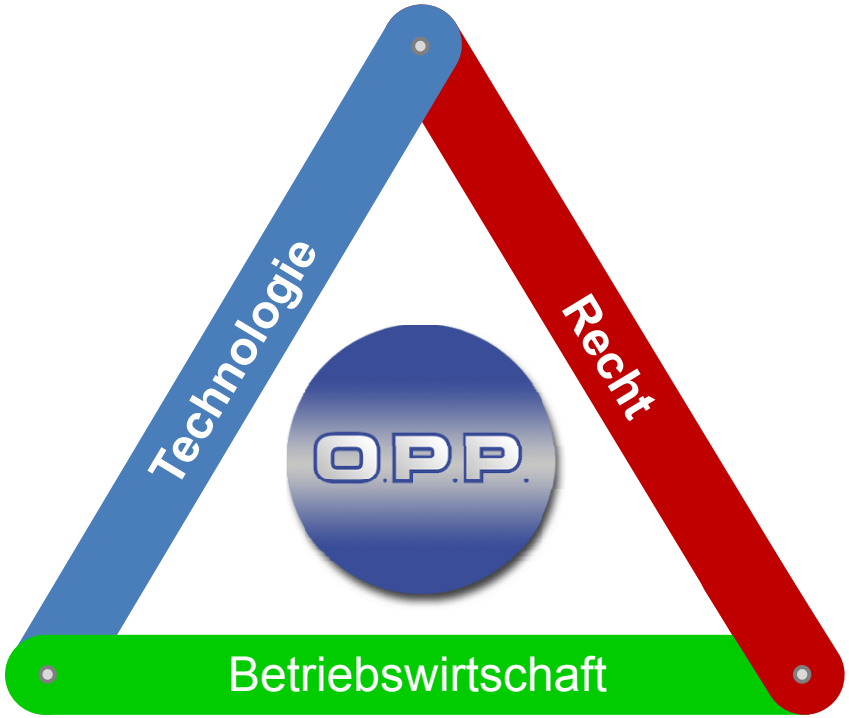
Kendox
Informationsveranstaltung



Grundlagen zum Datenschutz

Themen

DSG 2000 (derzeit gültig)

- Einführung
- Grundlagen des Datenschutzrechtes
- Melde- und Genehmigungspflichten
- Die Rechte der Betroffenen
- Datensicherheitsmaßnahmen in der Praxis
- Pflicht zur Verschwiegenheit
- der Umgang mit DVR-Online
- Zulässigkeit von Kontrollmaßnahmen

Aktuelle Entwicklungen iZmd EU-Datenschutz-Grundverordnung

Daten-Schutz

- Daten!
- was sind Daten?
- welche Daten meinen wir?
- welche Daten meint das DSG?

- Schutz!
- warum schützen wir Daten?
- vor oder für wen?
- was schützt das DSG?
- wie schützt das DSG?
- was schützt das DSG nicht?

GRUNDLAGEN DES DATENSCHUTZRECHTES

Begriffe (die wichtigsten)

1. Angaben
2. personenbezogene Daten
3. sensible Daten (potentiell sensible Daten)
4. Datei
5. Datenanwendungen
6. Betroffener
7. Auftraggeber
8. Dienstleister
9. Überlassen
10. Übermitteln
11. Verwenden
12. Verarbeiten
13. Informationsverbundsystem

1. Angaben

Jede Form von Information

- egal worüber
- unabhängig davon, in welcher Form diese vorliegen
  - ob auf Papier
  - auf Datenträger
  - im Kopf
  - strukturiert
  - unstrukturiert
  - etc.

2. personenbezogene Daten

§ 4 Z 1 DSG

Angaben über Personen deren Identität bestimmt oder bestimmbar ist;

Beispiel: „Mag. Max Oppenheimer“ + „4600 Wels“

„nur indirekt personenbezogen“ sind Daten dann, wenn der Personenbezug der Daten derart ist, dass die Identität der Personen *(im jeweiligen Fall)* mit rechtlich zulässigen Mitteln nicht bestimmt werden kann.

3. sensible Daten

§ 4 Z 2 DSG

Daten natürlicher Personen über ihre

- rassische und ethnische Herkunft,
- politische Meinung,
- Gewerkschaftszugehörigkeit,
- religiöse oder philosophische Überzeugung,
- Gesundheit oder
- ihr Sexualleben

Diese Aufzählung ist abschließend!

