iapp

WISSENSFUNDUS FÜR DEN CIPP/E

VERSION 1.3.2

GÜLTIG AB: 02.09.2024

Europäische Datenschutz-Zertifizierung

Kurzbeschreibung des Wissensstands für Certified Information Privacy Professionals/Europe (CIPP/E™)

I. Einführung in den europäischen Datenschutz

A. Ursprünge und historischer Kontext des Datenschutzrechts

1. Grundlage für den Datenschutz
2. Menschenrechtsgesetze
3. Frühe Gesetze und Vorschriften
   a. OECD-Richtlinien und der Europarat
   b. Übereinkommen 108
4. Erfordernis eines einheitlichen europäischen Ansatzes
5. Der Vertrag von Lissabon
6. Übereinkommen 108+
7. Brexit

B. Organe der Europäischen Union

1. Europäischer Gerichtshof für Menschenrechte
2. Europäisches Parlament
3. Europäische Kommission
4. Europäischer Rat
5. Gerichtshof der Europäischen Union

C. Gesetzgeberischer Rahmen

1. Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten von 1981 (die „Konvention des Europarats")
2. Die Datenschutzrichtlinie der EU (95/46/EG)
3. Die EU-Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (2002/58/EG) (ePrivacy-Richtlinie), in der jeweils gültigen Fassung

4. Die EU-Richtlinie für E-Commerce (2000/31/EG)
5. Europäische Regelungen zur Datenaufbewahrung
6. Die Datenschutz-Grundverordnung (DSGVO) (EU) 2016/679 und verwandte Gesetzgebung
   a. Verhältnis zu anderen Gesetzen (Zahlungsdiensterichtlinie 2, Data Governance Act, Verordnung (EU) 2018/1725 EU-Datenschutzgesetz etc.)
7. NIS-Richtlinie (2016)/NIS-2-Richtlinie (2022)
8. EU-Gesetz über künstliche Intelligenz (2021)

II. Europäische Datenschutzgesetze und -vorschriften

A. Konzepte des Datenschutzes

1. Personenbezogene Daten
2. Sensible personenbezogene Daten
   a. Besondere Kategorien personenbezogener Daten
3. Pseudonyme und anonyme Daten
4. Verarbeitung
5. Verantwortlicher
6. Auftragsverarbeiter
   a. Leitlinien 07/2020 zu den Begriffen Verantwortlicher und Auftragsverarbeiter in der DSGVO
7. Betroffene Person

B. Räumlicher und sachlicher Anwendungsbereich der Datenschutz-Grundverordnung

1. Bei Niederlassung in der EU
2. Keine Niederlassung in der EU
   a. Leitlinien 3/2018 zum räumlichen Anwendungsbereich der DSGVO

C. Grundsätze der Datenverarbeitung

1. Treu und Glauben sowie Rechtmäßigkeit
2. Zweckbindung
3. Verhältnismäßigkeit
4. Richtigkeit
5. Speicherbegrenzung (Aufbewahrung)
6. Integrität und Vertraulichkeit

D. Grundlagen für die rechtmäßige Verarbeitung

1. Einwilligung
2. Vertragliche Notwendigkeit
3. Gesetzliche Verpflichtung, lebenswichtige Interessen und öffentliches Interesse
4. Berechtigte Interessen
5. Besondere Kategorien der Verarbeitung

E. Informationspflichten

1. Transparenzgrundsatz
2. Datenschutzerklärungen
3. Mehrstufige Datenschutzerklärungen

F. Betroffenenrechte

1. Zugang
   a. Leitlinien 01/2022 zu den Rechten der betroffenen Person – Recht auf Auskunft
2. Berichtigung

3. Löschung und das Recht auf Vergessenwerden
    a. Leitlinien 5/2019 zu den Kriterien für das Recht auf Vergessenwerden bei Suchmaschinen im Rahmen der DSGVO
4. Beschränkung und Widerspruch
5. Einwilligung, einschließlich des Rechts auf Widerruf
6. Automatisierte Entscheidungsfindung einschließlich Profiling
7. Datenübertragbarkeit
8. Einschränkungen
    a. Leitlinien 10/2020 zu den Beschränkungen gemäß Artikel 23 DSGVO

