Innofly Management

Checkliste Datenschutzgrundverordnung

Einführung und Neuerungen

Am 4. Mai 2016 wurde die „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung; kurz „DSGVO")" kundgemacht. Die Datenschutz-Grundverordnung ist am 25. Mai 2018 in Geltung getreten. Alle Datenverarbeitungen haben dieser Rechtslage zu entsprechen.

Wesentliche Neuerungen für Unternehmen:

- Es gibt keine Meldepflicht bei der Datenschutzbehörde (Datenverarbeitungsregister) mehr. Stattdessen stärkere Verantwortung für Verantwortliche („Auftraggeber") und Auftragsverarbeiter („Dienstleister") und weitreichende Neuregelung der Pflichten bei der Datenverarbeitung.
- (Neue) Informationspflichten und Betroffenenrechte
    - Auskunftsrecht (ua auch über geplante Speicherdauer)
    - Recht auf Berichtigung
    - Recht auf Löschung und auf „Vergessen werden"
    - Recht auf Einschränkung der Verarbeitung
    - Mitteilungspflicht bei Berichtigung, Löschung oder Einschränkung an alle Empfänger
    - Recht auf Datenübertragbarkeit
    - Widerspruchsrecht
    - Regelungen betreffend automatisierte Generierung von Einzelentscheidungen einschließlich Profiling
- Befugnisse und Aufgaben der Aufsichtsbehörden wurden erweitert
- Höhere Strafen

Analyse des Ist-Zustandes und Anpassungsbedarf

1. Welche **personenbezogenen Daten** werden verarbeitet?
2. Welche **Datenverarbeitungen** bestehen?
    - Waren Datenverarbeitungen nach der alten Rechtslage (DSG 2000) im Datenverarbeitungsregister registriert? Wenn ja, welche?
    - Wird eine Bildverarbeitung (z.B. Videoüberwachung) durchgeführt?
    - Erfolgt Profiling?
    - Gibt es bisher bereits AGB, Datenschutzerklärungen, Impressum, laufende Verträge, Website-Einstellungen, etc mit Datenschutzhinweisen?
3. Was sind die **Zwecke** meiner Datenverarbeitungen?
    - Was ist die **Rechtsgrundlage** der Datenverarbeitung? Liegt eine Einwilligung vor?
4. Welche **sensiblen Daten** (nun: besondere Kategorien personenbezogener Daten) werden verarbeitet?
5. Werden **Kindern** Dienste der Informationsgesellschaft angeboten?

6. Werden **Auftragsverarbeiter** („Dienstleister“) herangezogen?
    - Gibt es schriftliche Vereinbarungen für die Auftragsverarbeitung?
    - Weist der Auftragsverarbeiter die erforderliche Zuverlässigkeit auf?
7. Wie werden die **Informationspflichten** (nach der DSGVO) erfüllt?
8. Wie werden die **Betroffenenrechte** (nach der DSGVO) erfüllt?
9. Welche **Datensicherheitsmaßnahmen** sind bereits vorhanden?
10. Wie ist **privacy by design**/**privacy by default** implementiert? Besteht für meine Datenverarbeitungen **Dokumentationspflicht**?
11. Welche Vorkehrungen gegen **Datenschutzverletzungen** existieren schon in meinem Unternehmen?
12. Ist für meine Datenverarbeitungen eine **Datenschutz-Folgenabschätzung** durchzuführen?
    - Bewirkt der Verarbeitungsvorgang ein (potentielles) Bewerten oder Einstufen betroffener Personen (etwa das Erstellen von Profilen und Prognosen), insbesondere auf Grundlage von Aspekten, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel der Person betreffen?
    - Beinhaltet der Verarbeitungsvorgang eine automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung?
    - Beinhaltet der Verarbeitungsvorgang möglicherweise eine systematische Überwachung, d.h. Vorgänge, die die Beobachtung, Überwachung oder Kontrolle betroffener Personen zum Ziel haben?
    - Werden vertrauliche Daten oder höchst persönliche Daten verarbeitet?
    - Erfolgt eine Datenverarbeitung in großem Umfang?
        - Zahl der betroffenen Personen
        - verarbeitete Datenmenge bzw. Bandbreite der unterschiedlichen verarbeiteten Datenelemente
        - Dauer oder Dauerhaftigkeit der Datenverarbeitung
        - geografisches Ausmaß der Datenverarbeitung
    - Beinhaltet die Datenverarbeitung ein (potentielles) Abgleichen oder Zusammenführen von Datensätzen?
    - Werden möglicherweise Daten schutzbedürftiger betroffener Personen verarbeitet?
    - Beinhaltet der Verarbeitungsvorgang eine innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen?
    - Kann die Datenverarbeitung die betroffenen Personen (potentiell) an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindern?
13. Brauche ich einen **Datenschutzbeauftragten**?
14. Welcher **Datenverkehr mit dem EU-Ausland** besteht und auf welcher Rechtsgrundlage?
15. Besonderheiten **Arbeitnehmerdatenschutz**
    - Überprüfung von Dienstverträgen, Betriebsvereinbarungen, Dienstordnungen, etc
    - Rechtzeitige Kommunikation mit dem Betriebsrat