Exkurs: potentiell sensible Daten

sensible Daten sind nicht beabsichtigt, können aber passieren
(zB Video von Rollstuhlfahrer, E-Mail an „info@aidshilfe.at“)

4. Datei

§ 4 Z 6 DSG

„strukturierte Sammlung von Daten,

die nach mindestens einem Suchkriterium zugänglich sind.“

Sagt noch nichts über allfällige automatisationsunterstützte Verarbeitung

Auch Karteien in Papierform (sortiert nach Alphabet, Kundennummer, Aktenzahl, etc.) ist eine Datei

Nicht aber ein Papierakt *(Achtung bei Digitalisierung!)*:

- Personalakt
- Auftragsakt (Produktionspapiere, etc.)

5. Datenanwendungen

§ 4 Z 7 DSG

„die Summe der in ihrem Ablauf **logisch verbundenen** **Verwendungsschritte** (Z 8), die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zweckes der Datenanwendung) geordnet sind und **zur Gänze oder auch nur teilweise automationsunterstützt**, also maschinell und programmgesteuert, erfolgen (automationsunterstützte Datenanwendung) „

6. Betroffener

§ 4 Z 3 DSG

jede vom Auftraggeber (Z 4) verschiedene natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet (Z 8) werden

7. Auftraggeber

§ 4 Z 4 DSG

„natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie allein oder gemeinsam mit anderen die **Entscheidung** getroffen haben, **Daten zu verwenden** ……."

8. Dienstleister

§ 4 Z 5 DSG

„natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie Daten nur zur Herstellung eines ihnen aufgetragenen Werkes verwenden“

Aber:

Dienstleister **gelten dann als Auftraggeber**, wenn sie Daten zu einem Zweck verwenden, der ihnen ausdrücklich untersagt wurde, oder wenn der Beauftragte auf Grund von Rechtsvorschriften oder Verhaltensregeln über die Verwendung eigenverantwortlich zu entscheiden hat. (§ 4 Z 4 SDG)

9. Überlassen

§ 4 Z 11 DSG

„die Weitergabe von Daten zwischen Auftraggeber und Dienstleister im Rahmen des Auftragsverhältnisses“

10. Übermitteln

§ 4 Z 12 DSG

„die Weitergabe von Daten an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister, insbesondere auch das **Veröffentlichen** von Daten; darüber hinaus auch die Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers“

Veröffentlichen:

Daten einem nicht nur eingeschränkten Kreis von Personen zur Kenntnis bringen.

- Vereinszeitung?
- Internet?

11. Verwenden

§ 4 Z 8 DSG

„jede Art der Handhabung von Daten, also sowohl das Verarbeiten (Z 9) als auch das Übermitteln (Z 12) von Daten“

12. Verarbeiten

§ 4 Z 9 DSG

„das Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen (Z 11), Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten mit Ausnahme des Übermittelns (Z 12) von Daten“

13. Informationsverbundsystem

§ 4 Z 13 DSG

„die gemeinsame Verarbeitung von Daten in einer Datenanwendung durch mehrere Auftraggeber und die gemeinsame Benützung der Daten in der Art, dass jeder Auftraggeber auch auf jene Daten im System Zugriff hat, die von den anderen Auftraggebern dem System zur Verfügung gestellt wurden“

Beispiele:

- Kreditnehmerevidenz der Banken
- Buchungs- und Reservierungssysteme für Hotels
- zentrales Melderegister (ZMR)

Überlassung an Dienstleister

§ 10 Abs 1DSG

Auftraggeber dürfen bei ihren Datenanwendungen **Dienstleister in Anspruch nehmen**, wenn

diese ausreichende Gewähr für eine rechtmäßige und sichere Datenverwendung bieten.

Der Auftraggeber hat mit dem Dienstleister die hiefür notwendigen **Vereinbarungen zu treffen** und sich von ihrer Einhaltung durch Einholung der erforderlichen Informationen **über die vom Dienstleister tatsächlich getroffenen Maßnahmen zu überzeugen**.

