BADISCHE TREUHAND GESELLSCHAFT

1967 - 2017 50 JAHRE

manager magazin
Deutschlands beste Wirtschaftsprüfer 2018
Challenger
★★★★☆
www.manager-magazin.de

Digitalisierung im Rechnungswesen und der Steuerberatung

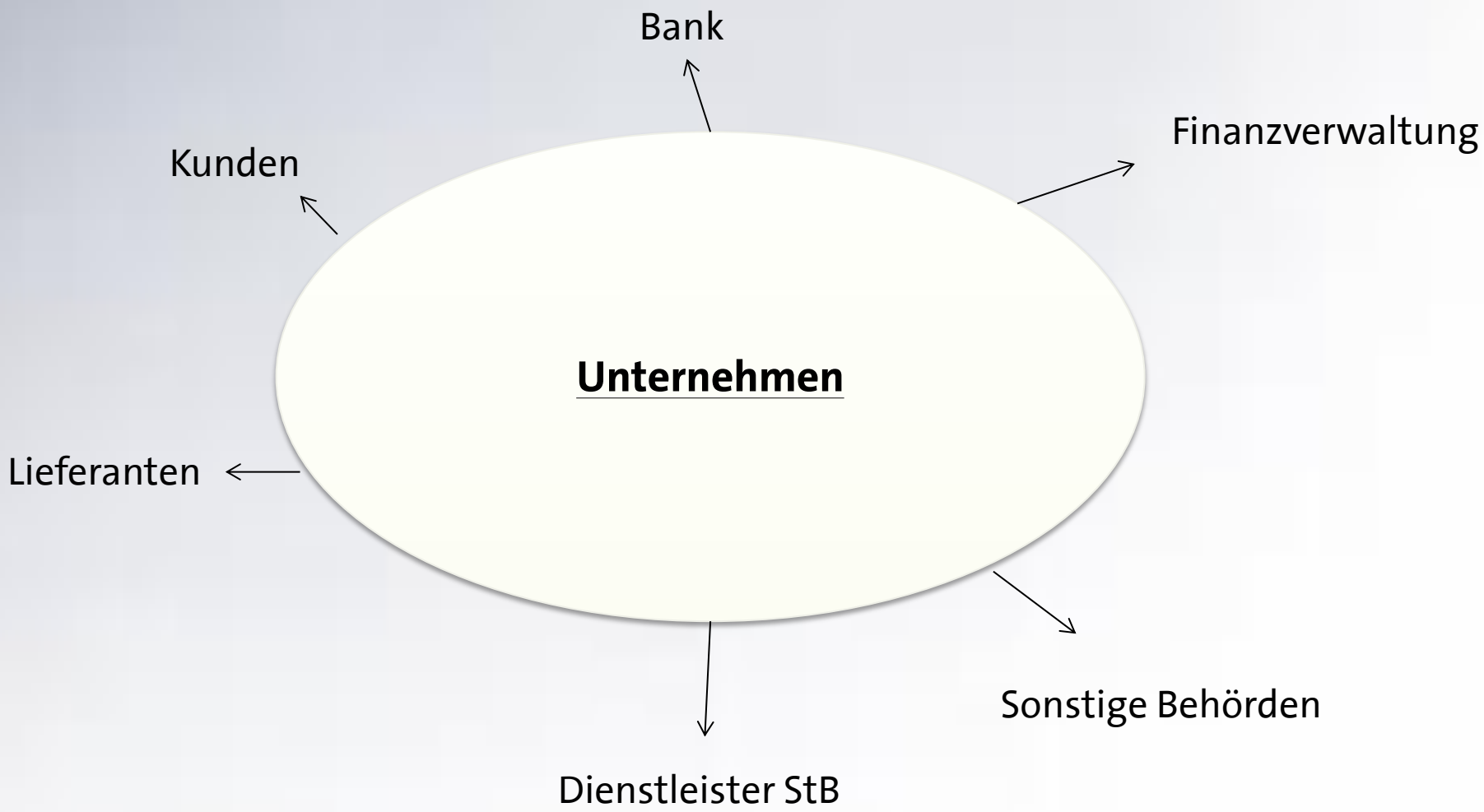
Badische Treuhand GmbH
Wirtschaftsprüfungsgesellschaft
Steuerberatungsgesellschaft
Lahr/Schwarzwald

Referent: WP/StB Thomas J. Adam

Binäres Zahlensystem als Grundlage der elektronischen Datenverarbeitung

Gottfried Wilhelm Leibnitz 1646 bis 1716

Vernetzte Unternehmen



Begriffe Digitalisierung

1. Big Data
2. Cloud Computing
3. Archivierung
4. Industrie 4.0
5. Blockchain

Digitale Projekte in Rechnungswesen

Aktuelle Prioritäten		Zukünftige Prioritäten
1.	Homogenität der Systeme	2
2.	Management der Datenqualität	3
3.	Papierlose Buchhaltung	1
4.	Integriertes Konsolidierungssystem	7
5.	Schaffung von Transparenz	6
6.	Prozessautomatisierung	5
7.	Big Data-Analysen	8
8.	Realtime-Reporting	9
9.	Schnittstelle zu externen Systemen	4
10.	Tools zur Visualisierung	10
11.	Cloud Computing	11

Papierlose Buchhaltung

- Eingangsrechnungen
- Ausgangsrechnungen
- Kassenbelege
- Bankbelege

Vorteile der Digitalisierung und einer papierlosen Buchhaltung

- Zeit, Personal und Kostenersparnis durch die digitale Verfügbarkeit

- Einsparungen bei
  - Papier
  - Ordner
  - Toner
  - Drucker
  - Lagerräume

- Suchzeiten entfallen

Nachteile der Digitalisierung

- Umstellungsaufwand
- Sicherheitsanforderungen
- Zusätzliche Software, Rechner- und Speicherkapazitäten

Tax Compliance Einhaltung von steuerlichen Regelungen

A. Archivierung

GoBD Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff

1. Elektronische Archivierung ist technologieneutral
   → keine Vorgaben für das Archivsystem
2. Zeitnahe Archivierung
   → Belege in Papierform und elektronischer Form möglichst unmittelbar nach Eingang
3. Unveränderbarkeit
   → hardwareseitig durch unveränderbare Datenträger
   → softwareseitig durch z.B. Festschreibung, Sichern, Historisierung
4. Indizierung
   → Sicherstellung, dass das elektronische Dokument unter dem zugeteilten Index verwaltet und registriert werden kann

Elektronische Archivierung und GoBD

5. Lesbarkeit und Auswertbarkeit

6. Auch steuerlich aufbewahrungspflichtige Daten dürfen archiviert werden

7. Elektronische archivierte Objekte unterliegen der Betriebsprüfung

8. Einsichtnahme der BP direkt am Bildschirm

9. Archivierung auch im Ausland möglich

10. Archivierungsverfahren ist in einer Verfahrensdokumentation zu beschreiben

⇨ Papierdokumente können vernichtet werden, wenn eine ordnungsgemäße elektronische Archivierung nebst Verfahrensdokumentation sichergestellt ist und gesetzliche (außerordentliche) Gründe nicht dagegen sprechen

