PSP
MÜNCHEN

Datenschutz-Compliance: Die neue Datenschutz-Grundverordnung

Haftungsrisiken vermeiden und Sicherheit gewinnen

Datenschutz und Compliance

Compliance ist die **Einhaltung der gesetzlichen Bestimmungen und unternehmensinternen Richtlinien** (DCGK)

- **Klassische Compliance-Gebiete:**
  - Kartellrecht
  - Kapitalmarktrecht
  - Arbeitsrecht
  - Steuerrecht

und **Datenschutzrecht?**

Compliance-Druck und die bisherige Kontrolldichte (1)

- **Bisheriges Bußgeldrisiko im Datenschutzrecht**:

  Bis TEUR 300, Überschreitung zur Abschöpfung des rechtswidrig erlangten wirtschaftlichen Vorteils möglich

- **Größere Fälle (> EUR 1 Mio. Bußgeld)**
  - 2008: Lidl (35 Vertriebsgesellschaften): 1,5 Mio.
  - 2009: Deutsche Bahn: 1,12 Mio.
  - 2014: Debeka-Krankenversicherung: 1,3 Mio.

PSP MÜNCHEN

Compliance-Druck und die bisherige Kontrolldichte (2)

- **Kleinere Fälle (1)** - www.lda.bayern.de/media/pm2015_11.pdf
  - **Behörde:** Bayerisches Landesamt für Datenschutzaufsicht (BayLDA)
  - **Höhe:** Fünfstelliger Betrag
  - **Vorwurf:**
    - Unzureichende schriftliche Aufträge mit mehreren Auftragsdatenverarbeitern:

      Keine konkreten technisch-organisatorischen Maßnahmen zum Schutz der Daten (z. B. gegen Auslesen oder Kopieren durch Unbefugte, gegen Verfälschung oder sonstige unberechtigte Abänderung oder gegen zufällige Zerstörung)
- **Kleinere Fälle (2)** – www.heise.de/ix/meldung/E-Mail-Fehlbedienung-zieht-Bussgeld-wegen-Datenschutzverstosses-nach-sich-1902442.html
  - **Behörde:** Bayerisches Landesamt für Datenschutzaufsicht (BayLDA)
  - **Höhe:** Unbekannt
  - **Vorwurf:**

    Versand eines kompletten E-Mail-Verteilers (fast zehn Druckseiten) an zahlreiche Adressaten, gefolgt von einer kurzen Auskunft

PSP MÜNCHEN

*

Compliance-Druck und die bisherige Kontrolldichte (3) – aus der Praxis des sächsischen Datenschutzbeauftragten

Bereits im März 2012 erreichte mich eine eher banale Eingabe zu einer unzulässigen werblichen Ansprache durch einen Internethändler. Zu diesem Zeitpunkt ahnte ich noch nicht, dass sich dieser Fall zu dem bisher langwierigsten Aufsichtsfall meiner Behörde entwickeln würde und dass ich in diesem fast das gesamte mir zur Verfügung stehende aufsichtsrechtliche Instrumentarium zur Anwendung bringen würde. Der eigentliche Sachverhalt konnte recht schnell geklärt und Anfang Mai 2012 mit der Feststellung eines diesbezüglichen Datenschutzverstoßes abgeschlossen werden. Der Kunde hatte über den Amazon-Marketplace einen Artikel des betreffenden Händlers erworben; anschließend war ihm von diesem Händler entgegen den Amazon-Teilnahmebedingungen und auch noch nach gemäß § 28 Abs. 4 BDSG erhobenem Widerspruch postalische Werbung zugesandt worden. Die Krux bei der Sache war aber die, dass ich mich entschlossen hatte, diese Eingabe im Rahmen einer örtlichen Kontrolle des Händlers zu bearbeiten. Bei dieser örtlichen Kontrolle habe ich eine ganze Reihe weiterer datenschutzrechtlicher Mängel feststellen müssen, u. a.

- die unterlassene Bestellung eines Datenschutzbeauftragten,
- die nicht erfolgte Verpflichtung auf das Datengeheimnis,
- fehlende Auftragsdatenverarbeitungsverträge mit mehreren Dienstleistern,
- keine Unterrichtung über das Widerspruchsrecht in den Werbesendungen,
- werbliche Kundenansprache entgegen der eigenen Datenschutzerklärung,
- ungesicherte Weitergabe von Kundendaten an die Dienstleister.

PSP MÜNCHEN

*

Compliance-Druck und die bisherige Kontrolldichte (4) – aus der Praxis des sächsischen Datenschutzbeauftragten

Im Weiteren gestaltete sich die Kommunikation mit der verantwortlichen Stelle sehr schwierig und auch zeitaufwändig. Auskunftsaufforderungen wurde nur selten rechtzeitig, oft erst nach Erlass eines Heranziehungsbescheides und Festsetzung eines Zwangsgeldes, nachgekommen und auch inhaltlich hinterließ die Geschäftsführung nicht den Eindruck, dass sie verstanden hatte, worum es beim Datenschutz im Allgemeinen wie auch bei den festgestellten Datenschutzmängeln, insbesondere der Auftragsdatenverarbeitung, im Speziellen eigentlich ging. So waren beispielsweise meine an den Händler als verantwortliche Stelle gerichteten Aufforderungen zum Abschluss rechtskonformer Auftragsdatenverarbeitungsverträge durch die Geschäftsführung einfach als zusätzliche Bedingung aller zukünftig zu erteilenden Aufträge an die Dienstleister weitergereicht worden. Die Geschäftsführung hatte also schlichtweg lange nicht begriffen oder nicht begreifen wollen, dass sie als verantwortliche Stelle selbst in der Pflicht ist, die gesetzlichen Vorgaben des § 11 BDSG umzusetzen. Leider bewirkte auch die nachgeholte Bestellung eines betrieblichen Datenschutzbeauftragten wegen der diesbezüglichen Dominanz der Geschäftsführung hier nur sehr wenig.