→ *spezielle Problematik „Cloud Services“*

§ 10 Abs 2 enthält Bestimmungen für AG des öffentl. Bereiches

Pflichten des Dienstleisters

§ 11 Abs 1 DSG

1. Verwendung ausschließlich im Rahmen der Aufträge des Auftraggebers
2. keine Übermittlung ohne Auftrag des Auftraggebers
3. treffen der erforderlichen Datensicherheitsmaßnahmen (§ 14)
4. Mitarbeiter zur Einhaltung des Datengeheimnisses (§ 15) verpflichten (evtl. gesetzliche Verschwiegenheitspflicht)
5. Subauftragnehmer nur mit Zustimmung des AG
6. Schaffen der Voraussetzungen für die Erfüllung der Auskunfts- Richtigstellungs- und Löschungspflicht des Auftraggebers
7. nach Beendigung die Daten dem Auftraggeber zu übergeben oder in dessen Auftrag für ihn weiter aufzubewahren oder zu vernichten

Übermittlung / Überlassung ins Ausland

Genehmigungspflichtig § 13 DSG (Überblick):

Soweit der Datenverkehr mit dem Ausland nicht gemäß § 12 genehmigungsfrei ist, hat der Auftraggeber vor der Übermittlung oder Überlassung von Daten in das Ausland eine Genehmigung der Datenschutzbehörde einzuholen.

Die Datenschutzbehörde kann die Genehmigung an die Erfüllung von Bedingungen und Auflagen binden.

Voraussetzung ist die Rechtmäßigkeit der Datenanwendung im Inland

Die DSB ist bei der Erteilung der Genehmigung an Regeln gebunden

- insb. Standardvertragsklauseln (entwickelt von der EU Kommission)

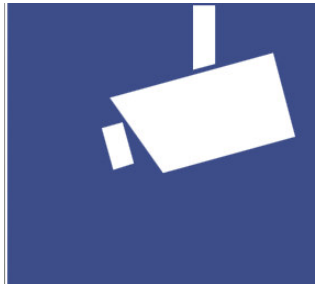
Videoüberwachung

Videoüberwachungen unterliegen der **Meldepflicht**

Soweit gemäß § 96a ArbVG Betriebsvereinbarungen abzuschließen sind, sind diese im Registrierungsverfahren vorzulegen.

Ausnahmen von der Meldepflicht bestehen für:

1. in Fällen der Echtzeitüberwachung oder
2. wenn eine Speicherung (Aufzeichnung) nur auf einem analogen Speichermedium erfolgt.



Für Videoüberwachung besteht eine **Kennzeichnungspflicht**

Die Kennzeichnung hat örtlich derart zu erfolgen, dass jeder potentiell Betroffene, der sich einem überwachten Objekt oder einer überwachten Person nähert, tunlichst die Möglichkeit hat, der Videoüberwachung auszuweichen.

Pflichten des Auftraggebers

Überprüfung der Zulässigkeitsvoraussetzungen § 7

Beurteilung der Geheimhaltungsinteressen §§ 8 + 9

Erfüllen der Meldepflicht(en) §§ 17 + 18

Einhaltung der Grundsätze § 6

Treffen der Datensicherheitsmaßnahmen § 14

Verpflichtung der Mitarbeiter/Datengeheimnis § 15

Prüfung der Kriterien bei Einsatz eines Dienstleisters §§ 10 + 11

genehmigungspflichtige Übermittlung/Überlassung ins Ausland nur nach vorhergehender Bewilligung § 13

Informationspflicht § 24

Offenlegungspflicht § 25

Wahrung der Betroffenenrechte (Auskunft § 26, Richtigstellung oder Löschung § 27, Widerspruch § 28)

DSG 2000

MELDE- UND GENEHMIGUNGSPFLICHTEN

Meldepflicht (1)

§ 17 Abs 1 DSG

Jeder Auftraggeber hat vor Aufnahme einer Datenanwendung eine Meldung an die Datenschutzbehörde zum Zweck der Registrierung im Datenverarbeitungsregister zu erstatten.