B. Anforderungen an die Kasse

1. Gefahr der Schätzung in Betriebsprüfungen
   - Kassensturzfähigkeit

2. Anforderungen ab 01.01.2017

   steuerlich relevante Daten
   - unveränderbar
   - vollständig
   in einem auswertbaren Datenformat

Steuerlich relevante Daten: Journal-, Auswertungs-, Programmier- und Stammdatenänderungsdaten sowie Protokolle über die Einsatzzeiträume und –orte der Kasse

Elektronische Archivierung und GoBD

3. Anforderungen ab 2020
   § 146a AO – verwendete elektronische Aufzeichnungssysteme müssen zertifiziert sein

4. Offene Ladenkasse
   ⇨ keine Pflicht zur Führung einer elektronischen Registrierkasse

Der gläserne Steuerbürger

- Elster — Programm elektronischer Steuererklärungen der Finanzverwaltung
- EHUG — Gesetz über elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister
- BEA — Bescheinigungen elektronisch annehmen
- E-Bilanz — Elektronische Übermittlung einer Bilanz an das Finanzamt
- ELSTAM — Elektronische Steuerabzugsmerkmale

Der gläserne Steuerbürger

Behörde	übermittelte Daten an das Finanzamt
Gemeldete Einnahmen	
Rentenversicherungsanstalt	Rentenbezugsmitteilung
z.B. Bundesagentur für Arbeit oder Krankenkassen	Lohnersatzleistungen (z.B. Arbeitslosengeld)
(ehem.) Arbeitgeber	elektronische Lohnsteuerbescheinigung
Elterngeldstellen	Elterngeld
Banken + Fondgesellschaften	alle steuerfrei gutgeschriebene Kapitalerträge
Berufliche Versorgungswerke	Rentenbezugsmitteilung
Krankenversicherungen	Bezug von Kranken- und Mutterschaftsgeld

Der gläserne Steuerbürger

Behörde	übermittelte Daten an das Finanzamt
Lebensversicherungen	steuerschädliche Verwendung, wie - Abtretung (Sicherheitsgestellung) - vorzeitige Auszahlung - steuerschädliche Vertragsänderungen
Landratsamt	Kontrollmitteilungen über bei der Wohngeldstelle bezuschusste Mieten (Sozialhilfe)
Zuständige Behörde	Riester-Rente zur Überprüfung der steuerlichen Förderung

Der gläserne Steuerbürger

Behörde	übermittelte Daten an das Finanzamt
Gemeldete Ausgaben	
Krankenkasse	Beiträge zur Kranken- und Pflegeversicherung, Zusatzbeiträge, Erstattungen, etc.
Arbeitgeber	Beiträge zur Kranken- und Pflegeversicherung, Rentenbeitrag
Gesetzliche Rentenversicherung	Kranken- und Pflegeversicherungsbeiträge

Sofortige Auswertungsmöglichkeit der E-Bilanz

- Mehrjahresvergleich innerhalb der Gesellschaft
- Materialquoten
- Personalquoten
- Analyse der sonstigen betrieblichen Aufwendungen
- Externe Unternehmensvergleiche

Nutzen und Gefahren im Internet

- WhatsApp
- WLAN
- Hacker-Angriffe

www.allianz-fuer-cybersicherheit.de
www.aktionsbund.de
www.initiative-it-websicherheit.de

Nutzen und Gefahren im Internet

Zuviel digitale Nähe führt zu analoger Entfremdung

Vielen Dank für Ihre Aufmerksamkeit!

Beschäftigtendatenschutz in der Personalpraxis

Veranstaltung am 26.04.2018

Dr. Thomas Daum
Rechtsanwalt

Hinweis

Diese Präsentation ersetzt keine einzelfallbezogene Rechtsberatung und erhebt keinen Anspruch auf Vollständigkeit. Bitte wenden Sie sich für Fragen an den Referenten bei Schrade & Partner.

Die Präsentation berücksichtigt den Stand von Gesetzgebung und Rechtsprechung am 30.04.2018.

Allgemeines

Datenschutzrechtliche Grundsätze

- Das Datenschutzrecht schützt die Grundrechte natürlicher Personen bei der Verarbeitung der ihnen zugeordneten Daten.

- Begriffe

  - Personenbezogene Daten

    Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Abs. 1 DSGVO).

  - Verarbeitung

    Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten (Art. 4 Abs. 2 DSGVO).

Datenschutzrechtliche Grundsätze

- Beispiele für die Verarbeitung:
  - Speichern
  - Anpassen oder Verändern
  - Auslesen
  - Abfragen
  - Verwenden
  - Offenlegung durch Übermittlung, Verbreitung oder Bereitstellung
  - Abgleich oder Verknüpfung
  - Löschen oder Vernichten

- Nahezu jeder denkbare Vorgang wird also vom Begriff des „Verarbeitens“ erfasst.

Gesetzliche Regelwerke

- Bundesdatenschutzgesetz (seit 01.01.1978 in Kraft)

- Grundrecht auf informationelle Selbstbestimmung

  „Beschränkungen bedürfen einer gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht.“

  BverfG „Volkszählungsurteil“ vom 15.12.1985, Az.: 1 BvR 484/83

- Es folgten zahlreiche Anpassungen des BDSG bis hin zum Umsetzungsgesetz EU vom 30.06.2017. Ständige Versuche eines Beschäftigtendatenschutzgesetzes scheiterten.

- Jetzt: Europäische Datenschutzgrundverordnung und (endlich) BDSG-2018!

Die EU-DSGVO

- Inkrafttreten: 25.05.2018
- Bisher: BDSG & EU-Datenschutzrichtlinie (RL 95/46/EG)
- Zeitgleich: Inkrafttreten des Datenschutz-Anpassungs- und Umsetzungsgesetzes (DSAnpUG) in Deutschland
- Ergänzung durch EU-e-Privacy-Verordnung (für Internet- und Telemediendienste)
- DSGVO geht dem nationalen Regelungen vor – BDSG hat Auffangfunktion
  - Beachte stets: BDSG-2018

Anwendungsbereich

- Sachlich:

  Ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder werden sollen.

  (Ausnahmen: Art. 2 Abs. 2 DSGVO)

  – Personenbezogene Daten: Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen

- Räumlich: Marktortprinzip!

  Es genügt, wenn sich die Angebote des Unternehmens an EU-Bürger wenden, gleichgültig, wo das Unternehmen seinen Sitz hat.

  Beachte: Auch Beobachtung des Surfverhaltens im Internet (Cookies) hiervon erfasst.

Wesentliche Neuerungen

- Marktortprinzip
- Höherer Prozess- und Dokumentationsaufwand
- Stark erhöhte Bußgelder
- Vereinheitlichung des Datenschutzrechts in der EU
- Änderungen bei den Anforderungen an Erlaubnisnormen und Einwilligungserklärungen
- Neue Gestaltungsmöglichkeiten gegenüber Auftragsdatenverarbeitern
- Einführung neuer Betroffenenrechte (Information, Widerspruch, Auskunft, Löschung etc.)
- Behördliche Aufsicht

Wann ist die Verarbeitung personenbezogener Daten erlaubt?