Alles in allem habe ich diese Angelegenheit aber schließlich nach

- zwei örtlichen Kontrollen,
- vier Heranziehungsbescheiden,
- fünf Zwangsgeldfestsetzungen,
- einer Anordnung und
- sieben Bußgeldbescheiden

und daraus resultierend Zahlungseingängen in Höhe von **insgesamt mehr als 70.000 €** nach mehr als vier Jahren im April 2016 doch noch erfolgreich, d. h. mit der Feststellung, dass alle von mir zu Beginn des Aufsichtsvorgangs festgestellten Datenschutzmängel durch die verantwortliche Stelle abgestellt worden sind, abschließen können.

(Quelle: https://www.saechsdsb.de/images/stories/sdb_inhalt/noeb/taetigkeitsberichte/8-TB-Endfassung-Version-5.pdf)

PSP MÜNCHEN

Wären es nach der EU-DSGVO 4,62 Mio. EUR gewesen (66 x 70 TEUR)?

*

Compliance-Druck und die bisherige Kontrolldichte (5)

- **Paradigmenwechsel durch EU-DSGVO (ab Mai 2018)!**

  Bußgeldrisiko: höherer Betrag aus

  (a) EUR 20 Mio. (vorher 300 TEUR – Faktor 66!) und

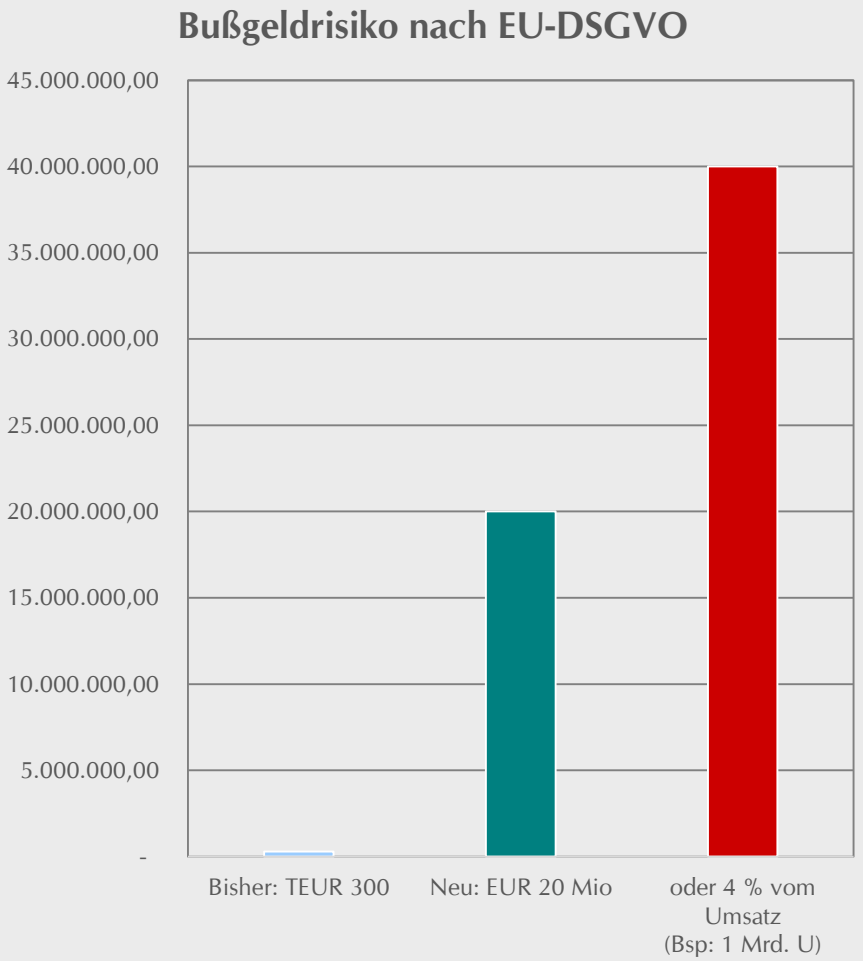
  (b) 4% des weltweiten Jahresumsatzes (wohl gesamte Unternehmensgruppe)

  sowie Schadensersatzansprüche der Betroffenen, auch wegen immaterieller Schäden (Schmerzensgeld)

- **Ergo:**

  Starke Erhöhung des Rechtsrisikos im Bereich des Datenschutz!

Compliance Management Systeme müssen neu justiert werden!



*

Grundgedanke des Datenschutzrechts seit 1970

- Schutz des „Betroffenen“, wenn Dritte mit ihren personenbezogenen Daten umgehen
- Betroffene = „Eigentümer“, Verarbeiter = (nur) „Besitzer“ bzw. „Treuhänder“ der Daten
- Besitz bedarf aber traditionell einer Berechtigung und ist stets an Pflichten gegenüber dem Eigentümer gekoppelt
- Kein formales Eigentum an Daten => Datenschutzrecht

Was sind personenbezogene Daten?