Ausnahmen:

1. Datenanwendungen mit ausschließlich veröffentlichten Daten
2. Register & Verzeichnisse die von Gesetz wegen öffentlich einsehbar sind
3. Datenanwendungen die nur indirekt personenbezogene Daten beinhalten
4. Datenanwendungen natürlicher Personen ausschließlich für private oder familiäre Interessen
5. Datenanwendungen für publizistische Tätigkeiten (§ 48)
6. Datenanwendungen die einer Standardanwendung entsprechen (Standard- und Musterverordnung)

Die wichtigsten Standardanwendungen

SA001 Rechnungswesen und Logistik

SA002 Personalverwaltung für privatrechtliche Dienstverhältnisse

SA007 Verwaltung von Benutzerkennzeichen

SA022 Kundenbetreuung und Marketing für eigene Zwecke

SA032 Videoüberwachung

SA033 Datenübermittlung im Konzern

Genehmigungspflicht

§ 18. (1) Der Vollbetrieb einer meldepflichtigen Datenanwendung darf unmittelbar nach Abgabe der Meldung aufgenommen werden. - außer wenn sie:

1. **sensible Daten** enthalten oder
2. **strafrechtlich relevante Daten** im Sinne des § 8 Abs. 4 enthalten oder
3. die **Auskunftserteilung über die Kreditwürdigkeit** der Betroffenen zum Zweck haben oder
4. **in Form eines Informationsverbundsystems** durchgeführt werden sollen.

Diese Anwendungen dürfen erst nach ihrer Prüfung (Vorabkontrolle) durch die Datenschutzbehörde nach den näheren Bestimmungen des § 20 aufgenommen werden.

RECHTE DER BETROFFENEN

Rechte der Betroffenen (1)

Welche Rechte hat der Betroffene?

Auskunftsrecht § 26 DSG

Recht auf Richtigstellung oder Löschung § 27 DSG

Recht auf Widerruf § 28 DSG

Nach dem Datenschutzgesetz

MAßNAHMEN ZUR DATENSICHERHEIT

Datensicherheitsmaßnahmen (1)

§ 14 DSG Abs 1

Für alle Organisationseinheiten eines Auftraggebers oder Dienstleisters, die Daten verwenden,

sind Maßnahmen zur Gewährleistung der Datensicherheit **zu treffen**. Dabei ist je nach der Art der verwendeten Daten und nach Umfang und Zweck der Verwendung sowie unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit sicherzustellen, daß die Daten **vor zufälliger oder unrechtmäßiger Zerstörung** und **vor Verlust** geschützt sind, daß ihre **Verwendung ordnungsgemäß** erfolgt und daß die Daten **Unbefugten nicht zugänglich** sind.

Datensicherheitsmaßnahmen (2)

Festlegen der ausdrücklichen Aufgabenverteilung bei der Datenverwendung zwischen den Organisationseinheiten und zwischen den Mitarbeitern

Definition der Organisationseinheiten (Abgrenzung) sowie Beschreibung von Rollen der Mitarbeiter in diesen Organisationseinheiten im Zusammenhang mit einzelnen Datenanwendungen und den damit verbundenen Rechten einzelner Rollen-Inhaber (eventuell im Rahmen von Stellenbeschreibungen).

Zu beschreiben sind jedenfalls:

- Aufgabenart (Ausführung, Leitung, Beratung, etc.)
- Aufgabenumfang und
- Befugnisse (Entscheidungen, Anordnungen).

Allenfalls Kategorisierung der Datenanwendungen unter Bezug auf die Art der darin verarbeiteten Daten. (zB Finanzbuchhaltung, Personalverrechnung, Kunden-, Patientendaten). Kategorisierung jedenfalls in Bezug auf das DSG.
Anm.: Eine zusätzliche Kategorisierung der (auch nicht personenbezogenen) Daten nach internen Regeln, zB in Bezug auf Grad der innerbetrieblich erforderlichen Geheimhaltung, erweist sich in der Praxis als sinnvoll (öffentlich, intern, vertraulich, geheim)

Datensicherheitsmaßnahmen (3)

Bindung der Verwendung von Daten an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter

Forderung: Nur derjenige darf Daten verwenden, der diese aufgrund seiner Rolle benötigt

Lösung: Einrichten von Berechtigungen nach dem „need to know“-Prinzip. Das System der Vergabe von Berechtigungen ist zu beschreiben und sicher zu stellen, dass dieses System in der Praxis umgesetzt und eingehalten wird.

Regelungen im Zusammenhang mit dem Wechsel einer Person innerhalb der Organisation sollen sicher stellen, dass „historische“ Berechtigungen entzogen werden und keine „Rechtekumulation“ erfolgt.