G. Sicherheit personenbezogener Daten

1. Geeignete technische und organisatorische Maßnahmen
    a. Schutzmechanismen (Verschlüsselung, Zugriffskontrolle usw.)
2. Meldung einer Verletzung
    a. Risikobasierte Meldepflichten
    b. Leitlinien 01/2021 zu Beispielen für die Meldung von Verletzungen des Schutzes personenbezogener Daten
    c. Leitlinien 9/2022 zur Meldung von Verletzungen des Schutzes personenbezogener Daten nach der DSGVO
3. Dienstleistermanagement
4. Weitergabe von Daten

H. Rechenschaftspflichten

1. Zuständigkeiten der Verantwortlichen und der Auftragsverarbeiter
    a. gemeinsame Verantwortliche
2. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
3. Dokumentation und Zusammenarbeit mit den Aufsichtsbehörden
4. Datenschutz-Folgenabschätzung (DSFA)
    a. festgelegte Kriterien für deren Durchführung
5. Pflicht zur Benennung von Datenschutzbeauftragten
6. Auditierung von Datenschutzprogrammen

I. Internationale Datenübermittlung

1. Begründung für Verbote
    a. Leitlinien 05/2021 über das Zusammenspiel zwischen der Anwendung von Artikel 3 und den Bestimmungen über internationale Übermittlungen gemäß Kapitel V der DSGVO
2. Länder mit Adäquanzentscheidung
3. Safe Harbor, Privacy Shield und der transatlantische Datenschutzrahmen
    a. Schrems-Entscheidungen, Auswirkungen von
4. Standardvertragsklauseln
5. Binding Corporate Rules (BCRs)
6. Verhaltensregeln und Zertifizierungen
    a. Leitlinien 04/2021 zu Verhaltensregeln als Instrument für Übermittlungen
7. Ausnahmeregelungen
    a. Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679
8. Transfer Impact Assessments (TIAs)
    a. Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten

J. Überwachung und Durchsetzung

1. Aufsichtsbehörden und ihre Befugnisse
    a. Leitlinien 8/2022 zur Bestimmung der federführenden Aufsichtsbehörde eines Verantwortlichen oder eines Verarbeiters

2. Der Europäische Datenschutzausschuss (EDSA)
3. Die Rolle des Europäischen Datenschutzbeauftragten (EDSB)

K. Folgen für Verstöße gegen die DSGVO

1. Ablauf und Verfahren
2. Verstöße und Geldbußen
3. Sammelklagen
4. Entschädigung betroffener Personen

III. Einhaltung der europäischen Datenschutzrechte und -vorschriften

A. Beschäftigungsverhältnis

1. Rechtliche Grundlage für die Verarbeitung von Mitarbeiterdaten
2. Speicherung von Personalunterlagen
3. Überwachung am Arbeitsplatz und Vermeidung von Datenverlusten
4. EU-Betriebsräte
5. Whistleblowing-Systeme
6. Programme zur Nutzung Ihres eigenen Geräts (Bring Your Own Device, BYOD)
7. Risiken im Zusammenhang mit Mitarbeiterdaten (z. B. über soziale Medien und KI-Systeme)

B. Überwachungsaktivitäten

1. Überwachung durch öffentliche Stellen
2. Kommunikationsüberwachung
3. Videoüberwachung
   a. Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte
4. Geolokalisierung
5. Biometrik/Gesichtserkennung
   a. Leitlinien 05/2022 für den Einsatz der Gesichtserkennungstechnologie in der Strafverfolgung

C. Direktmarketing

1. Telemarketing
2. Direktmarketing
3. Verhaltensorientierte Internetwerbung
   a. Leitlinien 8/2020 über die gezielte Ansprache von Nutzer:innen sozialer Medien

D. Internettechnologie und Kommunikation

1. Cloud-Computing
2. Cookies
3. Suchmaschinenmarketing
4. Social-Media-Plattformen
   a. Dark Patterns
      i. Leitlinien 3/2022 zu dunklen Mustern in den Schnittstellen sozialer Medienplattformen
5. Künstliche Intelligenz (KI)
   a. maschinelles Lernen
   b. ethische Fragen