- **Grundsatz:**

  Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)

- **Grenzfälle - Beispiele**:
  - **Unternehmenszugehörigkeit** als solche (z. B. in geschäftlicher Korrespondenz)
  - **Identifikatoren**, z. B. dynamische IP-Adressen (dazu jüngst Rechtsprechung des EuGH und BGH), Cookie-IDs, Autokennzeichen, Aufzeichnung von Verhaltensdaten (Website-Benutzung etc.)
  - Verschlüsselte Daten (mit welchen Mitteln kann jemand an den Schlüssel gelangen?)
  - Bezug zu Steuerzahlungen (Grundstückswert), Arbeitsleistung (bestimmte Industrie 4.0-Daten), technische Nutzungsdaten (Telemetrie-Daten)
- **Wer ist alles „Betroffener“?**
  - Beispiel: Dritte, um die es bei einer Kommunikation geht

Betroffene Dritte

- **Beispiel Datenschutzrichtlinie Whatsapp:**

  „Adressbuch. Du stellst uns regelmäßig die **Telefonnummern von** WhatsApp-Nutzern und **deinen sonstigen Kontakten in deinem Mobiltelefon-Adressbuch** zur Verfügung. Du **bestätigst, dass du autorisiert bist, uns solche Telefonnummern zur Verfügung zu stellen**, damit wir unsere Dienste anbieten können."

- **Dazu Hamburgischer Datenschutzbeauftragter:**

  „Es ist praxisfern zu unterstellen, dass Whatsapp-Nutzer **alle Kontakte, die sie im Telefonbuch gespeichert haben, gefragt haben**, ob diese eine Übermittlung ihrer Telefonnummer an das Unternehmen erlauben."

- **Beispiel Rechtsanwälte:**

  Im Rahmen eines Mandats werden Daten über den Gegner erhoben. Nach der EU-DSGVO müsste dieser eigentlich über die Datenerhebung informiert werden und hätte Auskunftsansprüche. Derartige Rechte des Dritten werden daher im Wege einer Sonder- bzw. Ausnahmeregelung im neuen BDSG-2018 sektoral für Geheimnisträger eingeschränkt.

Unter welchen Voraussetzungen dürfen die Daten der Betroffenen verarbeitet werden?

- **Einwilligung**
  - Erfordert entsprechende Aufklärung
- **Vertragszweck**
  - Grenze zum Missbrauch bei „konstruierten“ bzw. überdehnten Vertragszwecken unklar (Beispiel: Betreiber, die Daten für den Vertragspartner nur speichern, um an sie heranzukommen)
- **Interessenabwägung**
  - Abwägung der Interessen des Verarbeiters (auch IT-Sicherheitsaspekte) und des Betroffenen
- **Problemfeld nachträgliche Zweckänderung / Zweckerweiterung**
  - Daten werden später zu einem anderen Zweck verwendet als dem, zu dem sie ursprünglich erhoben wurden (Beispiel: Big Data – Thema „Daten als Rohstoff“, der später einmal weiter ausgebeutet werden soll)
- **Ausweitung von Informations- und Auskunftspflichten gegenüber den Betroffenen**

PSP
MÜNCHEN

Wie „liest“ sich eine Interessenabwägung?

OLG Celle: Anspruch auf Entfernung eines Suchmaschinen-Links zu Berichterstattung über strafrechtliche Verurteilung und Teilnahme des Klägers an rechten Demonstrationen (Urteil vom 01.06.2017, 13 U 178/16)

Bei der gemäß § 29 Abs. 2 Nr. 1 BDSG erforderlichen Abwägung ist einerseits das Interesse des Betreibers der Suchmaschine zu berücksichtigen, der Öffentlichkeit die Nutzung des Internets zu ermöglichen bzw. zu erleichtern, andererseits das Persönlichkeitsrecht des Betroffenen, insbesondere sein Interesse, davon verschont zu bleiben, dass ihn betreffende Veröffentlichungen im Internet aufgefunden werden. Zwar kann sich der Suchmaschinenbetreiber selbst nicht auf die Presse- und Meinungsfreiheit berufen. Jedoch ist jedenfalls dann, wenn der Suchmaschinenbetreiber einen zulässigerweise veröffentlichten Beitrag der Presse verlinkt, in die Abwägung neben seiner eigenen Berufsfreiheit und der Informationsfreiheit der Internetnutzer auch die Presse- und Meinungsfreiheit des für den Inhalt des verlinkten Beitrags Verantwortlichen mit einzustellen. Denn hierdurch wird das Allgemeininteresse an der Verfügbarkeit der Information erhöht. Allerdings ist der Umstand, dass der Webseitenbetreiber sich auf die Meinungs- und Pressefreiheit berufen kann, nicht in jedem Fall gleichbedeutend mit einer Zulässigkeit der Verlinkung der Veröffentlichung über die Suchmaschine der Beklagten. Denn die Tätigkeit der Suchmaschine kann die Grundrechte des Betroffenen erheblich beeinträchtigen, und zwar zusätzlich zur Tätigkeit der Herausgeber von Websites […]. Deshalb kann die Abwägung im Rahmen des Anspruches aus § 35 Abs. 2 Satz 2 Nr. 1 BDSG gegen den Suchmaschinenbetreiber zu einem anderen Ergebnis führen als im Rahmen des Anspruchs gegen den Herausgeber der Website, da sowohl die berechtigten Interessen, die die Datenverarbeitungen rechtfertigen, unterschiedlich sein können als auch die Folgen, die die Verarbeitungen für die betroffene Person, insbesondere für ihr Privatleben, haben.