Datensicherheitsmaßnahmen (4)

Belehrung der Mitarbeiter über seine nach diesem Bundesgesetz und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten

Erstellen von innerbetrieblichen Datenschutz- und Datensicherungsvorschriften (in Schriftform). Je nach Organisationseinheit können diese Vorschriften unterschiedliche Ausprägungen haben (zB Mitarbeiter der IT, der Fachbereiche, Mitarbeiter in leitenden Positionen). Diese Vorschriften müssen jedem Mitarbeiter (=jeder der entsprechende Datenanwendungen nutzt, auch Werkvertragsnehmer, Mitarbeiter von Fremdfirmen, Gäste, etc.) zur Kenntnis gebracht werden.

Sinnvolle Maßnahmen in diesem Zusammenhang sind zB Schulungen. Ein Nachweis darüber, dass diese Vorschriften zur Kenntnis gebracht wurden ist jedenfalls sinnvoll (unterschriebene Teilnehmerlisten, schriftliche Bestätigung, dass die Information vermittelt und verstanden wurde).

Datensicherheitsmaßnahmen (5)

Regelung der Zutrittsberechtigung zu den Räumlichkeiten des Auftraggebers oder Dienstleisters

Forderung: Schaffung physischer Barrieren und Beschreibung der Regeln, wie dieser Zutritt geregelt ist.

Lösung: Erstellung eines Konzeptes für Sicherheitszonen für den eigenen Bereich, sowie Dokumentation der Zutrittsberechtigungen in den Räumlichkeiten des (der) Dienstleister. Prüfung der Zutrittsregelungen in Bezug auf die jeweiligen Anforderungen.

Datensicherheitsmaßnahmen (6)

Regelung der Zugriffsberechtigung auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte

Beschreibung der Regeln für die Erteilung von Zugriffsberechtigungen auf Daten- bzw. Programm-Ebene. Definition von Rollen, Zuständigkeiten und Verantwortlichkeiten. Beschreibung jener Maßnahmen, die geeignet sind um Einsichtnahme und Verwendung von Datenträgern durch Unbefugte zu verhindern. Regelungen für die Gestaltung von Zugriffsberechtigungen: zB Username und Passwort. (Komplexität der Passwörter, Änderungsintervall, Wiederverwendung) allenfalls 2-Faktoren Authentifizierung.
Auf Datenträger-Ebene:

- Verschlüsselung auf System-Ebene.
- Sichere Entsorgung von nicht mehr verwendeten Datenträgern.
- Umgang mit Backup-Medien, Datenträgeraustausch.

Sonderproblem: Reparatur-Arbeiten durch Dritte, evtl. außerhalb der Räumlichkeiten des Auftraggebers.

Datensicherheitsmaßnahmen (7)

Festlegung der Berechtigung zum Betrieb der Datenverarbeitungsgeräte und Absicherung bei den eingesetzten Maschinen oder Programmen gegen unbefugte Inbetriebnahme

Die entsprechenden Regelungen und Maßnahmen sind zu beschreiben und umzusetzen. Die Einhaltung derselben, sowie deren Wirksamkeit sind laufend zu prüfen. Die Maßnahmen können

- baulich,
- technisch oder
- organisatorisch

sein.

Datensicherheitsmaßnahmen (8)

Führen von Protokollen, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können

Forderung: Führung von Protokollen über die Verwendung personenbezogener Daten, insbesondere der Übermittlung. Die Protokolle müssen dazu geeignet sein, einen erforderlichen Nachweis zu führen.

Lösung: Klärung welche Protokollierungen aufgrund der bestehenden Anwendungen möglich sind. Falls die Möglichkeiten der Protokollierung nicht ausreichen um den gesetzlichen Forderungen zu entsprechen, Begründung weshalb dieser Zustand dennoch beibehalten wird (zB technische Machbarkeit, wirtschaftliche Gründe).

Diese Protokolle müssen gem § 14 Abs 5 DSG 3 Jahre lang aufbewahrt werden!

