Fragebogen zur Umsetzung der EU-DSGVO bis zum 25. Mai 2018

Januar | 2018 (Sonderausgabe)

Wichtige Datenschutzinformationen für Ihr Unternehmen

WORK and PLAY COMPUTERSYSTEME

Inhaltsverzeichnis

Begrüßung | Ihr Datenschutzbeauftragter vor Ort

Liebe Leserin, lieber Leser,

am 25. Mai 2018 treten die neuen Datenschutzverordnungen und –gesetze in Kraft (EU-DSGVO & BDSG-neu), die ab diesem Zeitpunkt alle Gegebenheiten rund um den Datenschutz in Deutschland und in Europa einheitlich bestimmen.

Da der Einzug dieser vielen Neuerungen einen sehr starken Einfluss auf viele Unternehmen in Deutschland hat, gilt es aktuell nur eine Frage zu beantworten:

„Ist auch unser Unternehmen auf die am 25. Mai 2018 in Kraft tretenden Neuerungen der europäischen Datenschutz-Grundverordnung (EU-DSGVO) und dem neuen Bundesdatenschutzgesetz (BDSG-neu) optimal vorbereitet?“

Um sich diese Frage so einfach wie möglich beantworten zu können, haben wir in dieser Sonderausgabe genau dieses Thema aufgegriffen und einen „*Fragebogen zur Umsetzung der EU-DSGVO zum 25. Mai 2018*“ zusammengestellt, der auf Basis einer Vorgabe des bayerischen Landesamtes für Datenschutzaufsicht entwickelt und uns zum Zweck der Umsetzung der Datenschutzvorgaben in deutschen Unternehmen von Herrn Thomas Kranig (Präsidenten des Bayerischen Landesamtes für Datenschutzaufsicht in Bayern) zur Verfügung gestellt wurde.

Mit diesem Fragebogen sollen Sie einen Überblick erhalten, was zu tun ist, um auch ab dem 25. Mai 2018 aus Sicht des Datenschutzes mit Ihrem Unternehmen rechtssicher zu agieren.

Sollten Sie darüber hinaus weitere Informationen benötigen oder eine ausführliche Beratung in Anspruch zur Umsetzung der neuen Vorgaben nehmen wollen, stehen wir Ihnen jederzeit sehr gerne zur Verfügung.

Sie erreichen uns unter der Telefonnummer + 49 395 7782864 oder per E-Mail an datenschutz@workandplay.de

Mit besten Grüßen

Peter Schmidt
Externer Datenschutzbeauftragter (nach DIN EN ISO/IEC 17024)
Consultant für Datenschutz und Informationssicherheit

Fragebogen zur Umsetzung der EU-DSGVO zum 25. Mai 2018

I. Struktur und Verantwortlichkeit im Unternehmen

01. Gibt es das Bewusstsein im Unternehmen, dass Datenschutz Chefsache ist, beispielsweise durch
    - ✓ Vorhandensein einer Datenschutzleitlinie
    - ✓ Beschreibung der Datenschutzziele
    - ✓ Regelung der Verantwortlichkeiten
    - ✓ Bewusstsein über Datenschutzrisiken
    - ✓ Transparenz über Zielkonflikte (z.B. zwischen Marketing- und Rechtsabteilung)

02. Verfügt Ihr Unternehmen über einen betrieblichen Datenschutzbeauftragten?
    - ✓ Wenn nein, warum nicht?
    - ✓ Wenn ja, ist geklärt, wann er von wem einzubeziehen ist?
    - ✓ Wenn ja, ist er schon gem. Art. 37 Abs. 8 EU-DSGVO der zuständigen Aufsichtsbehörde gemeldet?

II. Übersicht über Verarbeitungen

01. Haben Sie ein Verzeichnis Ihrer Verarbeitungstätigkeiten gem. Art. 30 EU-DSGVO?
    - ✓ Wenn nein, warum nicht? Ist das dokumentiert?
    - ✓ Wie haben Sie sichergestellt, dass datenschutzrechtliche Belange bei Beginn oder Änderung eines jeden Prozesses in Ihrem Unternehmen Berücksichtigung finden (Privacy by Design –Art. 25 EU-DSGVO)?

