

EU-Datenschutz- Grundverordnung

Trifft mich das wirklich?

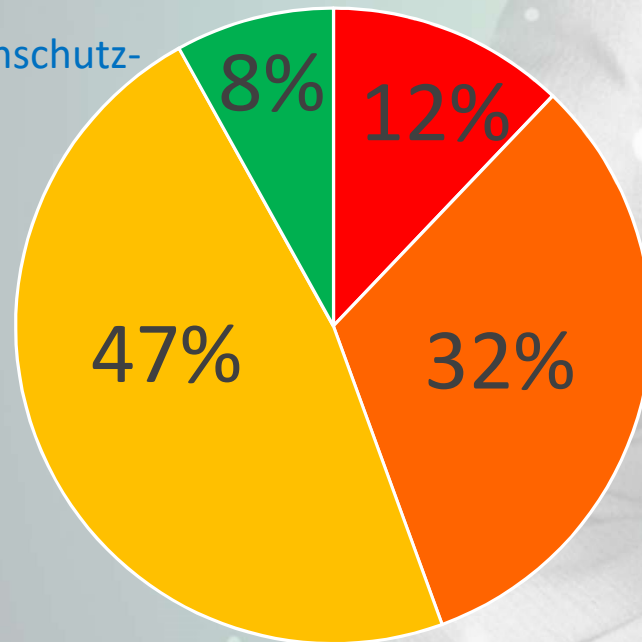


Axel Vogelsang
Datenschutzbeauftragter & IT-Consultant

KÄMMER
CONSULTING

Umfrage Bitkom

Befragte: 509 Datenschutzverantwortliche



- die DSGVO ist uns überhaupt nicht bekannt
- Haben uns noch nicht damit beschäftigt
- Beschäftigen uns aktuell damit
- erste Maßnahmen angefangen und umgesetzt

EU-Datenschutz-Grundverordnung

- Veröffentlichung im EU-Amtsblatt am 4. Mai 2016
- Anzuwenden ab dem 25. Mai 2018
 - also in 374 Tage aber
 - nach Abzug WE und Feiertage nur noch 256 Tage!
- gilt direkt für alle Unternehmen innerhalb der EU



Datenschutzanpassungs- und Umsetzungsgesetz EU (DSAnpUG-EU)

- Nachfolgegesetz zum BDSG
- Regelt Öffnungsklauseln der EU-DSGVO
- Zustimmung Bundesrat am 12.05.2017
- Tritt zum 25.05.2018 in Kraft und löst dann BDSG ab

Auswirkungen auf andere Gesetze

- Anpassungen in verschiedenen Gesetzen notwendig: TKG, TMG, UWG, SGB usw.
- Ersatz der EU-ePrivacy-Richtlinie durch EU-ePrivacy-Verordnung

Was ist neu?

- Dokumentationspflichten deutlich erweitert
- Betroffenenrechte deutlich ausgeweitet
- neue Bußgeldtatbestände und Bußgeldhöhen
- an vielen Stellen Risikoabschätzung erforderlich
- Datenschutz Folgeabschätzung ersetzt Vorabkontrolle
- Umfangreichere Pflichten für Auftragsverarbeiter

Dokumentationspflichten

- Beweislastumkehr
- kein Verfahrensverzeichnis → Bußgeldtatbestand
- Dokumentation Grundlage für weitere Pflichten
- Nachweis der Wirksamkeit von Maßnahmen

Betroffenenrechte

- deutlich umfangreichere Informationspflichten und Auskunftsrechte
- Neue Rechte:
 - Recht auf „Vergessenwerden“
 - Recht auf Datenübertragbarkeit
- Verbindliche Reaktionszeit

Betroffenenrechte - Informationspflicht

- Kontaktdaten des für die Verarbeitung Verantwortlichen
- Falls vorhanden: Datenschutzbeauftragter
- Zweck der Verarbeitung
- Rechtsgrundlage der Verarbeitung
- Ggfs. Empfänger oder Kategorien von Empfängern

Betroffenenrechte - Informationspflicht

- ggfs. Drittländer oder internationale Organisationen, an die Daten übermittelt werden, dazu
- Speicherdauer der Daten (oder die Kriterien für die Festlegung der Dauer)
- Hinweis auf Recht auf *Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruchsrecht* sowie auf *Datenübertragbarkeit*
- Bei Verarbeitung aufgrund einer Einwilligung muss auf das Recht, die Einwilligung mit Wirkung für die Zukunft widerrufen zu können, hingewiesen werden

Betroffenenrechte - Informationspflicht

- Hinweis,
 - ob die Bereitstellung der pbDaten gesetzlich oder vertraglich vorgeschrieben ist
 - oder ob die Bereitstellung für einen Vertragsabschluss erforderlich ist
 - ob die betroffene Person verpflichtet ist, die Daten bereit zu stellen
 - welche Folgen die Nichtbereitstellung hätte
 - auf das Beschwerderecht bei der Aufsichtsbehörde
- Bei automatisierten Einzelfallentscheidungen
 - Aussagekräftige Informationen über die Logik
 - Tragweite und Auswirkungen der Verarbeitung für die betroffene Person

Bußgeld

- deutlich höher
 - bis 10.000.000 € oder 2 % des weltweiten Jahresumsatzes
 - bis 20.000.000 € oder 4 % des weltweiten Jahresumsatzes
- wirksam, verhältnismäßig und abschreckend
- Neue Bußgeldtatbestände
 - Verstoß gegen Dokumentationspflichten
 - Privacy-by-Design; Privacy-by-Default

Risikoabschätzung

- bestehende Risiken identifizieren
 - Unmittelbare Risiken für Betroffene
 - Risiken für das Unternehmen
- Risiken bewerten
- Maßnahmen festlegen und umsetzen

Datenschutz Folgeabschätzung

- DSFA ist immer durchzuführen, wenn

„(...) eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten zur Folge (hat)“

Datenschutz Folgeabschätzung

- systematische Beschreibung der Verarbeitungsvorgänge und der Zwecke der Verarbeitung
- Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge
- Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen
- Zur Bewältigung der Risiken geplante Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren

Auftragsverarbeiter

- ähnliche Regelung wie BDSG
- Datenverarbeitung im Auftrag kann auch außerhalb der EU stattfinden
- schärfere Haftungsregeln für Auftragsverarbeiter
- Auftragsverarbeiter muss Verzeichnis über Verarbeitungstätigkeiten führen

Was ist zu tun?

- bestehende Einwilligungen Betroffener prüfen
- Prozess zur Wahrung der Betroffenenrechte implementieren
- Prozess zur Meldung von Datenschutzverstößen implementieren
- Dokumentation prüfen / aktualisieren
- Verzeichnisse aktualisieren

Was ist zu tun?

- Datenschutz Folgeabschätzung durchführen
- Umsetzung „Privacy-by-Design“ / „Privacy-by-Default“
- Verträge zur Auftragsdatenverarbeitung prüfen
- AGBs / Datenschutzerklärungen prüfen



EU-Datenschutz Grundverordnung

Trifft mich das wirklich?

Ja



Vielen Dank für Ihre Aufmerksamkeit

Axel Vogelsang
Datenschutzbeauftragter
Tel: 0531.702249-49
datenschutz@kaemmer-consulting.de
www.kaemmer-consulting.de

Kämmer Consulting GmbH
Nordstr. 11, 38106 Braunschweig