Datensicherheitsmaßnahmen (9)

Führen einer Dokumentation über die nach § 14 Abs 2 Z 1 bis 7 DSG getroffenen Maßnahmen, um die Kontrolle und Beweissicherung zu erleichtern

Die Erstellung einer Gesamtdokumentation der Datensicherungsmaßnahmen ist gesetzlich vorgegeben. Es wird empfohlen, diese Dokumentation (allenfalls erweitert um innerbetriebliche Maßnahmen) zu erstellen und sicher zu stellen, dass erforderliche Änderungen (sowohl technischer als auch organisatorischer Natur) laufend in diese Dokumentation einfließen. Aus Gründen der Beweisführung wird eine durchgehende Versionierung und Archivierung historischer Versionen empfohlen.

Datensicherheitsmaßnahmen (10)

§ 14 Abs 3 DSG

Nicht registrierte Übermittlungen aus Datenanwendungen, die einer Verpflichtung zur Auskunftserteilung gemäß § 26 unterliegen, sind so zu protokollieren, daß dem Betroffenen Auskunft gemäß § 26 gegeben werden kann.

Die Protokollierungspflicht nicht registrierter Datenanwendungen ist in der Praxis umstritten, da nicht umfassend geklärt ist, welche Anwendungen hier betroffen sind. Ausgenommen von dieser Pflicht sind jedenfalls Übermittlungen aus Standard- und Musteranwendungen. Ob Anwendungen die gem § 17 DSG dem Datenverarbeitungsregister (DVR) gemeldet wurden betroffen sind, ist strittig. Zusätzlich betroffen könnten nicht meldepflichtige Datenanwendungen sein, die ausschließlich veröffentlichte oder Daten für publizistische Tätigkeiten verarbeiten.

Aus Gründen der Rechtssicherheit wird eine umfassende Protokollierung von Übermittlungen personenbezogener Daten für alle Anwendungen empfohlen, die keine Standard- und Musteranwendungen sind.

Datensicherheitsmaßnahmen (11)

§ 14 Abs 4

Die Verwendung der Protokolldateien zu anderen Zwecken als der Protokollierung der Verwendung der entsprechenden Daten ist nicht zulässig. Insbesondere dürfen diese Daten nicht dazu verwendet werden um die Leistungen der Mitarbeiter zu überprüfen.

§ 14 Abs 5

Die Protokolle über die Verarbeitung bzw. Übermittlung personenbezogener Daten sind in der Regel 3 Jahre aufzubewahren. Soweit es zulässig ist, die betroffenen Daten früher zu löschen oder länger aufzubewahren, sind auch die Protokolle so lange aufzubewahren, als auch diese Daten zulässigerweise nicht gelöscht werden.

§ 14 Abs 6

Die Datensicherheitsvorschriften müssen so aufbewahrt werden, dass sich die Mitarbeiter jederzeit Einblick darin verschaffen können. In der Praxis sollten die diesbezüglichen Dokumente an zentraler Stelle in Papierform aufliegen. Soweit möglich empfiehlt sich zudem die Veröffentlichung der Dokumente in elektronischer Form (Intranet, Extranet).

Datengeheimnis (§15 DSG)

- Richtet sich an
  - Auftraggeber und Dienstleister sowie deren Mitarbeiter
- Inhalt:
  - Z1: die anvertrauten Daten sind geheim zu halten soweit kein zulässiger Grund zur Übermittlung besteht
  - Z2: Mitarbeiter müssen vertraglich (nachweislich!) zur Wahrung des Datengeheimnisses verpflichtet werden (über das Ende des Dienstverhältnisses hinaus) – sofern nicht ohnehin eine gesetzliche Verpflichtung der Mitarbeiter besteht
  - Z3: Mitarbeiter sind über die für sie geltenden Regeln der Datenübermittlung und die Folgen der Verletzung des Datengeheimnisses zu belehren (nachweislich!)
- Verwaltungsstrafbestimmungen
  - Verstöße sind gem § 52 Abs 1 Z 3 mit Geldstrafe bis zu € 25.000,-- bedroht
  - auch der Versuch ist strafbar