- Verbot mit Erlaubnisvorbehalt

- Erlaubnistatbestände Art. 6 Abs. 1 DSGVO
  - Einwilligung der betroffenen Person
  - Erforderlich für Zwecke des Beschäftigungsverhältnisses
  - Erforderlich für Vertragserfüllung
  - Erfüllung einer rechtlichen Verpflichtung
  - Schutz lebenswichtiger Interessen
  - Wahrnehmung der Aufgabe im öffentlichen Interesse / Ausübung öffentlicher Gewalt
  - Wahrung berechtigter Interessen

Wann ist die Verarbeitung personenbezogener Daten erlaubt?

- Einwilligung gem. Art. 6 Abs. 1 lit. a, 7 DSGVO
  - Hohe Bedeutung in der Rechtspraxis!
  - Begriffsdefinition in Art. 4 Nr. 11 DSGVO
  - Wirksamkeitsanforderungen gem. Art. 7 DSGVO:
    - zeitlich vorhergehend
    - freiwillig
    - informiert (Person des Verantwortlichen, Zweck der Verarbeitung, Hinweis auf Widerrufsrecht, verständliche und leicht zugängliche Sprache)
    - Einwilligungsfähigkeit (Einwilligung ab dem 16. Lj. möglich)
  - stets „Opt-in“ erforderlich

Wann ist die Verarbeitung personenbezogener Daten erlaubt?

- Erforderlich für die Begründung oder Durchführung eines Beschäftigungsverhältnisses (§ 26 Absatz 1 BDSG-2018)

- Erforderlich für Vertragserfüllung
  - Der Austausch von Leistungen und Gütern ist ohne einen parallelen Austausch von Informationen und Daten schlicht nicht möglich.

- Wahrung berechtigter Interessen
  - Zentrale Interessenabwägungsklausel der DSGVO

Wesentliche Neuerungen im Beschäftigtendatenschutz

- Grundsätzlich gilt, dass das deutsche Datenschutzrecht „Pate“ für die DSGVO war. D.h., dass auf nationaler Ebene die Auswirkungen im Beschäftigtendatenschutz aufgrund des bereits zuvor weitgehenden Schutzes des BDSG eher gering – aber dennoch dringend zu beachten – sind.

- Öffnungsklausel für Beschäftigtendatenschutz in Art. 88 DSGVO

- BDSG-2018 regelt in § 26 den wesentlichen Kern des Beschäftigtendatenschutzes
  - Ggü. der DSGVO ist § 26 BDSG-2018 vorrangig, solange die Vorschrift spezifischere Regelungen enthält. I.Ü. bleibt die DSGVO anwendbar.

Wesentliche Neuerungen im Beschäftigtendatenschutz

- Der Begriff „Beschäftigte“
  - Entspricht der bisherigen Definition gem. § 3 Nr. 11 BDSG
  - § 26 Abs. 8 BDSG-2018
  - Neu im Vergleich zu § 3 Nr. 11 BDSG: Leiharbeitnehmer ausdrücklich in den Kreis der Beschäftigten i.S.d. BDSG mit aufgenommen

- Personenbezogene Daten
  - § 26 Abs. 3 BDSG-2018
  - Sensible Daten mit aufgenommen

Beschäftigtendaten in der Praxis

- Anforderungen an eine wirksame Einwilligung im Arbeitsverhältnis
  - Beachte: Auch Kollektivvereinbarung als Einwilligung möglich
    - Betriebsvereinbarungen (siehe unten)
  - Schriftform wählen
  - Zeitlich VOR der Veröffentlichung einholen
  - Aufklärung über konkreten Verwendungszweck
  - Freiwilligkeit
    - Besondere Problematik im Arbeitsverhältnis
      - Über- und Unterordnungsverhältnis zwischen ArbG und ArbN
      - § 26 Abs. 2 S. 2 BDSG-2018
        - „gleichgelagerte Interessen“
      - Sanktionslose Verweigerung muss möglich sein
      - Hinweis auf jederzeitiges Widerrufsrecht

Beschäftigtendaten in der Praxis

- Auswirkungen im Bewerbungsverfahren
  - Wirksame Einwilligung?
  - Fragerecht
  - „Active Sourcing“
  - Aufbewahrung von Bewerbungsunterlagen/Talentpools
    - Ohne Einwilligung längstens fünf Monate

- Auswirkungen im bestehenden Arbeitsverhältnis
  - Interne Talentpools/Beurteilungsdaten

Beschäftigtendaten in der Praxis

- Veröffentlichung auf der Homepage
  - Ermächtigungsvorschrift: § 26 Abs. 1 S. 1 BDSG-2018
  - Unterscheidung von Funktionsträgern (keine Einwilligung für die Veröffentlichung von „Basisdokumentationsdaten“ erforderlich) und Nichtfunktionsträgern
    - Funktionsträger: Kundenbetreuer, Geschäftsführer etc.
    - Nichtfunktionsträger: Schreibkraft, Pförtner etc.

- Verwendung von Mitarbeiterfotos
  - Persönlichkeitsrechte des Arbeitnehmers (§ 22 S. 1 KUG)
    - Einwilligung erforderlich – sonst Persönlichkeitsrechte verletzt
  - Urheberrechte des Fotografen (§ § 15 ff. UrhG)
    - Zur Vermeidung von Abmahnungen: Nutzungserlaubnis einholen

Beschäftigtendaten in der Praxis

- Mitarbeiterdaten nach Beendigung des ArbV
  - Einwilligung beschränkt auf Zeitraum des Beschäftigungsverhältnisses
  - Ausnahme: Veröffentlichung als solche ist Teil des ArbV (z.B.: Model)
  - Bei Widerruf der Einwilligung durch ArbN: Sofortige Löschung der Daten!
  - Ende des ArbV ohne Widerruf:
    - Löschung der Daten (Foto) im Mitarbeiterprofil auf der Homepage
    - Problem: Bilder abseits des persönlichen Mitarbeiterprofils
      - Illustrierender Charakter
      - Persönlicher Charakter

  - Löschungspflicht im Impressum nach Ausscheiden, sonst drohen kostspielige Entfernungs- und Unterlassungsansprüche
  - Beachte: Löschungspflicht gilt auch auf allen Social-Media-Kanälen

Beschäftigtendaten in der Praxis

- Löschung des E-Mail-Accounts?
  - Hauptproblem: Erlaubte Privatnutzung
  - Rspr.: Die Löschung hat so lange zu unterbleiben, bis hinreichend geklärt ist, ob der ArbN an einer Nutzung der Datenbestände seines Accounts kein Interesse mehr hat.
    - Ansonsten droht Schadensersatzpflicht!
  - Praxistipp:
    - Klausel in Nutzungsbedingungen aufnehmen, dass der ArbN vor Beendigung seines ArbV eine Sicherung seiner privaten E-Mail-Datenbestände eigenständig vorzunehmen hat.