Neu: Umfangreiche Rechenschaftspflichten („Accountability“)

- Bestandsaufnahme und **Risikoanalyse**
  - Es besteht daneben die Pflicht, risikobehaftete Prozesse bzw. Geschäftsmodelle im Vorhinein der Aufsichtsbehörde zu erläutern bzw. im Rahmen einer **Datenschutz-Folgenabschätzung** vorab intern zu untersuchen und zu dokumentieren
- Planung / Umsetzung **geeigneter technischer und organisatorischer Maßnahmen (TOMs)**
  - Technisch: zur Konzeptionierung, **Sicherheit** und Verwendung von IT-Systemen nach dem Stand der Technik (Problemfeld unverschlüsselte E-Mails)
  - Organisatorisch: **Datenschutz-Policy**, Arbeitsanweisungen, kontrollierte unternehmensinterne Prozesse einschließlich Löschkonzept (Löschregelungen in Abhängigkeit des Zwecks), Schulungen der Mitarbeiter, Vertragsmanagement
- **Dokumentation** und **Nachweisbarkeit** der Einhaltung der DSGVO (**Datenschutzmanagement-System**)
- Turnusmäßige und anlassabhängige **Überprüfung und Aktualisierung** der Maßnahmen
- Die Beweislast für die Rechtmäßigkeit der Verarbeitungen liegt beim Verantwortlichen, nicht bei der Aufsichtsbehörde!

PSP MÜNCHEN

*

Neu: Auswirkungen auf die Gestaltung der Systemlandschaft

- Gestaltung der IT-Systeme zur Sicherstellung der Datenschutzgrundsätze („***privacy by design***“), z. B. Datenminimierung, Speicherbegrenzung, Integrität, Vertraulichkeit
- **Verpflichteter:** „Datenschutzrechtlich verantwortliche Stelle“ bei der Auswahl entsprechender Produkte
- **Absehbare Probleme:** Nutzung von Standard-Software und „gemischte“ Nutzung von IT-Systemen für personenbezogene und nicht-personenbezogene Daten; „Mangelhaftigkeit“ (im kaufrechtlichen Sinne) von Software wegen Nichterfüllung der Vorgaben
- Gestaltung der IT-Systeme zur Sicherstellung insbes. der Datensparsamkeit („***privacy by default***“), d. h. Menge, Umfang, Dauer und Zugänglichkeit so minimal wie möglich
- **Zertifizierungsmechanismen** noch unklar (Zertifikat begründet Indiz für ordnungsgemäße Verarbeitung)
  - Das verantwortliche Unternehmen bleibt weiterhin (neben der Verantwortlichkeit des Zertifizierungsunternehmens) voll verantwortlich

Neu: Erweiterte Verantwortung gegenüber den Betroffenen

- Vorgaben für **Informationen und Mitteilungen gegenüber dem Betroffenen** (klare Sprache, leicht zugänglich, fristgerecht, unentgeltlich, transparent)
- **Betroffenenrechte**: Auskunftsrecht, Recht auf Berichtigung, Recht auf Löschung („Vergessenwerden"), Recht auf Einschränkung der Verarbeitung und Mitteilungspflicht im gegenüber Dritten im Zusammenhang mit Berichtigung oder Löschung, Recht auf Datenübertragbarkeit, Widerspruchsrecht, Rechts auf Benachrichtigung bei „Datenpannen"
- Klare (dokumentierte) **interne Prozesse** („Anweisungslage") und **Zuständigkeiten** beim Verantwortlichen zur Erfüllung der Betroffenenrechte, regelmäßige Überprüfung der Prozesse
- Einholung des **Nachweises der Identität** bei Ausübung von Betroffenenrechten
- Keine Unterwerfung Betroffener unter eine **ausschließlich auf automatisierter Verarbeitung beruhende Entscheidung** (außer bei Abschluss und Erfüllung eines Vertrages oder Einwilligung; dann aber „Recht auf Erwirkung des Eingreifens einer Person zur Darlegung des eigenen Standpunkts und Anfechtung der Entscheidung")

PSP
MÜNCHEN

Erweitert: Datenschutzbeauftragter

- **Bisher:** > 10 Mitarbeiter
- **NEU:** Auch kleine Unternehmen (z. B. Start-ups), wenn Geschäftsmodell „datenschutzintensiv“
- **NEU:** Konzerndatenschutzbeauftragter möglich
- **NEU:** Verantwortlichkeit des Datenschutzbeauftragten steigt – **Chief Compliance Officer für Datenschutz**
  - **Achtung:** Strafbarkeitsrisiken steigen
  - **Achtung:** Haftungsrisiken steigen

