RECHTSANWALT FACHANWALT FÜR URHEBER- UND MEDIENRECHT

Thilo Zachow FACHANWALT FÜR IT-RECHT

DATENSCHUTZBEAUFTRAGTER (TÜV)

BESTELLTER EXTERNER DATENSCHUTZBEAUFTRAGTER SEIT 2012

Nur noch 2 Monate bis zur Geltung der Datenschutz-Grundverordnung!

Ab dem 25.05.2018 ist die Datenschutzgrundverordnung (DS-GVO) sowie das neue Bundesdatenschutzgesetz durch jedes Unternehmen anzuwenden. Die Nichtbeachtung der Verpflichtungen sieht drastische Bußgelder bis 20 Mio. EUR vor.

Aufgrund meiner Erfahrung als externer Datenschutzbeauftragter und durch das Feedback aus meinen Vorträgen zur neuen Datenschutzgrundverordnung habe ich einen **10 Punkte-Plan** entwickelt. Dieser berücksichtigt die aktuellen Verlautbarungen der Aufsichtsbehörden, worauf diese bei zukünftigen Prüfungen ab dem 25.05.2018 besonders achten werden.

Gostritzer Str. 61 • 01217 Dresden

+49 (0) 351 21 06 69 70

+49 (0) 351 21 06 69 79

frage@aa13.info

www.aa13.info

1. **Vorbereitung**
   Seien Sie vorbereitet. Es ändert sich nicht nur der Name einer Datenschutzregelung. Die DS-GVO wird direkte Auswirkungen auf Ihr Unternehmen **ab dem 25.05.2018 haben**.
   Die Geschäftsleitung sollte sich daher mit
   - der verschärften Rechenschaftspflicht,
   - den Informationspflichten gegenüber Betroffenen,
   - den Rechten der Betroffenen,
   - dem Recht auf Datenportabilität des Betroffenen,
   - den technischen organisatorischen Maßnahmen,
   - der Risikofolgenabschätzung und
   - der Meldepflicht von Verstößen vertraut machen.

   Diese Vorbereitung sollte dokumentiert werden, damit die Aufsicht auf Anfrage über Ihre Aktivitäten informiert werden kann.

2. **Bestandsaufnahme**
   Um die Änderungen festzustellen, welche künftig nach der DS-GVO eintreten werden, ist eine Bestandsaufnahme hinsichtlich der Verfahren durchzuführen, bei denen personenbezogene Daten verarbeitet werden. Zuständigkeiten im Unternehmen und die Fortführungsverpflichtung sind zu regeln.
   - Kundendaten
   - Beschäftigtendaten
   - Verarbeitung von Kinderdaten
   - Auftragsdatenverarbeitung (Drittbezug)

3. **Rechtsgrundlage (Einwilligung oder gesetzliche Erlaubnis)**
   Für alle Verfahren muss auch nach der DS-GVO eine Rechtsgrundlage gegeben sein. Die Rechtsgrundlage ist zur dokumentieren. Informations- und Auskunftsverpflichtungen sind zu erfüllen (bspw. one-page-website).

Gostritzer Str. 61 • 01217 Dresden
+49 (0) 351 21 06 69 70
+49 (0) 351 21 06 69 79
frage@aa13.info
www.aa13.info

4. **Betroffenenrechte**
   Betroffene sind über die Verarbeitung ihrer Daten transparent und leicht verständlich zu informieren.
   - Kontaktdaten des Datenschutzbeauftragten oder GF
   - Zweck der Verarbeitung
   - Rechtgrundlage
   - Dauer der Verarbeitung
   - bspw. Hinweis auf Auskunft, Widerspruch, Berichtigung, Löschung, Sperrung, Herausgabe (Datenportabilität), Widerruf bei Einwilligung

5. **personenbezogene Daten von Kindern**
   Art. 8 DS-GVO. Hier ist insbesondere der Vertragsschluss als Verarbeitungszweck zu beachten (Geschäftsfähigkeit!).

6. **Verträge, Auslandsbezug (außerhalb der EU) und tatsächlicher gelebter Ablauf prüfen**
   Bestehende Verträge sind auf Auftragsdatenverarbeitungen, Funktionsübertragungen und/oder gemeinsame Verantwortlichkeit zu prüfen. Wie werden die Verträge gelebt?

7. **Datenschutzfolgeabschätzung (Risikofolgenabschätzung)**
   Die Datenschutzfolgeabschätzung ersetzt die bisherige Vorabkontrolle. Hier sind Gremien zu bilden und gegebenenfalls die Aufsicht zwingend anzuhören.

8. **Privacy by Design oder Privacy by Default (code isn´t law!)**
   - Datenschutz durch Technikgestaltung und/oder Voreinstellung (bspw. einer Softwareoption)

Gostritzer Str. 61 • 01217 Dresden
+49 (0) 351 21 06 69 70
+49 (0) 351 21 06 69 79
frage@aa13.info
www.aa13.info

9. **Meldepflicht**
   Es gibt ein Mitwirkungsgebot des Verantwortlichen (Zusammenarbeit mit der Aufsicht) nach der DS-GVO, welches sich bspw. in der kurzen Meldefrist von 72 Stunden von Datenschutzverletzungen bei der Aufsicht wiederspiegelt. Hier muss ein Management installiert sein, welches Zuständigkeiten und verschiedene Eskalationsstufen berücksichtigt.
   Ein Datenschutzbeauftragter ist der Datenschutzaufsicht zu melden.

10. **Dokumentation**
    Die vorgenannten Punkte 1.-9. sind zu dokumentieren.

Aus meiner Sicht wird es am 25.05.2018 sehr wichtig sein, die Aufsicht davon überzeugen zu können, dass die Anforderungen der DS-GVO umgesetzt wurden und werden.

Anlasslose Prüfungen durch die Aufsicht sind möglich und einfache Abfragen bspw. auch nach diesem 10-Punkte-Plan als Muster erwarte ich ab dem 25.05.2018.

Dresden, den 02.03.2018

Thilo Zachow ist Rechtsanwalt und Fachanwalt für Informationstechnologierecht, Fachanwalt für Urheber- und Medienrecht, Datenschutzbeauftragter (zertifiziert durch den TÜV-Nord) in Dresden. Er beschäftigt sich seit dem Jahr 2005 mit dem Thema Datenschutzrecht. Seit dem Jahr 2012 als externer Datenschutzbeauftragter von Unternehmen des e-commerce bestellt.

Gostritzer Str. 61 • 01217 Dresden
+49 (0) 351 21 06 69 70
+49 (0) 351 21 06 69 79
frage@aa13.info
www.aa13.info