Beschäftigtendaten in der Praxis

- Veröffentlichung von Beschäftigtendaten
  - Umfang prüfen
  - Einwilligungen überprüfen bei Nichtfunktionsträgern
  - Ggf. neue Einwilligungserklärungen einholen

- Verwendung von Mitarbeiterfotos nur mit Einwilligung
  - Prüfen, ob urheberrechtliche Befugnisse bestehen
  - Einwilligungen überprüfen
  - Ggf. Nutzungsrechte des Fotografen einholen
    - Wenn kein Nutzungsrecht:
      - Fotos von Homepage entfernen: Abmahngefahr!

Beschäftigtendaten in der Praxis

- Betriebsvereinbarungen
  - Art. 88 Abs. 1 DSGVO i.V.m. Erwägungsgrund 155 nennt BV
  - Daten können verwendet werden für Einstellung, Durchführung, Beendigung der Arbeitsverhältnisse
  - Anforderungen an die BV:
    - geeignete Maßnahmen zum Schutz der ArbN im Hinblick auf
      - Transparenz der Datenverarbeitung
      - Datenübermittlungen innerhalb der Unternehmensgruppe
      - Überwachungssysteme am Arbeitsplatz
    - Weitere zweckmäßige Regelungen (Hinweis, dass BV Erlaubnis nach DSGVO sein soll, Verfahren bei Datenverletzung, Vorbehalt des Rückgriffs auf gesetzliche Erlaubnistatbestände etc.)

Praxistipp

- Überarbeiten Sie Ihre Einwilligungserklärungen
- Überprüfen Sie Ihre bestehenden BVs auf DSGVO-Anforderungen!
- Überarbeiten Sie BVs, die nicht den neuen Anforderungen entsprechen!
- Schließen Sie neue BVs zum Thema Datenschutz und DSGVO-Compliance ab!

Übermittlung von Daten innerhalb des Konzerns und an Drittstaaten

- Es gibt auch weiterhin kein so genanntes Konzernprivileg.

- Die DSGVO hält für international tätige Unternehmen die gleichen Rechtsinstrumente zur Datenübermittlung wie bisher galten bereit.
  - Einwilligung
  - Vertrag
  - Standardvertragsklauseln
  - Binding Corporate Rules
  - Zertifizierung
  - Codes of Conduct

Übermittlung von Daten innerhalb des Konzerns und an Drittstaaten

- Beachte: Seit Juli 2016 gilt das EU-US Privacy-Shield-Abkommen, nachdem der EuGH das Safe-Harbour abkommen als unzureichend „kassiert“ hat.

- US-amerikanische Unternehmen können sich dazu verpflichten, die Datenschutzgrundsätze in dem neuen Instrument einzuhalten, damit eine Datenübermittlung aus deutschen Unternehmen erfolgen darf.

- Grund war hierfür ein angemessenes Datenschutzniveau zu gewährleisten.

- Es bestehen jedoch Zweifel an der Rechtmäßigkeit. Kritisiert wird von der eingesetzten Art. 29-Datenschutzgruppe in ihrer Stellungnahme, dass Bedenken bestehen hinsichtlich der Zugriffsmöglichkeit durch die U.S. amerikanischen Behörden auf Datentransfers aus der EU (Stichwort: PRISM – Edward Snowden). Ob das Privacy-Shield einer rechtlichen Überprüfung durch den EuGH standhält, ist zweifelhaft. Bis zu einer gerichtlichen Entscheidung sollten sich Unternehmen jedoch nach den Vorgaben richten.

Compliance und die DSGVO

- Bei der Durchführung von Compliance-Maßnahmen und internen Ermittlungen sowie bei der Vorbereitung und Durchführung bestimmter arbeitsrechtlicher Maßnahmen verarbeiten ArbG notwendigerweise Beschäftigtendaten.
  - Schutz der DSGVO zugunsten der ArbN beachten
  - Dokumentationspflichten! Die vollständige Rechtmäßigkeit von Compliance-Kontrollen muss nachgewiesen werden können.
  - Bei Verstoß droht die Unwirksamkeit von Compliance-Kündigungen.

Überwachungsmaßnahmen

- Bisherige Rspr.:

  „Eine verdeckte Videoüberwachung kann zulässig sein, wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers besteht, weniger einschneidende Mittel zur Aufklärung des Verdachts ergebnislos ausgeschöpft sind, die verdeckte Videoüberwachung damit das praktisch einzig verbleibende Mittel darstellt und sie insgesamt nicht unverhältnismäßig ist.“

  BAG Urteil vom 20.10.2016, Az.: 2 AZR 395/15

- Nach Inkrafttreten der DSGVO:

  Auch die DSGVO nennt in Art. 6 Abs. 1 lit. f das Prinzip der Interessenabwägung. **Aber**: Die restriktive Rspr. des EuGH deutet auf sehr viel strengere Anforderungen an die Zulässigkeit verdeckter Videoüberwachung hin.

Überwachungsmaßnahmen

- Praxistipp:
  - Lückenlose (schriftliche) Dokumentation!
    - Erkenntnis eines konkreten Verdachts einer Straftat oder schweren Verfehlung
    - Ergebnislose Durchführung weniger einschneidender Maßnahmen (z.B. Mitarbeitergespräche)
    - Darstellung, dass andere (mildere) Maßnahmen nicht verfügbar sind
  - Aufmerksam sein hinsichtlich gerichtlicher Entscheidungen (insbesondere BAG)

Praxistipp

- In der Praxis sind Betriebsvereinbarungen zu Compliance-Kontrollen das wohl probateste Mittel, um im Betrieb Rechtssicherheit, Transparenz und Vorhersehbarkeit zu schaffen.
- Mit einer gut formulierten Betriebsvereinbarung können datenschutzrechtliche Risiken, die bei Compliance-Kontrollen und internen Ermittlungen stets bestehen, reduziert werden.
- Compliance-Ermittlungen nur in äußersten Ausnahmefällen auf Einwilligungen der betroffenen Personen stützen.
- In Compliance-Sachverhalten sind Einwilligungen der Beschäftigten meist nicht freiwillig.
- Arbeitgeber und Beschäftigte verfolgen keine gleichgelagerten Interessen.
- Auch sind interne Ermittlungen für den Beschäftigten nicht lediglich vorteilhaft.

Mitbestimmungsrechte des Betriebsrats

- Sehr weitreichende Mitbestimmungsrechte im Zusammenhang mit der Verarbeitung von Beschäftigtendaten.

- § 75 Abs. 2 Satz 1 BetrVG verpflichtet Arbeitgeber und Betriebsrat, die freie Entfaltung der Persönlichkeit der im Betrieb Beschäftigten zu schützen und zu fördern.

- Da das Recht auf informationelle Selbstbestimmung Teil des allgemeinen Persönlichkeitsrechts ist, gilt dies auch für die Verarbeitung von Beschäftigtendaten im Betrieb.

Mitbestimmungsrechte des Betriebsrats

- Erstellung von Personalfragebögen
  - § 94 Abs. 1 BetrVG
  - Recht des Betriebsrates, die Erhebung mitzugestalten
  - Pflicht, die geforderte Information vor allem auf die für das konkrete Arbeitsverhältnis objektiv wirklich notwendigen Daten zu beschränken
  - Der Mitbestimmung des Betriebsrates unterliegen darüber hinaus auch persönliche Angaben der Beschäftigten in Formulararbeitsverträgen (§ 94 Abs. 2 BetrVG).

