TIPPS & TRICKS FÜR
DIE UMSETZUNG
DER DSGVO BIS
ZUM 25. MAI 2018

CHECKLISTE ZUR DSGVO

DAS SOLLTEN SIE BIS ZUM 25.05. UMGESETZT HABEN!

DEADLINE 25. MAI 2018

Auch wenn Unternehmen zwei Jahre Zeit hatten, um die neuen Maßnahmen für die DSGVO umzusetzen, haben viele das leidliche Thema auf die lange Bank geschoben.

Nur ist diese „lange Bank“, jetzt vor dem finalen Inkrafttreten der EU-DSGVO nicht mehr ganz so lang, dafür aber der auszufüllende Maßnahmen-Katalog.

Aus diesem Grund haben wir für Sie in Zusammenarbeit mit der IHK, die wichtigsten Aufgaben in dieser Checkliste zusammengefasst, die Sie definitiv bis zum 25. Mai 2018 umgesetzt haben sollten. Das soll nicht heißen, dass Sie nun die restlichen Maßnahmen vernachlässigen sollten, aber eine realistische vollständige Umsetzung ist in dieser kurzen Zeit kaum noch möglich.

Daher: Erledigen Sie alles mit Außenwirkung zuerst! Und setzten Sie sich danach einen Projekt- oder Maßnahmen-Plan auf, der alle weiteren Aufgaben mit ihren Fristen umfasst. So können Sie bei einer eventuellen Prüfung durch die Aufsichtsbehörde zumindest vorweisen, dass Sie sich dem Thema gerade annehmen.

1.

Maßnahmen mit Außenwirkung

- [x] Datenschutzbeauftragten benennen und auf der Webseite veröffentlichen (später auch an die Aufsichtsbehörde melden)
- [x] Prüfung der Datenschutzerklärung auf der Webseite (inkl. Erweiterung der Informationspflicht)
- [x] Einwilligungserklärungen bei Datenerhebung anpassen
- [x] Newsletter Prozess anpassen (Impressum verlinken, Widerspruchserklärung, Einwilligung, Kopplungsverbot, DoubleOpt-In)

TIPP:
Denken Sie auch daran eine direkte Kontaktmöglichkeit z. B. eine Datenschutz-Emailadresse oder ein Formular auf ihrer Webseite zu hinterlegen, um Ihren Datenschutzbeauftragten erreichen zu können. Diese Möglichkeit soll künftig dazu dienen Rechte wie das Auskunftsrecht oder Recht auf Löschen/ Vergessen einfacher für den Kunden zu gestalten.
Beachten Sie, dass bei diesen Anfragen eine Reaktion von Ihnen nach spätestens 30 Tagen erfolgen sollte.

TIPP:
Überprüfen Sie, welche der neuen Dokumentationspflichten Sie bereits durch interne Leitfäden/Richtlinien nur erweitern müssen. Dies kann vor allem bei dem Verfahrensverzeichnis oder den technisch & organistorischen Maßnahmen hilfreich sein. Zudem sollten Sie eine Vorlage für die Aufträge zur Datenverarbeitung erstellen. Vorlagen finden Sie dazu auch bei der Aufsichtsbehörde.

2.

Wichtige organisatorische Maßnahmen

- [x] Identifikation von Dokumentationslücken und Anforderungen aufgrund neuer Nachweispflichten
- [x] Prüfung von ADV-Verträgen mit Ihren Dienstleistern: Identifikation von Haftungsrisiken
- [x] Mitarbeiter-Schulungen zu den Neuerungen der DSGVO

3.

Meldepflichten

- Prozess der Meldung von Datenpannen innerhalb der verantwortlichen Stelle definieren
- Prozess der Meldung bei Datenpannen an die Aufsichtsbehörde
- Prozess für die Dokumentation von Datenpannen
- Prozess für die Meldung von Datenpannen an die betroffene Person

TIPP:
Datenpanne müssen nicht nur gemeldet, sondern auch immer genau dokumentiert werden. Zusätzlich muss aufgelistet werden, welche Maßnahmen Sie daraufhin ergriffen haben. Zudem sollten Sie sicherstellen, dass Sie für einen derartigen Fall eine geeignete Kommunikationsstrategie geplant haben, für den Fall, dass die Medien darauf aufmerksam werden.

TIPP:
Vor allem bei dem Recht auf Auskunft, Änderung oder Löschung sollten Sie sich einen Verifizierungsprozess überlegen, der sicherstellt, dass die Anfrage auch von der Person kommt, für die sie sich ausgibt. Bei dem Recht auf Löschung sollten Sie zudem Ihre gesetzlichen Aufbewahrungspflichten berücksichtigen. Alle Daten die Sie gesetzlich nicht speichern müssen, sollten Sie dann umgehend löschen. Hier kann es hilfreich sein, sich eine Übersicht anzulegen in welchen Systemen die Daten gespeichert bzw. verarbeitet werden.
Eine derartige Übersicht ist auch für das Verfahrensverzeichnis notwendig.

4.

Wahrung der Rechte Betroffener

- Prozess zur Auskunftserteilung
- Prozess zum Widerruf der Einwilligung
- Prozess um Daten in gängigem elektronischen Format übertragen zu können
- Prozess zur Umsetzung der Rechte auf Löschung, Sperrung, Vergessenwerden

5.

Dokumentation der Datenverarbeitungsprozesse

- ☑ Erstellung oder Aktualisierung der Verarbeitungsübersicht
- ☑ TOMs dokumentieren und Wirksamkeit prüfen (lassen)
- ☑ Einführung von Risiko(Datenschutz)-Bewertungen
- ☑ Durchführung von Datenschutzfolge-abschätzungen
- ☑ Überarbeitung vorhandener Vereinbarung zur Auftragsverarbeitung

TIPP:
Bei den technischen Maßnahmen können Sie meist mit wenigen Mitteln mit Ihrer bestehenden Lösungen optimale Bedingungen für die Anforderungen der DSGVO schaffen.
Je nach Kategorie und Sensibilität der personenbezogenen Daten, ist die Schwere der Maßnahmen für deren Schutz abzuleiten. Die Risikobewertung dient dazu, festzustellen, wie hoch das Sicherheitsniveau für jede Kategorie sein soll. Berücksichtigen Sie dabei das Risiko für den Betroffen bei Verlust oder Bekanntwerden der Daten.

TIPP:
Nicht nur gegenüber Ihren Kunden müssen Sie die Einwilligungserklärung anpassen, sondern auch gegenüber Ihren aktuellen und auch künftigen Mitarbeitern. Überprüfen Sie bestehende Verträge und Einwilligungen nach Gültigkeit und passen Sie diese gegebenenfalls an. Denken Sie dabei auch daran, die Hinweise für die private Nutzung von geschäftlichen Geräten anzupassen, wenn diese Datenströme nicht anonymisert analysiert werden.

6.

Organisatorische Maßnahmen gegenüber Ihren Mitarbeitern

- ☑ Datenschutzinformation der Mitarbeiter (Erweiterung der Informationspflichten)
- ☑ Einwilligungserklärungen von Mitarbeitern (Verschärfung der formalen Vorgaben)
- ☑ Prozess und Informationspflicht bei Datenerhebung und -verarbeitung von Bewerberdaten


bitbone