PSP MÜNCHEN

*

Erweitert: Verzeichnis der Verarbeitungstätigkeiten

- In der Praxis muss jedes Unternehmen, das dauerhaft personenbezogene Daten verarbeitet, ein Verarbeitungsverzeichnis führen als **prozessorientierte Übersicht der Verarbeitungen**
  - Für die Führung ist das Unternehmen verantwortlich, aber die Aufgabe kann auf den betrieblichen Datenschutzbeauftragten delegiert werden
  - Das Verzeichnis stellt in der Praxis einen zentralen Punkt des gesamten Datenschutzmanagements dar (strukturierte Dokumentation und Ausgangspunkt von Risikobewertungen und Überwachung)
  - Das Verzeichnis muss den Datenschutzbehörden vorgelegt werden, d. h. es sollte keine detaillierten sensiblen Informationen zur Informationssicherheit enthalten
- Auch **Auftragsdatenverarbeiter** müssen künftig ein Verzeichnis zu den im Auftrag durchgeführten Verarbeitungen führen, einschließlich Name und Kontaktdaten des verantwortlichen Auftraggebers sowie Angaben zu Datenübermittlungen an Drittländer (erheblicher Mehraufwand für z. B. Cloud-Anbieter, insbesondere wenn unbekannt ist, wessen Daten genau verarbeitet werden)

Kerninhalte des Verarbeitungsverzeichnisses

- (Unternehmensgeläufige) Bezeichnung der Verarbeitungstätigkeit
- Verantwortlicher Fachbereich / Führungskraft (auch interne/externe Mitverantwortliche)
- Zweck der Verarbeitungstätigkeit (eine „Verarbeitungstätigkeit“ kann auch mehrere Teil-Geschäftsprozesse zusammenfassen)
- Rechtsgrundlage der Verarbeitungstätigkeit
- Beschreibung der Kategorien betroffener Personen (z. B. Kunden, Interessenten, Arbeitnehmer etc.)
- Beschreibung der Kategorien personenbezogener Daten (z. B. Adresse, Geburtsdatum)
- Kategorien von Empfängern bei Offenlegung (inkl. Dienstleister, Konzernunternehmen)
- Weitere Angaben bei Datenübermittlungen in Drittländer
- Löschfristen je Datenkategorie (oder Hinweis auf Löschkonzept bei komplexeren Abhängigkeiten)
- Allgemeine Beschreibung der TOMs (oder Verweis auf weitere Richtlinien etc.)

Neu: (Mehr) Meldepflichten bei Datenschutzverletzungen

- **Bislang:** Keine echte Praxisrelevanz
- **NEU:** Pflicht zur Mitteilung von sämtlichen Datenschutzverletzungen
  - sowohl den Behörden als auch
  - den Betroffenen (bei hohem Folgerisiko (Diskriminierung, Identitätsdiebstahl, finanzieller Verlust, Rufschädigung etc.))
  - innerhalb von in der Regel 72 Stunden nach Kenntniserlangung
  - mit erheblichem Bußgeldrisiko bei Unterlassung

PSP MÜNCHEN

*

Neu: Recht auf Datenübertragung / Pflichten bei Berichtigung und Löschung

- Datenübertragung an bzw. für den Betroffenen
  - In den Fällen, in denen der Betroffene die Daten selbst zur Verfügung gestellt hat, kann er diese vom verantwortlichen Datenverarbeiter in einem „strukturierten, gängigen und maschinen-lesbaren Format“ heraus- oder die Übertragung an einen Dritten verlangen.
  - Diese „Datenexportverpflichtung“ kann zu zusätzlichem Implementationsaufwand beim Verantwortlichen oder dessen Auftragsdatenverarbeiter führen.
- Verhalten bei Berichtigung, Löschung und Sperrung von Daten
  - Werden Daten über einen Betroffenen berichtigt, gelöscht oder gesperrt, nachdem sie an Dritte übermittelt wurden, muss die Berichtigung / Löschung / Sperrung dem Dritten mitgeteilt werden. Bei vorheriger Veröffentlichung der Daten (z. B. Ansprechpartner in einem Unternehmen) Verpflichtung zum Bemühen, entsprechende Links hierauf etc. zu korrigieren.

Erweitert: Eingriffsbefugnisse der Datenschutzbehörden

- Anweisungen, für die Behörde notwendige Informationen bereitzustellen
- Befugnis, anlassunabhängige Untersuchungen und Überprüfungen vor Ort vorzunehmen (Zugang zu allen Daten und zu den Geschäftsräumen)
- Befugnis, Datenverarbeitungsvorgänge zu untersagen, zu beschränken oder in bestimmter Weise vorzugeben
- Befugnis zur Anordnung, Daten zu berichtigen oder zu löschen, und die Übermittlung von Daten in Drittstaaten auszusetzen
- Die Datenschutzbehörden unterliegen weder einer Dienst-, Fach- oder Rechtsaufsicht (Unabhängigkeit der Datenschutzbehörden und damit Abkopplung von demokratischen Prozessen)
- Entscheidungen der Datenschutzbehörden können vor den Gerichten angegriffen werden

Sonstige Punkte

- Die Übermittlung personenbezogener Daten in Drittländer ist weiterhin nur zulässig, wenn der jeweilige Anbieter (z. B. Auftragsdatenverarbeiter, ausländisches Konzernunternehmen) über ein **angemessenes Datenschutzniveau** verfügt (in der Praxis meist Standard-Vertrags-bedingungen bzw. Garantie des Anbieters, Corporate Binding Rules). Sie ist außerdem dem Betroffenen vorab anzuzeigen.