Mitbestimmungsrechte des Betriebsrats

- Aufstellung allgemeiner Beurteilungsgrundsätze
  - § 94 Abs. 2 BetrVG
  - Kein Initiativrecht!
  - Regelungen, welche eine Bewertung des Verhaltens oder der Leistung der Arbeitnehmer verobjektivieren und nach einheitlichen Kriterien ausrichten sollen.
  - Bspe.:
    - Durchführung von psychologischen Tests
    - Assessment-Centern
    - Ärztliche Untersuchungen
    - Verwendung von Beurteilungsformularen

Mitbestimmungsrechte des Betriebsrats

- Auswahlrichtlinien
  - § 95 Abs. 1 BetrVG
  - Auch Richtlinien über die personelle Auswahl bei Einstellungen, Versetzungen, Umgruppierungen und Kündigungen bedürfen der Zustimmung des Betriebsrates.
  - Die Aufstellung solcher Auswahlrichtlinien beeinflusst zwangsläufig die Erhebung und Nutzung von Beschäftigtendaten.
  - Initiativrecht erst ab 500 Mitarbeitern (§ 95 Abs. 2 BetrVG)

Mitbestimmungsrechte des Betriebsrats

- Überwachung von Mitarbeitern
  - § 87 Abs. 1 Nr. 6 BetrVG
  - Dient dem Schutz der Arbeitnehmer vor den besonderen Gefahren, die mit einer Überwachung ihrer Arbeitsleistung durch technische Einrichtungen des Arbeitgebers verbunden sein können.
  - Regelung ist im Wege der betrieblichen Zwangsschlichtung (Einigungsstelle) durchsetzbar (§ 87 Abs. 2 i.V.m. § 76 BetrVG).
  - Erfasst sind ausschließlich Überwachungsmaßnahmen durch technische Einrichtungen. Überwachung des Arbeitnehmerverhaltens durch Personen (Detektive, Vorgesetzte oder Testkunden) können aber unter § 87 Abs. 1 Nr. 1 BetrVG fallen.

Mitbestimmungsrechte des Betriebsrats

- Überwachung von Mitarbeitern
  - Tatbestand wird weit gefasst.
    - Arbeitszeiterfassungssysteme
    - Videoüberwachung
    - Bildschirmarbeitsplätze
    - Biometrische Zugangskontrolle (Fingerprint-Scanner)
    - Erfassung der Telefondaten
    - Personalinformationssysteme
  - Die bloße Absicht, die Verarbeitung zu automatisieren, reicht für ein erzwingbares Mitbestimmungsrecht des Betriebsrates nach § 87 Abs. 1 Nr. 6 BetrVG aus.

Vielen Dank für Ihre Aufmerksamkeit

DR. Thomas Daum
RECHTSANWALT

Hegau-Tower
Maggistraße 5
78224 Singen
Telefon: +49/7731/59145-500
Telefax: +49/7731/59145-510
thomas.daum@schrade-partner.de
www.schrade-partner.de

Kundendatenschutz
Veranstaltung am 26.04.2018

Christof Brößke
Rechtsanwalt

Hinweis

Diese Präsentation ersetzt keine einzelfallbezogene Rechtsberatung und erhebt keinen Anspruch auf Vollständigkeit. Bitte wenden Sie sich für Fragen an den Referenten bei Schrade & Partner.

Die Präsentation berücksichtigt den Stand von Gesetzgebung und Rechtsprechung am 30.04.2018.

Übersicht
Kundendatenschutz

Kundendaten als personenbezogene Daten

- Eine besondere Regelung für den Kundendatenschutz gibt es nicht, es gelten die allgemeinen Regeln
- Datenschutz nach DSGVO gilt für „personenbezogene Daten“, d.h. alle Informationen, die sich auf eine identifizierte oder identifizierbare **natürliche Person** beziehen (Art. 4 Abs. 1 DSGVO)
- Kunden können natürliche Personen sein (Verbraucher - B2C Kunden) in diesem Fall unterliegen die gesamten Daten dem Datenschutz
- Für juristische Personen und Personengesellschaften etc., auch im Hinblick auf deren Firmennamen und sonstigen Daten (B2B Kunden), gilt der Datenschutz grundsätzlich nicht, auch wenn der Namen Eigennamen enthält (anders eventuell bei Einmann-GmbH oder dem Einzelkaufmann)

Kundendaten als personenbezogene Daten

- Personenbezogene Daten von Geschäftsführern, sonstigen Organen und Mitarbeitern von juristischen Personen unterfallen dem Datenschutz. Dies gilt z.B. in der Regel für den Namen, die Funktionsbezeichnung, die Telefondurchwahl, die persönliche E-Mail-Adresse etc. des jeweiligen Ansprechpartners, auch wenn der Kunde selbst eine juristische Person ist.
- Beim Privatkunden unterliegt demgemäß der gesamte Datensatz dem Datenschutz nach der DSGVO und bei Kunden, bei denen es sich um juristische Personen handelt, unterliegen nur die personenbezogenen Daten von Geschäftsführern, Organen, Mitarbeitern etc. dem Datenschutz nach der DSGVO.

Wann ist die Erhebung/Verarbeitung von personenbezogenen Kundendaten erlaubt?

Grundregel für personenbezogene Daten:

- Verbot mit Erlaubnisvorbehalt
- **Vor** jeder Erhebung/Verarbeitung von Kundendaten mit Personenbezug sollten die entsprechenden Erlaubnistatbestände geklärt sein.
- Für Kundendaten sind folgende Erlaubnistatbestände gemäß Art. 6 Abs. 1 DSGVO relevant:
  - die Vertragserfüllung Art. 6 Abs. 1 lit. b) DSGVO
  - das berechtigte Interesse Art. 6 Abs. 1 lit. f) DSGVO
  - die Einwilligung Art. 6 Abs. 1 lit. a) DSGVO
- Es können auch verschiedene Erlaubnistatbestände gleichzeitig für eine Datenverarbeitung gegeben sein
- Besonderheiten gelten bei Einwilligungen von Kindern unter 16 Jahren, bei der Einwilligung zur Zusendung von Werbung und im Hinblick auf Einwilligung beim Einsatz von Telemedien (Einwilligungen die z.B. auf Internet-Seiten erklärt werden)

Wann ist die Erhebung/Verarbeitung von personenbezogenen Kundendaten erlaubt?

Erlaubnistatbestand **Vertragserfüllung** Art. 6 Abs. 1 lit. b) DSGVO:

- Verarbeitung zur Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen
- Erforderlichkeit der Daten; d.h. die Datenerhebung muss zu den Vertragszwecken erforderlich sein (z. B. Basisdaten und wesentliche Eckpunkte des Vertrages). Daten, die für die Erfüllung der Haupt- und Nebenpflichten aus dem Vertrag sowie zu dessen Abschluss, Änderung und Abwicklung erforderlich sind.
- Unmittelbarer Zusammenhang zwischen dem Vertragszweck und der Datenerhebung bzw. -verarbeitung muss nach vernünftiger Würdigung gegeben sein.
- Bei Vertragsanbahnung können alle Daten, die für ein individualisiertes Angebot erforderlich sind, erhoben werden.