III. Einbindung Externer

01. Haben Sie Externe zur Erledigung Ihrer Arbeiten (Auftragsverarbeiter) eingebunden?
    - ✓ Wenn ja, haben Sie eine Übersicht über die Auftragsverarbeiter?
    - ✓ Wenn ja, haben Sie mit allen Ihren Auftragsverarbeitern die erforderlichen Vereinbarungen mit dem Mindestinhalt nach Art. 28 Abs. 3 EU-DSGVO abgeschlossen?

IV. Transparenz, Informationspflichten und Sicherstellung der Betroffenenrechte (a)

01. Haben Sie Ihre Texte zur datenschutzrechtlichen Information der betroffenen Personen bei der Datenerhebung an die Anforderungen nach Art. 13 bzw. 14 EU-DSGVO angepasst?
    - ✓ Wenn nein, warum nicht?

02. Haben Sie insbesondere folgende Informationen neu aufgenommen, sofern nicht bereits vorher enthalten:
    - ✓ Kontaktdaten des Datenschutzbeauftragten
    - ✓ Rechtsgrundlage(n) für die Verarbeitung personenbezogener Daten
    - ✓ Falls Sie die Verarbeitung mit Ihren berechtigten Interessen oder berechtigten Interessen eines Dritten begründen: die berechtigten Interessen
    - ✓ Falls Sie Daten in Drittländer übermitteln: die von Ihnen zum Einsatz gebrachten geeigneten Garantien zum Schutz der Daten (z.B. Standarddatenschutzklauseln)
    - ✓ Dauer der Speicherung; sofern nicht möglich, die Kriterien für die Festlegung dieser Dauer
    - ✓ Bestehen der Rechte betroffener Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, auf Widerspruch aufgrund besonderer Situation einer betroffenen Person sowie auf Datenportabilität
    - ✓ Sofern Verarbeitung auf Einwilligung beruht: das Recht zum jederzeitigen Widerruf der Einwilligung
    - ✓ Recht auf Beschwerde bei der Aufsichtsbehörde
    - ✓ Ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist
    - ✓ Sofern einschlägig: die Vornahme einer automatisierten Entscheidungsfindung einschl. Profiling sowie – in diesem Fall – Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen der Verarbeitung für die betroffene Person
    - ✓ Sofern Sie die Daten nicht bei der betroffenen Person erhoben haben: aus welcher Quelle die personenbezogenen Daten stammen und ggf. ob sie aus öffentlich zugänglichen Quellen stammen
    - ✓ Haben Sie Ihre Werbe-Einwilligungserklärungen für Kunden, Interessenten usw., an die Anforderungen von Art. 7 und 13 EU-DSGVO angepasst (insbesondere: erweiterte Informationspflichten, auch zur jederzeitigen Widerrufbarkeit der Einwilligung)?

IV. Transparenz, Informationspflichten und Sicherstellung der Betroffenenrechte (b)

03. Haben Sie ein Verfahren eingerichtet, um Anträge von betroffenen Personen auf Auskunft zu den eigenen Daten nach Art. 15 EU-DSGVO zeitnah und vollständig erfüllen zu können (Art. 12 Abs. 1 EU-DSGVO)?

04. Haben Sie Verfahren eingerichtet, um Anträge auf Datenübertragbarkeit betroffener Personen erfüllen zu können (Art. 20 EU-DSGVO)?

V. Verantwortlichkeit, Umgang mit Risiken (a)

01. Gibt es für jede Verarbeitungstätigkeit Angaben, mit der Sie die Rechtmäßigkeit Ihrer Verarbeitung nachweisen können, z.B. bezüglich Zwecken, Kategorien personenbezogener Daten, Empfängern und/oder Löschfristen (Art. 5 Abs. 2 EU-DSGVO)?
    - ✓ Haben Sie geprüft, ob die Einwilligungen, auf die Sie eine Verarbeitung stützen, noch den Voraussetzungen der Art. 7 und/oder 8 EU-DSGVO entsprechen?
    - ✓ Können Sie das Vorliegen der Einwilligung nachweisen?