- Marktortprinzip: Unter die DSGVO fallen nun auch sämtliche Anbieter, die **ohne Niederlassung in der EU** personenbezogene Daten verarbeiten, soweit diese „im Rahmen der Tätigkeit […] in der Union erfolgt“, d. h. auf EU-Bürger einwirkt. Es muss dann ein **Vertreter des Unternehmens in der EU** bestellt werden.

- Es gibt weiterhin **kein Konzernprivileg** (!) für den Datenaustausch innerhalb einer Unter-nehmensgruppe, aber möglicherweise erleichterte Bedingungen (mit im Einzelnen unklaren Voraussetzungen).

- Sind mehrere Parteien parallel in der Lage, (mit unterschiedlichen Zugriffsrechten) auf Bestände personenbezogener Daten zuzugreifen und die Daten zu verarbeiten, stellt sich die Frage nach der **Verantwortlichkeitsverteilung**.

- Es ist (weiterhin) unklar, welche „Industrie 4.0“-spezifischen Daten Personenbezug aufweisen.

- Auf das **Datengeheimnis** müssen nicht mehr nur diejenigen Personen **verpflichtet** werden, die „bei der Datenverarbeitung beschäftigt“ sind, sondern sämtliche Personen, „die **Zugang** zu personenbezogenen Daten haben“ (Bsp.: Reinigungskräfte).

PSP
MÜNCHEN

Welche unternehmensinternen Prozesse sind involviert?

- Einzelne unternehmensinterne Prozesse, in deren Rahmen personenbezogene Daten erhoben, verarbeitet, gespeichert und/oder übermittelt werden (operative Prozesse)
- Prozess der Identifikation, Bewertung, Dokumentation, (Prozess-) Strukturierung und turnusmäßigen sowie anlassbedingten Überprüfung der unternehmensinternen Datenverarbeitungstätigkeiten (Metaprozess)
- Prozess der Identifikation, Bewertung, Dokumentation und Beschaffung / Implementierung der für Datenschutz und Datensicherheit notwendigen Ressourcen und Strukturen (Infrastrukturprozess)
- Prozess der Identifikation (z. B. Schreib- und Übersetzungsbüro, Call-Center, Wartung von IT-Systemen, Cloud- und Backup-Dienste, Outsourcing von Personaldaten) und richtigen Umsetzung von Auftragsdatenverarbeitungs-Sachverhalten (Auslagerungsprozess)
- Prozesse der Bearbeitung der Betroffenenrechte
- Eskalationsprozess bei Datenpannen
- Übergeordnet: Integration des Datenschutzbeauftragten in sämtliche Prozesse, Regelung der Zuständigkeiten, Anforderungen an die Dokumentation, unternehmensinterne Sanktionierung bei Verstößen

4-Punkte-Plan

- Nr. 1 („Discover“): Welche personenbezogenen Daten sind im Unternehmen vorhanden und wo sind diese gespeichert?
- Nr. 2 („Manage“): Steuern, wie personenbezogene Daten genutzt werden und wie auf diese zugegriffen wird
- Nr. 3 („Protect“): Kontrollen einrichten, um Risiken und Datenschutzverletzungen zu verhinden bzw. zu erkennen und darauf reagieren zu können.
- Nr. 4 („Report“): Archivierung von Dokumentationen, Verwaltung von Datenanfragen und Benachrichtigungen zu Datenschutzverletzungen.

(nach Microsoft Trust Center mit Fragenkatalog von 162 Fragen)

Discover
D.1: Search for and identify personal data
D.2: Facilitate data classification
D.3: Maintain an inventory of personal data holdings
Manage
M.1: Enable data governance practices and processes
M.2: Provide detailed notice of processing activities to data subjects
M.3: Discontinue processing on request
M.4: Collect unambiguous, granular consent from data subjects
M.5: Facilitate communication mechanism between data subject and organization to handle data subject requests
M.6: Rectify inaccurate or incomplete personal data regarding data subjects
M.7: Erase personal data regarding a data subject
M.8: Provide data subject with their personal data in a common, structured format
M.9: Restrict the processing of personal data
M.10: Review data processing conducted by automated means
M.11: Appoint a Data Protection Officer (DPO)
M.12: Define enterprise risk management strategy, inclusive of data privacy risks
Protect
P.1: Data protection and privacy by design and default
P.2: Secure personal data through encryption
P.3: Secure personal data by leveraging security controls that ensure the confidentiality, integrity, and availability of personal data
P.4: Prepare for, detect, and respond to data breaches
P.5: Facilitate regular testing of security measures
Report
R.1: Keep record to display GDPR compliance
R.2: Track and record flows of personal data into and out of the EU
R.3: Track and record flows of personal data to third-party service providers
R.4: Facilitate data protection impact assessment

PSP MÜNCHEN

Die Zukunft: Vollautomatischer Datenschutz?

- Der **KI-Ansatz**: Google hat jüngst eine „Data Loss Prevention“-API vorgestellt, die sensible (inkl. personenbezogene) Daten identifiziert und schützt (durch Entfernen, Teil-Maskierung und Tokenisierung/Pseudonymisierung mit oder ohne „Wegwerfen“ des Schlüssels). Dies kann z. B. bei Datenbankabfragen „zwischengeschaltet“ werden.