Wann ist die Erhebung/Verarbeitung von personenbezogenen Kundendaten erlaubt?

Erlaubnistatbestand **Vertragserfüllung** Art. 6 Abs. 1 lit. b) DSGVO:

- Was ist vom ursprünglichen Zweck umfasst und was ist Verarbeitung für einen Sekundärzweck, Art. 6 Abs. 4 DSGVO?
- Ist die Weitergabe der Daten an ein Inkassobüro oder einen Rechtsanwalt zur Einziehung der Forderung aus einem Kaufvertrag nach Art. 6 Abs. 1 lit. b) DSGVO erlaubte Verarbeitung?

  Die Weitergabe von Daten ist gem. Art. 4 Nr. 2 DSGVO auch Verarbeitung. Zur Durchführung bzw. Abwicklung eines Vertragsverhältnisses gehört auch noch die Einziehung von Forderungen, damit ist die Weitergabe vom Erlaubnistatbestand abgedeckt.

Wann ist die Erhebung/Verarbeitung von personenbezogenen Kundendaten erlaubt?

Erlaubnistatbestand **Berechtigtes Interesse** Art. 6 Abs. 1 lit. f) DSGVO:

- Es ist abzuwägen, zwischen den berechtigten Interessen des Verantwortlichen oder eines Dritten an der Verarbeitung der personenbezogenen Daten und den Interessen der betroffenen Person am Schutz der Daten. Dies ist ein Erlaubnistatbestand, da die Ergebnisse der Interessenabwägung teilweise schwer vorhersehbar sind und Rechtsprechung insoweit noch nicht besteht.
- Prüfung in drei Stufen
  - Berechtigte Interessen des Verantwortlichen oder eines Dritten
  - Erforderlichkeit der Datenverarbeitung, Wahrung der berechtigten Interessen
  - Interessen oder Grundrechte und Grundverhalten des Betroffenen, die den Schutz personenbezogener Daten erfordern, überwiegen (insb. bei Kindern).

Wann ist die Erhebung/Verarbeitung von personenbezogenen Kundendaten erlaubt?

Erlaubnistatbestand **Berechtigtes Interesse** Art. 6 Abs. 1 lit. f) DSGVO:

- Als berechtigte Interessen werden in den Erwägungsgründen genannt:
  - Vorliegen einer Kundenbeziehung oder eines Dienstverhältnisses mit dem Verantwortlichen
  - Verarbeitung für die Verhinderung von Betrug unbedingt erforderlich
  - Verarbeitung erfolgt zum Zwecke der Direktwerbung
  - Verarbeitung besteht in der Übermittlung von Daten innerhalb einer Unternehmensgruppe für interne Verwaltungszwecke, einschl. der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten (**Vorsicht!** Insoweit sind die weiteren Rechtsgrundsätze zu beachten!)
  - Verarbeitung für die Gewährleistung der Netz- und Informationssicherheit erforderlich

Wann ist die Erhebung/Verarbeitung von personenbezogenen Kundendaten erlaubt?

Erlaubnistatbestand **Berechtigtes Interesse** Art. 6 Abs. 1 lit. f) DSGVO:

- Bei der Interessenabwägung sind die vernünftigen Erwartungen der betroffenen Person zu berücksichtigen
- Nach allgemeiner Meinung ist die Direktwerbung gegenüber Kunden bei bestehendem Vertragsverhältnis ohne ausdrückliche Zustimmung nach diesem Erlaubnistatbestand zulässig; jedoch z. B. nicht eine Weiterveräußerung von Adressdaten etc.
- Es gilt das Zitat Roßnagel/Hornung, MMR 2018, 197: *„Auch die von der Verordnung nicht adressierten Herausforderungen moderner Datenverarbeitungs-technologien wie Ubiquitous Computing, Big Data, Künstliche Intelligenz und viele weitere sollen mit diesem Erlaubnistatbestand gesteuert werden. Es ist offensichtlich, dass man dem Tatbestand von Art. 6 Abs. 1 1. Unterabs. lit. f DSGVO im Wege der Auslegung so gut wie keine Antworten zur grds. Zulässigkeit und zu den Anforderungen an diese Datenverarbeitungen entnehmen kann, sondern nur im Wege der Dezision. Es bedarf also einer Entscheidung durch Selbstregulierung, Aufsichtsbehörden oder Gerichte. Der europäische Gesetzgeber vertraut hier offensichtlich weithin in die Konkretisierungsleistung des Europäischen Datenschutzausschusses.“*

Wann ist die Erhebung/Verarbeitung von personenbezogenen Kundendaten erlaubt?

Erlaubnistatbestand Einwilligung Art. 6 Abs. 1 lit. a) DSGVO:

Hier gelten die gleichen Grundsätze wie beim Beschäftigtendatenschutz. Nochmal zur Erinnerung:

- Einwilligung gem. Art. 6 Abs. 1 lit. a, 7 DSGVO:
  - Hohe Bedeutung in der Rechtspraxis!
  - Begriffsdefinition in Art. 4 Nr. 11 DSGVO
  - Wirksamkeitsanforderungen gem. Art. 7 DSGVO
    - zeitlich vorhergehend
    - freiwillig
    - informiert (Person des Verantwortlichen, Zweck der Verarbeitung, Hinweis auf Widerrufsrecht, verständliche und leicht zugängliche Sprache)
    - Einwilligungsfähigkeit (Einwilligung ab dem 16. Lj. möglich)
  - stets „Opt-in“ erforderlich

Wann ist die Erhebung/Verarbeitung von personenbezogenen Kundendaten erlaubt?

Grundsatz der Zweckbindung/Zweckänderung:

- Die Einhaltung der **Zweckbindung**, d. h. dass die Daten nur zu dem Zweck verarbeitet werden dürfen, für den die Erhebung erfolgte und für den ein Erlaubnistatbestand festgestellt wurde, ist stets zu beachten. Dies sollte sich aus dem Kontext bzw. der Speicherung im System (z.B. Abonnentenverwaltungssystem o. ä.) ergeben. Aus diesem Grundsatz ergibt sich auch die Verpflichtung, die Daten, die zu unterschiedlichen Zwecken erhoben wurden, zu trennen.
- Art. 6 Abs. 4 DSGVO enthält eine Regelung zur **Zweckänderung** (auch bezeichnet als „Weiterverarbeitung“). Die Bedeutung der Regelung ist umstritten, ein Teil der Literatur sieht in Art. 6 Abs. 4 DSGVO einen eigenen Erlaubnistatbestand, wenn der neue und der ursprüngliche Zweck miteinander vereinbar (kompatibel) ist. Andere Autoren legen die Regelung enger aus.

Wann ist die Erhebung/Verarbeitung von personenbezogenen Kundendaten erlaubt?