Elektronische Meldungen

DVR-ONLINE

Allgemeines / Voraussetzungen

Seit 1.9.2012 in Betrieb

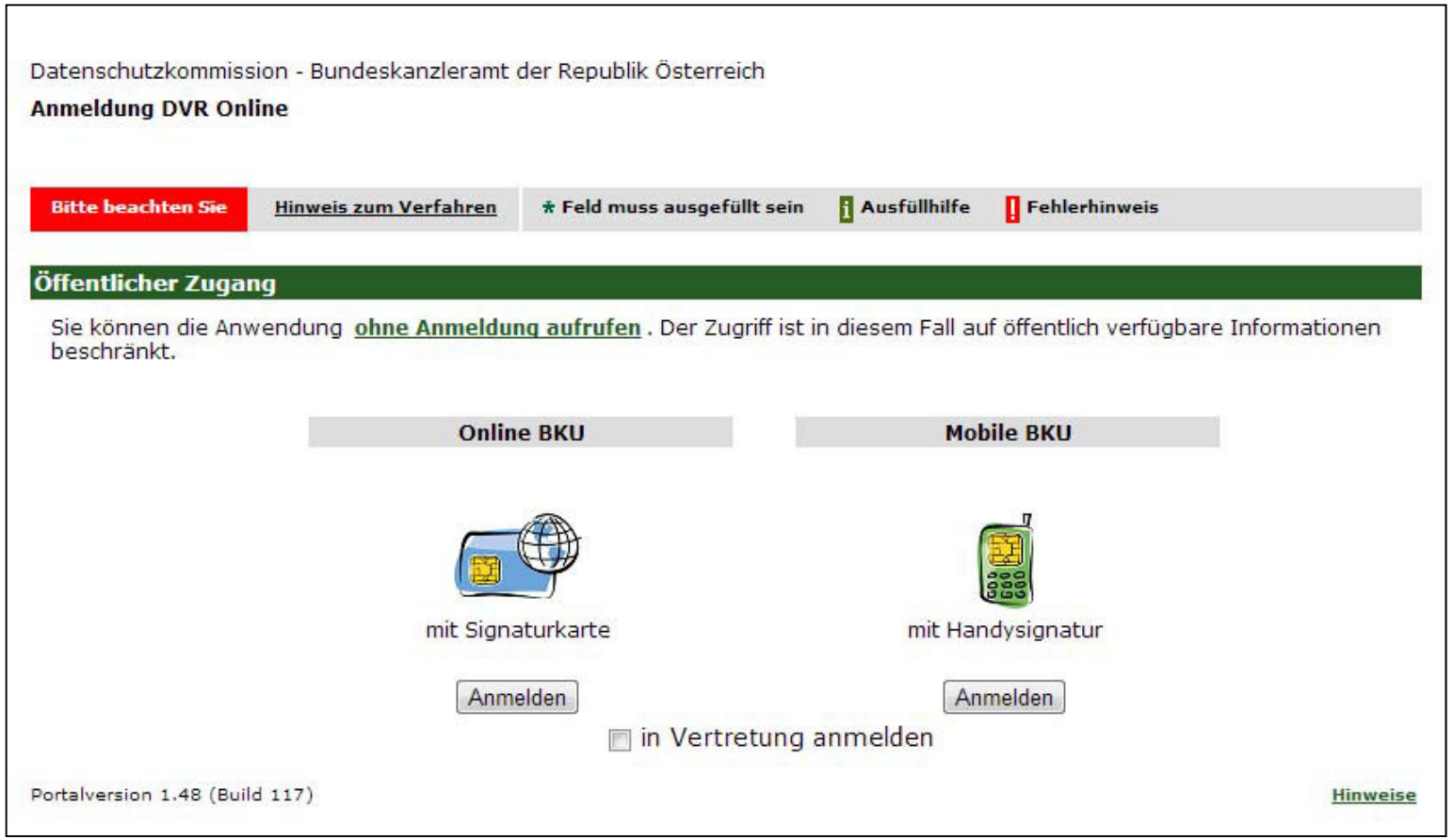
Meldungen sind seit diesem Zeitpunkt nur noch über DVR-Online möglich

Voraussetzung:

- Authentifizierung über Bürgerkarte
- Einzelvertretungsbefugnis lt. Firmebuch (Vereinsregister, etc.)
- Elektronische Vollmacht:
  - Über Vollmachtenservice der Stammzahlenregisterbehörde
  - Über Unternehmensserviceportal www.usp.gv.at