ID	Job Title	Phone	Comments
359740	Senior Engineer	307-964-0673	Please email them at jane@imadethisup.com
981587	VP, Engineer	713-910-6787	none
394091	Lawyer	692-398-4146	Updated phone to: 692-398-4146
986941	Senior Ops Manager	294-967-5508	none
490456	Junior Ops Manager	791-954-3281	Tried to verify account with their SSN 222-44-5555

- Der „smart data“-Ansatz: Daten enthalten Metadaten über die in ihnen enthaltenen personenbezogenen Daten, deren Zweck, Herkunft, Löschfristen etc. und stellen mehrere (unterschiedlich verschlüsselte) Zugriffsebenen für verschiedene Benutzerrollen bereit – „der Benutzer muss sich bei den Daten selbst autorisieren“. Dies erfordert neue Datenformate und Zugriffssoftware mit entsprechenden Autorisierungsmechanismen.

PSP MÜNCHEN

Anhang: Beispiel eines „14-Punkte-Plans“ (Becker, ecckoeln.de)

- Nr. 1: Bilden Sie in Ihrem Unternehmen ein Team aus den relevanten Bereichen, in denen Daten erhoben werden (z.B. Personalabteilung, Lohnbuchhaltung; Kundenservice, Versand/Logistik, Werbeabteilung, IT). Ziehen Sie den Datenschutzbeauftragten von Beginn an hinzu. Binden Sie den Betriebsrat mit ein.

- Nr. 2: Identifizieren Sie die datenschutzrechtlich relevanten Bereiche und verabreden Sie, wie und in welcher Art die einzelnen Datenerhebungen, ihre Zwecke, die Berechtigungen und die Löschung der Daten beschrieben werden. Denken Sie auch an das Bewerbermanagement, Reisekostenabrechnungssystem, die Schlüsselverwaltung, Zeiterfassungen, E-Mail-System, Lieferantenverwaltung, Lagerverwaltung, Videoüberwachung, Firewall, Social Media Policy, Kundenkartenprogramme, Trackingmaßnahmen, Direktwerbeformen, personalisierte Werbung usw. Überall dort, wo personenbezogene Daten anfallen, setzt die Dokumentationspflicht an. Das gilt auch für inoffizielle Schubladenlisten und Excel-Tabellen Ihrer Mitarbeiter, mit denen man gleich im Zuge der Arbeiten aufräumen sollte. Vor allem mitarbeitereigene Hardware kann erhebliche Datenschutzprobleme und Risiken mit sich bringen.

14-Punkte-Plan (nach Becker, ecckoeln.de)

- Nr. 3: In diesem Zusammenhang sind sog. Verfahrensverzeichnisse bzw. nach der DS-GVO „Verarbeitungsverzeichnisse“ zu erstellen. Mit deren Hilfe kann man sich schon bei der Beschreibung vergewissern, ob der gesamte Prozess von der Datenerhebung bis zur Nutzung und Löschung datenschutzkonform erfolgt bzw. welche Maßnahmen getroffen werden müssen, um die Konformität sicherzustellen (Ist-Soll-Analyse). Im Verarbeitungsverzeichnis erfolgt die grundlegende Dokumentation aller datenschutzrelevanteren Vorgänge und die Behörde kann Einsicht in dieses verlangen.

- Nr. 4: Ein Verfahrensverzeichnis kann auch elektronisch geführt werden. Es gibt spezielle Softwareangebote, die mit Strukturen und vorgegebenen Inhalten die Erstellung erleichtern können. Das Verfahrensverzeichnis enthält jeweils u. a. Angaben zum Verantwortlichen, den Verarbeitungszwecken, den Kategorien der betroffenen Personen und Daten, den Kategorien der Empfänger, Angaben zu Übermittlungen außerhalb der EU (z. B. bei Trackern), Angaben zur Löschung und die Beschreibung der Sicherheitsmaßnahmen (technisch-organisatorische Maßnahmen, sogenannte TOM‘s).

14-Punkte-Plan (nach Becker, ecckoeln.de)

- Nr. 5: Identifizieren Sie am besten gleich, auf welcher Rechtsbasis die jeweilige Nutzung erfolgt. Entweder sind es gesetzliche Tatbestände, wie die Durchführung des Vertrages, oder es sind Einwilligungen. Dokumentieren Sie die Einwilligungstexte und die Prozesse der Einholung der Einwilligung und der Archivierung und lassen Sie diese auf Rechtskonformität prüfen. Halten Sie fest, welche Informationen bei jeder Datenerhebung vermittelt werden und lassen Sie rechtlich prüfen, ob diese ausreichen.

- Nr. 6: Erstellen Sie ein Überwachungskonzept: wie, wann und mit welcher Regelmäßigkeit können zumindest stichprobenartig die Übereinstimmung von Einwilligungen und Eintragungen in Ihrer Software geprüft werden? Welche sonstigen Sicherheitsmaßnahmen werden getroffen? Das Gesetz sieht vor, dass Sie Daten- und Sicherheitsmanagement implementieren und künftig leben. Die IT-Sicherheit steht dabei besonders im Fokus. Sie müssen alle Maßnahmen zusammentragen, die Sie hier ergriffen haben oder noch ergreifen wollen. Das fängt bei dem Zutritt zu den Büroräumen und dem Serverraum an und hört bei der Firewall nicht unbedingt auf. Hier alle relevanten Fakten zusammenzutragen und so zu beschreiben, dass sich die Zusammenstellung künftig pflegen und an Veränderungen anpassen lässt, ist eine besondere Herausforderung. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt eine Reihe von Checklisten und Formulare zur Verfügung.