Weitergabe von Kundendaten:

- Die Weitergabe von Daten an Dritte ist, wenn keine Auftragsdatenverarbeitung vorliegt, ein Fall der Bearbeitung und kann nur dann erfolgen, wenn ein Erlaubnistatbestand gegeben ist. Es kommen ebenfalls die vorgenannten Erlaubnistatbestände in Betracht, wenn z.B. die Weitergabe von Adressdaten an einen Spediteur im Rahmen eines Liefervertrages von dem Erlaubnistatbestand zur Vertragserfüllung (Art. 6 Abs. 1 S. 1 lit. b) DSGVO) abgedeckt ist.

Direktwerbung/Newsletter (elektronisch):

- Nach überwiegender Meinung ist die Versendung von Direktwerbung/Newslettern etc. an Kunden oder Personen, mit denen Geschäftskontakt besteht, für die Waren und Dienstleistungen, für die ein Vertragsabschluss erfolgt ist, ohne Einwilligung zulässig; § 7 Abs. 3 UWG ist zu beachten. Ein Widerruf des Empfängers ist jederzeit möglich. Für alle darüber hinausgehenden Werbungen/Newslettern etc. ist die ausdrückliche Einwilligung erforderlich.

Rechte der Betroffenen

Informations- und Auskunftsrechte

- Art. 13, 14, 15 DSGVO: Über die Erhebung personenbezogener Daten muss der Verantwortliche die betroffene Person informieren
- Die Information muss leicht verständlich und leicht zugänglich sein
- Inhalte (u.a.):
  - Name und Kontaktdaten des Verantwortlichen
  - Kontaktdaten des Datenschutzbeauftragten
  - Zweck der Verarbeitung / Rechtsgrundlage
  - ggf. Empfänger der Daten, Absicht der Drittlandsübermittlung
  - Dauer der Speicherung
  - Rechte des Betroffenen auf Auskunft, Berichtigung und Löschung
  - Hinweis auf Widerspruchsrecht
  - Beschwerderecht bei Aufsichtsbehörde

Informations- und Auskunftsrechte

- Der Betroffene kann jederzeit Auskunft verlangen
  - Wo stammen die Daten her?
  - An wen werden sie übermittelt?
  - Zu welchen Zwecken werden die Daten verarbeitet?
  - Wird daraus ein Profiling erstellt?
  - Wie lange werden sie gespeichert?

Praxistipp

- Passen Sie Datenschutzerklärungen entsprechend an!
- Führen Sie standardisierte Verfahren zur Erfüllung der Informations- und Auskunftspflichten ein!
- Überprüfen Sie den Umfang und die Durchführung bestehender Verarbeitungen!

Recht auf Löschung

- Art. 17 DSGVO, § 20 Abs. 2, § 35 Abs. 2 BDSG
- Anspruch bei
  - Zweckfortfall
  - Widerruf der Einwilligung
  - Widerspruch gegen die Verarbeitung (öffentliches oder berechtigtes Interesse)
  - Rechtswidrigkeit der Verarbeitung
  - Personenbezogene Daten von Minderjährigen

Recht auf Löschung

- Rechtsfolge: Unverzügliche Löschung
  - Weder der Verantwortliche noch ein Dritter sollen auf die vorhandenen Daten zugreifen und diese auslesen oder verarbeiten können.
  - Unverzüglich bedeutet i.S.v. § 121 BGB „ohne schuldhaftes Zögern“.

- Auch: Recht auf Vergessenwerden
  - Diese Löschungspflicht besteht, wenn der Verantwortliche die personenbezogenen Daten öffentlich gemacht hat und zur Löschung verpflichtet ist.
  - Recht des Betroffenen, die Löschung von Querverweisen zu verlangen

Widerspruchsrecht

- Widerspruchsrecht gem. Art. 21 DSGVO
  - Nach Art. 21 DSGVO besteht ein Widerspruchsrecht insb. wenn
    - die Verarbeitung der personenbezogenen Daten der betroffenen Personen auf dem Erlaubnistatbestand gem. Art. 6 Abs. 1 lit. f) DSGVO beruht; es sei denn, der Verantwortliche kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessenrechte und Freiheiten der betroffenen Personen überwiegen oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen
    - personenbezogene Daten verarbeitet werden, um die Direktwerbung zu betreiben; in diesem Fall besteht ein jederzeitiges Widerspruchsrecht für derartige Werbung, dies gilt auch für evtl. Profiling, soweit es mit der Direktwerbung in Verbindung steht. Bei einem Widerspruch erfolgt die Verarbeitung für Zwecke der Direktwerbung nicht mehr. Es besteht die Verpflichtung der ersten Kommunikation, ausdrücklich auf diese Rechte hinzuweisen.

Verbot automatisierter Entscheidungen

- Grundsätzliches Verbot automatisierter Entscheidungen
  - Art. 22 DSGVO formuliert ein grds. Verbot automatisierter Entscheidungen, soweit diese Entscheidungen rechtliche Wirkungen gegenüber den Betroffenen entfaltet oder die Betroffenen in ähnlicher Weise beeinträchtigt. Dieses Verbot gilt jedoch nicht, soweit die Entscheidung für Abschluss oder Erfüllung eines Vertrages zwischen den betroffenen Personen und dem Verantwortlichen erforderlich ist oder aufgrund bestimmter, näher beschriebener Rechtsvorschriften zulässig ist, oder die Entscheidung mit ausdrücklicher Einwilligung der betroffenen Person erfolgt. Auch bei zulässigen automatisierten Entscheidungen können die Interessen des Betroffenen gewahrt werden, d. h. der Betroffene muss seinen eigenen Standpunkt darlegen können und es muss die Möglichkeit eines Eingreifens einer natürlichen Person auf Seiten des Verantwortlichen gegeben sein.

Anforderungen an die Unternehmen

Pflichten der verantwortlichen Stelle

- Die Unternehmen müssen Verfahren und geeignete Maßnahmen zur Einhaltung ihrer datenschutzrechtlichen Verpflichtungen einführen und die Befolgung dieser Pflichten nachweisen! Art. 24 Abs. 1 DSGVO

- Maßnahmen:
  - I.d.R. Datenschutzrichtlinien/Datenschutzhandbuch mit Verfahrenshinweisen, z. B. bei Verletzungen des Datenschutzes etc.
  - Dokumentation von Datenverarbeitungsvorgängen (Verarbeitungsverzeichnis)
  - Risikoanalysen / Datenschutz-Folgenabschätzung
  - Durchführung von Audits
  - DSGVO-Compliance durch Standardprozesse sicherstellen

Verarbeitungsverzeichnis

- Eine der wesentlichen Dokumentationen ist das in Art. 30 DSGVO geregelte sog. „Verarbeitungsverzeichnis“. Dies gilt für Verantwortliche und Auftragsdatenverarbeiter. Die Verpflichtung besteht nicht für Unternehmen, die weniger als 250 Mitarbeiter beschäftigen, es sei denn, die vorgenommene Verarbeitung birgt ein Risiko für die Rechte und die Freiheiten der betroffenen Personen, die Verarbeitung erfolgt nicht nur gelegentlich oder es erfolgt eine Verarbeitung besonderer Datenkategorien gem. Art. 9 Abs. 1 oder Art. 10 DSGVO.