02. Haben Sie ein Datenschutzmanagementsystem installiert, um sicherzustellen und den Nachweis erbringen zu können, dass Ihre Verarbeitung gemäß der EU-DSGVO erfolgt (Art 24 Abs. 1 EU-DSGVO)?

03. Haben Sie Ihre bestehenden Prozesse zur Überprüfung der Sicherheit der Verarbeitung auf die neuen Anforderungen des Art. 32 EU-DSGVO angepasst?
    - ✓ Haben Sie insbesondere bestehende Checklisten zur Auswahl von technischen und organisatorischen Maßnahmen durch eine risikoorientierte Betrachtungsweise auf Basis von Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten ersetzt?
    - ✓ Wurde ein geeignetes Managementsystem zur regelmäßigen Überprüfung, Bewertung und Verbesserung der Security-Maßnahmen umgesetzt?
    - ✓ Wurden Schutzmaßnahmen wie Pseudonymisierung und der Einsatz von kryptographischen Verfahren zum Schutz vor unbefugten oder unrechtmäßigen Verarbeitungen sowohl bezüglich externer als auch interner „Angreifer“ umgesetzt?

V. Verantwortlichkeit, Umgang mit Risiken (b)

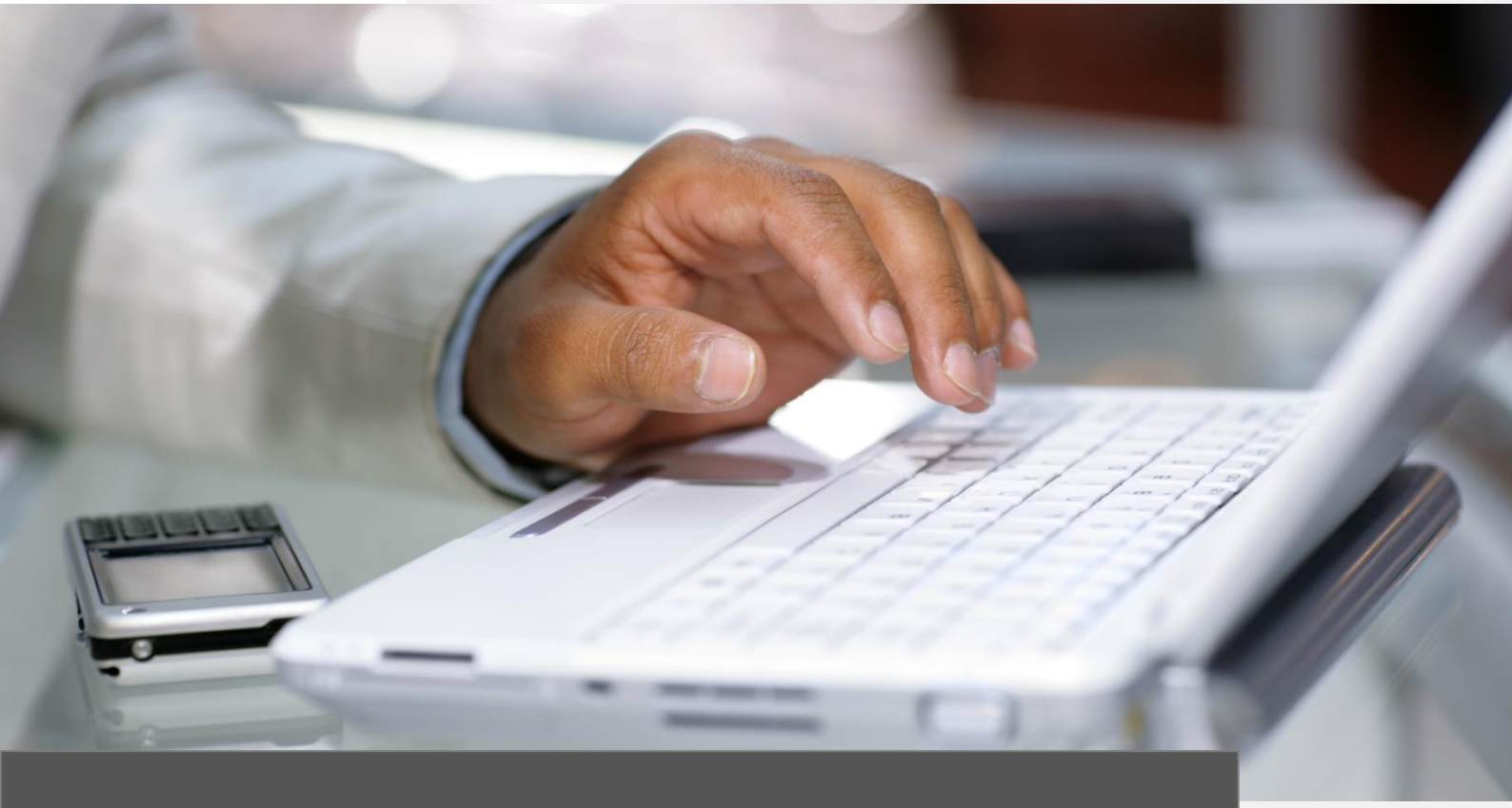
04. Haben Sie sich auf die eventuelle Notwendigkeit der Durchführung einer Datenschutz-Folgenabschätzung vorbereitet?
    - ✓ Haben Sie eine geeignete Methode zur Bestimmung der Frage, ob eine Datenschutz-Folgenabschätzung durchzuführen ist, in Ihrem Unternehmen eingeführt?
    - ✓ Haben Sie eine geeignete Risikomethode zur Durchführung einer Datenschutz-Folgenabschätzung in Ihrem Unternehmen eingeführt? Haben Sie sich für einen Prozess der Datenschutz-Folgenabschätzung entschieden; haben Sie diesen schon einmal getestet?