14-Punkte-Plan (nach Becker, ecckoeln.de)

- Nr. 7: Sie müssen durch Dokumentation nachweisen können, dass das Unternehmen Verfahren und Regeln aufgestellt hat (Richtlinien, Prozesse usw.), die die Informationssicherheit dauerhaft definieren, steuern, überwachen und verbessern. Nachweise für ein gesetzeskonformes Management können auch durch Zertifizierungen erbracht werden. Denken Sie frühzeitig über eine solche, dann allerdings möglichst DS-GVO-konforme, Zertifizierung, zumindest der IT, nach.

- Nr. 8: In besonders kritischen Bereichen müssen Sie eine sog. Datenschutzfolgenabschätzung implementieren. Das gilt, wenn die Datenverarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt. Die EU-Datenschutzgruppe (Art. 29-Gruppe) hat 10 Kriterien festgelegt, bei deren Erfüllung ein solches Risiko besteht. Jede Datenverarbeitung ist vorab daraufhin zu prüfen, ob es voraussichtlich solche Risiken birgt. Das Ergebnis sollten Sie dann im Verfahrensverzeichnis festhalten.

14-Punkte-Plan (nach Becker, ecckoeln.de)

- Nr. 9: Schaffen Sie sich einen Reaktionsplan für Datenpannen. Jede Cyberrisk-Versicherung, deren Abschluss Sie prüfen sollten, sieht so etwas vor. Halten Sie fest, wer durch wen wann alarmiert wird, welche Sofortmaßnahmen ergriffen werden müssen, was dokumentiert werden muss und wie die Auskunfts- und Meldepflichten an die Behörden realisiert werden. Cyberrisk-Versicherungen bieten gerade bei Datenpannen Schutzkonzepte.

- Nr. 10: Klären Sie, wer bei Ihnen für die Erfüllung der Betroffenenrechte zuständig ist. Sorgen Sie für die Ausstattung mit Antwortmustern und Mitarbeiterschulungen. Legen Sie in Zusammenarbeit mit der IT-Abteilung fest, welche Datensätze wie zusammengestellt und in welcher Form zur Übermittlung (vor allem elektronisch) dem Betroffenen auf Verlangen zur Verfügung gestellt werden. Legen Sie dabei fest, welche Daten auf Verlangen einer eingeschränkten Verarbeitung unterliegen, gelöscht oder gesperrt werden und welche archiviert werden müssen. Prüfen Sie die Prozesse und den Umgang mit Werbewidersprüchen und dokumentieren Sie das im Verfahrensverzeichnis. Legen Sie fest, wie die Richtigkeit von Daten überprüft werden kann.

14-Punkte-Plan (nach Becker, ecckoeln.de)

- Nr. 11: Prüfen Sie die Auswirkungen des neuen Rechts auf Vergessenwerden. Wo werden Daten von Betroffenen bei Ihnen an Dritte weitergegeben (gibt es beispielsweise eine Presseerklärung mit Fotos und Namen von Gewinnern eines Gewinnspiels?)? Wer wäre von Ihnen zu informieren, wenn der Betroffene sein Recht geltend machen will? Wie kann man das vermeiden? Gleiches gilt für das Recht auf Datenportabilität, nach dem Sie auf Wunsch des Kunden bestimmte Daten an den Wettbewerb übergeben müssen.

- Nr. 12: Aktualisieren Sie Ihr Vertragsmanagement. Alle Verträge mit Dienstleistern, bei denen personenbezogene Daten eine Rolle spielen, müssen rechtlich auf Einhaltung der neuen Datenschutzanforderungen geprüft werden. Das Gesetz verlangt Auftragsdatenverarbeitungsabreden mit ganz bestimmten Mindestinhalten.

- Nr. 13: Gehen Sie schließlich die Mitarbeiterverpflichtungserklärungen zum Datengeheimnis an. Die alten stimmen nicht mehr und müssen ohnehin am besten jährlich erneuert werden. Die Mitarbeiter sollten jetzt aus Nachweisgründen auf Vertraulichkeit verpflichtet werden, auch wenn das Gesetz eine ausdrückliche Verpflichtungserklärung außerhalb des öffentlichen Sektors nicht mehr kennt.

14-Punkte-Plan (nach Becker, ecckoeln.de)

- Nr. 14: Implementieren Sie in Zusammenarbeit mit dem Datenschutzbeauftragten regelmäßige Schulungen und Sensibilisierungsmaßnahmen für die Mitarbeiter.

Vielen Dank für Ihre Aufmerksamkeit

Dr. Axel-Michael
Wagner
a.wagner@psp.eu

Peters, Schönberger & Partner
Rechtsanwälte Wirtschaftsprüfer Steuerberater
Schackstraße 2
80539 München
Tel.: +49 89 3 81 72 - 0
Fax: +49 89 3 81 72 - 204
E-Mail: psp@psp.eu
Internet: www.psp.eu

PSP
MÜNCHEN