligungen von Kindern: Prüfung Wirksamkeit aufgrund Alter; ggf. Einsatz von Altersverifikationssystemen

5. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen („Privacy-by-Design“ und „Privacy-by-Default“) umsetzen

Die DS-GVO enthält bestimmte Rahmenbedingungen für die Art und Weise, wie die Anforderungen der DS-GVO schon bei der Prozessgestaltung und bei Voreinstellungen umzusetzen sind (Artikel 25 DS-GVO).

- *Prüfung Datenschutz durch Technik (da unzureichende TOMs nun bußgeldbewehrt)*
- *insbesondere auch Krypto-Konzept, Pseudonymisierung, Anonymisierung*
- *Notfallkonzept obligatorisch (inkl. Backup und Recovery)*
- *Prüfung, ob Privacy by design bzw. Privacy by default im Unternehmen umgesetzt sind*

6. Verträge checken

Unternehmen sollten insbesondere ihre bestehenden Verträge zur Auftrags(daten) verarbeitung überprüfen und überarbeiten. In den Artikeln 26 bis 28 DS-GVO sind Vorgaben für Vereinbarungen mit Auftrags(daten)verarbeitern und zwischen gemeinsam für die Verarbeitung Verantwortlichen geregelt.

7. Datenschutzfolgenabschätzung implementieren

Der europäische Gesetzgeber hat die bisherige Vorabkontrolle (§ 4d Abs. 5 BDSG) nicht in die DS-GVO übernommen. Sie wird abgelöst durch die Datenschutz-Folgenabschätzung (Artikel 35 DS-GVO). An eine Datenschutz-Folgenabschätzung kann sich eine verpflichtende Konsultation der zuständigen Aufsichtsbehörde anschließen (Art. 36 DS-GVO).

- *Risikoanalyse und Folgenabschätzung, ggf. frühzeitige Einbindung der Aufsicht*
- *Prüfung bisheriger Bewertungen auf Basis neuer Bedeutung z.T. bekannter Begriffe*
- *Risikoanalyse analog ISO27001 (Wahrscheinlichkeit/Schaden) nach Art. 32 /EG 83*
- *Durchführung der Datenschutz-Folgenabschätzung nach Art. 35*
- *Erstellung Checklisten: Welche Fälle relevant für die Prüfung?*

- *Wie wird die Prüfung konkret durchgeführt?*
- *Wann muss ggf. Aufsicht eingebunden werden?*
- *Output: welche Anpassungen sind erforderlich a) rechtlich und b) technisch-organisatorisch*

8. Melde– und Konsultationspflichten organisieren

Die Melde- und Konsultationspflichten gegenüber den Aufsichtsbehörden (Artikel 33, 36 und 37 DS-GVO) müssen in den internen Abläufen des Unternehmens abgebildet werden.

- *DSB ist der zuständigen Aufsichtsbehörde zu melden*
- *Meldepflicht bei Datenschutzverstößen gegenüber der Aufsichtsbehörde binnen 72 Stunden*

9. Betroffenenrechte und Informationspflichten umsetzen

Die in der DS-GVO geregelten Betroffenenrechte müssen in den unternehmensinternen Abläufen abgebildet und gegenüber den Betroffenen umgesetzt werden, etwa das Recht auf Löschung (Artikel 17) und das Recht auf Datenübertragbarkeit (Artikel 20) einschließlich der übergreifenden Rahmenbedingungen (Artikel 12) sowie die Informationspflichten des Verantwortlichen (Artikel 13, 14).

- *Etablierung Prozesse zur Wahrnehmung Rechte Betroffener binnen Frist von 1 Monat*
- *Insbesondere Löschung (inkl. Benachrichtigung Dritter)*
- *Auskunft, ggf. Portabilität Update der Einwilligungen; Einwilligungen, die neuen Standard erfüllen, bleiben wirksam (Einzelprüfung)*
- *Dokumentation von Einwilligungen; Schulung von Mitarbeitern: insbesondere Fristen bei Betroffenenrechten, Incident-Management*

10. Dokumentation organisieren

Die DS-GVO enthält an verschiedenen Stellen Dokumentationspflichten, beispielsweise in Artikel 30 (Verarbeitungsverzeichnis), Artikel 33 Abs. 5 (Dokumentation von Datenschutz vorfällen) oder Artikel 28 Abs. 3 lit. a (Dokumentation von Weisungen im Rahmen von Auftragsverarbeitungsverhältnissen).

- *Update Dokumentation und Vereinbarungen*
- *Update der heutigen Verfahrensverzeichnisse (öffentliches Verfahrensverzeichnis entfällt)*
- *Dokumentation der Datenflüsse,*
- *Zwischen verbundenen Unternehmen im EU/EWR-Raum*
- *in Drittstaaten*
- *Anpassung der ADVs an neue inhaltliche Anforderungen / Haftungsklauseln für ADV-Nehmer, z.B. eigenes VVZ (Art. 30 Abs. 2), EU-Vertretung (Art. 27)*
- *Update interner Dokumente wie BVs, Richtlinien, Policies, Arbeitsanweisungen etc.*

- *Update der Datenschutzerklärungen / Informationen an betr. Personen; Integration der Informationspflichten nach Art. 12-15, auch Piktogramme nach Art. 12 Abs. 7*
- *Prüfung konkrete Löschmaßnahmen: Feststellung Aufbewahrungspflichten, Klassifizierung, Speicherorte, Mitarbeiterinformation, Management-buy-in*

Sollten Sie Unterstützung bei der Umsetzung / Umstellung benötigen, wenden Sie sich bitte an:
ZB Datenschutz und –sicherheit GmbH & Co. KG, Edmund-Rumpler-Straße 6 A, 51149 Köln
Telefon: 02203 / 8984444, info@zb-datenschutz.de