VI. Datenschutzverletzungen

01. Haben Sie gem. Art. 33 EU-DSGVO sichergestellt, dass die Meldung von Verletzungen des Schutzes personenbezogener Daten innerhalb von 72 Stunden an die Aufsichtsbehörde möglich ist?
    - ✓ Haben Sie insbesondere sichergestellt, dass Datenschutzverletzungen in Ihrem Unternehmen erkannt werden können. Haben Sie dazu eine geeignete Methode zur Ermittlung eines Risikos bzw. eines hohen Risikos in Ihrem Unternehmen eingeführt?
    - ✓ Haben Sie einen Prozess aufgesetzt, wie mit potentiellen Verletzungen intern umzugehen ist?
    - ✓ Haben Sie festgelegt, wer, wann und wie mit der Datenschutzaufsichtsbehörde kommuniziert?

Quelle: Der „Fragebogen zur Umsetzung der EU-DSGVO zum 25. Mai 2018“ basiert auf einer Vorlage die vom bayerischen Landesamt für Datenschutzaufsicht entwickelt und uns zum Zweck der Umsetzung der Datenschutzvorgaben in deutschen Unternehmen von Herrn Thomas Kranig (Präsidenten des Bayerischen Landesamtes für Datenschutzaufsicht in Bayern) zur Verfügung gestellt wurde.

Januar | 2018



Impressum

Work and play computersysteme
Woldegker Str. 12
17033 Neubrandenburg
Tel.: +49 395 7782864
Fax: +49 395 7783862
Web: www.workandplay.de
E-Mail: datenschutz@workandplay.de

Redaktion:
Peter Schmidt

Bildnachweise:
Diese Datenschutzbroschüre wurde in unserem Auftrag von der Firma ITKservice GmbH & Co. KG, Fuchsstädter Weg 2, 97491 Aidhausn erstellt. Alle in diesem Dokument dargestellten Bilder wurden von der ITKservice GmbH & Co. KG bei der Firma ccvision.de gekauft und lizensiert.

WORK and PLAY COMPUTERSYSTEME