  Der Umfang der Ausnahme ist umstritten. Die h. M. geht davon aus, dass regelmäßige oder dauerhafte Standardverfahren im Unternehmen, wie z. B. Personalbuchhaltung/Personalakten, Finanzbuchhaltung, Kundendatenbank zu einer Ausnahme führen, sondern es bei der Verpflichtung ein Verfahrensverzeichnis zu führen verbleibt.

  Zu erfassen sind alle Verarbeitungstätigkeiten, z. B. Videoüberwachung, E-Mail und Telefonanlage, Kundendatenbank und Zeiterfassung, Personaldatenverarbeitung, Lohnbuchhaltung etc.

Verarbeitungsverzeichnis

- Mindestinhalte sind:
  - Namen und Kontaktdaten des Verantwortlichen (einschl. etwaiger Datenschutzbeauftragte
  - Zwecke der Verarbeitung
  - Kategorien der betroffenen Personen und Kategorien der herangezogenen Daten
  - Kategorien von Empfängern, von denen Daten offengelegt werden
  - Gegebenenfalls Übermittlung in ein Drittland
  - Wenn möglich, vorgesehene Fristen für Löschung verschiedener Datenkategorien
  - Wenn möglich, allgemeine Beschreibung der technischen und organisatorischen Maßnahmen.
- Das Verzeichnis ist schriftlich zu führen, was aber elektronisch erfolgen kann
- Auf Anfrage ist das Verzeichnis der Aufsichtsbehörde zur Verfügung zu stellen.

Technische und organisatorische Maßnahmen (TOM)

- Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen
- Art. 25 DSGVO – Der Begriff wird in § 9 BDSG definiert
- Art. 25 Abs. 1 DSGVO: Datenschutz „by Design“
  - Abwägung von Stand der Technik mit Kosten und Risiko mit Eintrittswahrscheinlichkeit
  - Entsprechende geeignete Maßnahmen treffen, die der Verordnung und den betroffenen Personen gerecht werden
- Art. 25 Abs. 2 DSGVO: Datenschutz „by Default“
  - Durch Voreinstellungen im technischen Verfahren soll das Prinzip der Erforderlichkeit umgesetzt werden

Auftragsdatenverarbeitung

- Erlaubnis nach Art. 28, 29 DSGVO
- Erhebung, Verarbeitung, Nutzung personenbezogener Daten durch einen Auftragsverarbeiter gem. den Weisungen des Verantwortlichen aufgrund schriftlichen Vertrages.
  - Bsp.: externes Rechenzentrum, externer Rechnungssteller
- Hinreichende Garantien für eine ordnungsgemäße Datenverarbeitung
- Neu: Auch der Auftragsverarbeiter muss zukünftig ein Verzeichnis der Verarbeitungstätigkeiten führen.
  - Dokumentation und Übersicht aller Verfahren, bei denen personenbezogene Daten verarbeitet werden.

Melde- und Informationspflichten

- Art. 33 DSGVO
- Alle Verletzungen des Schutzes personenbezogener Daten müssen binnen 72 Stunden der Aufsichtsbehörde gemeldet werden, es sei denn, dass Risiko für persönliche Rechte und Freiheiten ist unwahrscheinlich.
- Beachte: Um überprüfen zu können, ob der Verantwortliche seiner Meldepflicht nachgekommen ist, verpflichtet ihn Art. 33 Abs. 5 DSGVO zu einer umfassenden Dokumentation etwaiger Verletzungen des Schutzes personenbezogener Daten, auf welche die Aufsichtsbehörde im Nachhinein zugreifen kann.

Datenschutzbeauftragter

- Art. 37 DSGVO und § 38 DSAnpUG
- Die Regelung des DSAnpUG geht über die Anforderungen der DSGVO hinaus (Öffnungsklausel in Art. 37 IV DSGVO).
- Bestellpflicht, sofern in der Regel mindestens zehn Personen mit der automatisierten Verarbeitung von personenbezogenen Daten beschäftigt sind.
- Entsprechende berufliche und fachliche Qualifikation ist erforderlich.
  - Vertiefte Kenntnisse im Datenschutz
  - Hohe Kommunikationsfähigkeit
  - Kein Interessenkonflikt
- Betriebsintern oder extern? Beachte besonderen Kündigungsschutz!
- Evtl. Konzerndatenschutzbeauftragter

Datenschutzbeauftragter

- Aufgaben:
  - Unterrichtung und Beratung des Verantwortlichen / der Beschäftigten
  - Überwachung der Einhaltung der rechtlichen Regelungen
    - DSB als Compliance Manager
  - Beratung im Zusammenhang mit DSFA und Überwachung
  - Zusammenarbeit mit der Aufsichtsbehörde

Datenschutzbeauftragter

- Schutz und Haftung:
  - Schutz
    - DSB darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt oder abberufen werden
    - Aber nach wie vor Kündigungsschutz durch BDSG
  - Haftung
    - Bei der zivilrechtlichen Haftung des DSB keine Änderungen, da nicht „Verantwortlicher“ iSd § 82 ABS. 2 DSGVO
    - Wegen Ausweitung des Pflichtenkreises (“Compliance Manager“) wohl aber ausgeweitete ordnungsrechtliche und strafrechtliche Verantwortung

Bußgelder und Sanktionen

- Drastische Erhöhung der Bußgelder!
  - Geldbuße bis EUR 20 Mio. oder
  - 4% des weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres
  - Verhängung der Geldbußen soll „wirksam, verhältnismäßig und abschreckend“ sein
- Detaillierte Ermessensgründe für die Bemessung
- Sanktionen auch gegen Auftragsdatenverarbeiter
- Datenschutzmanagement rückt in den Fokus

Schadensersatzansprüche

- Verstoß gegen DSGVO kann Schadensersatzansprüche auslösen
  - Materielle und immaterielle Schäden
    - Voraussichtlich Anstieg der Schadenssummen bei Nichtvermögensschäden
      - Europäische Angleichung
      - Abschreckungswirkung
  - Beweislaständerungen
    - Nutzung des Informationsrechts
    - Rechenschaftsprinzip (Art. 5 Absatz 2 DSGVO)
  - Vermeidung der Inanspruchnahme durch Dokumentation der Umsetzung der DSGVO

Was muss überprüft werden?

- Dokumentation der Datenverarbeitungsprozesse
- Datenschutzerklärungen
- Einwilligungserklärungen
- Anpassung der Betriebsvereinbarungen
- Prozesse zur Umsetzung von Widersprüchen
- Vereinbarungen zur Auftragsdatenverarbeitung
- Prozess bei Datenpannen überarbeiten
- Durchführung von zielgruppengerechten Schulungen
- Festlegung geeigneter TOM
- Monitoring nationaler Gesetzgebung / Fortbildung

Welche Abteilungen betrifft es?

- Geschäftsleitung
- Recht und Compliance
- IT-Security
- Finanzen
- Forschung und Entwicklung
- Personalabteilung und Betriebsrat

Vielen Dank für Ihre Aufmerksamkeit

Christof Brößke
RECHTSANWALT

Max-Planck-Straße 11
78052 Villingen-Schwenningen
Telefon: +49/7721/20626-405
Telefax: +49/7721/20626-100
christof.broesske@schrade-partner.de
www.schrade-partner.de