Verwenden von DVR-Online

https://dvr.dsb.gv.at/



Beispiel DVR-Meldung

Zusammenfassung Datenanwendung

Gemeldet am:	15.10.2012
Registriert am:	07.12.2012
Gestrichen am:	-
Bezeichnung/Zweck:	VIDEOÜBERWACHUNG: M.-Corvinus-Str.15, 4600 Wels
Bereich öffentlich/privat:	privater Bereich
Automationsunterstützt/manuell:	Automationsunterstützt
Angaben zur Vorabkontrolle:	Verwendung von strafrechtlichen Daten Videoüberwachung (gemäß § 50c DSG 2000)
Rechtsgrundlagen:	§§ 50a ff DSG 2000 idgF §§ 353 ff ABGB (Eigentumsschutz) § 80 StPO Zweck: Eigen-/Objektschutz bzw. Erfüllung rechtlicher Sorgfaltspflichten, jeweils einschließlich der Beweissicherung, mit ausschließlicher Auswertung in dem durch die Zweckbezeichnung definierten Anlassfall, sofern bestimmte Tatsachen die Annahme rechtfertigen, das überwachte Objekt könnte das Ziel oder der Ort eines gefährlichen Angriffs werden

Zusammenfassung Daten des Auftraggebers

Daten des Auftraggebers

DVR-Nummer:	4008765
DAN-Nummer:	4008765/001
Bezeichnung des Auftraggebers:	O.P.P. - Beratungs GmbH
Adresse:	M.-Corvinus-Str. 15, 4600 Wels, Österreich
Telefonnummer:	Tel.: 069912518089
E-Mail Adresse:	office@opp-beratung.com

Vertreter des Auftraggebers

Name des Vertreters:	Markus, Oman, Mag. Ing., CSE, SBH
Telefonnummer:	Tel.: 069912518089
E-Mail-Adresse:	markus.oman@opp-beratung.com

Zuordnung betroffene Personengruppe(n) / Datenarten / Übermittlungsempfänger

Liste der Zuordnungen

Personenguppe	Datenart	Zugeordnete Übermittlungsempfänger
Personen, welche sich im videoüberwachten Bereich aufhalten	Bilddaten der Betroffenen (Aussehen, Verhalten)	01, 02, 03, 04
	Ort der Bildaufzeichnung (Räumlichkeit, Standort der Kamera)	01, 02, 03, 04
	Zeit der Bildaufzeichnung (Datum, Uhrzeit, Beginn/Ende der Bildaufzeichnung)	01, 02, 03, 04
Im Rahmen der Videoüberwachung aufgenommene Personen, welche im Anlassfall identifiziert werden	Bilddaten der Betroffenen (Aussehen, Verhalten)	01, 02, 03, 04
	Ort der Bildaufzeichnung (Räumlichkeit, Standort der Kamera)	01, 02, 03, 04
	Zeit der Bildaufzeichnung (Datum, Uhrzeit, Beginn/Ende der Bildaufzeichnung)	01, 02, 03, 04
	Identität der Betroffenen, soweit aus der Aufzeichnung für den Auswertenden erkennbar	01, 02, 03, 04
	Rolle der Betroffenen (z. B. Täter, Opfer, Zeuge), soweit aus der Aufzeichnung erkennbar	01, 02, 03, 04

Übermittlungsempfänger

Liste der Übermittlungsempfänger

LfdNr	Bezeichnung	Rechtsgrundlage
01	Zuständige Behörde bzw. zuständiges Gericht (zur Sicherung aus Beweisgründen in Strafrechtssachen)	§§ 80 bzw. 109 ff StPO iVm §§ 7, 8 und § 50a Abs. 6 Z 1 DSG 2000 idgF
02	Sicherheitsbehörden (zu sicherheits-polizeilichen Zwecken)	§§ 53 Abs. 5 SPG iVm § 50a Abs. 6 Z 2 DSG 2000 idgF
03	Gerichte (zur Sicherung von Beweisen in Zivilrechtssachen)	§§ 384 ff ZPO iVm §§ 7 und 8 Abs. 3 Z 5 DSG 2000 idgF
04	Versicherungen (ausschließlich zur Abwicklung von Versicherungsfällen)	§§ 7 und 8 Abs. 1 Z 4, 8 Abs. 3 Z 4 und 5 DSG 2000 idgF

Datenschutzbeauftragter

Datenschutzbeauftragter

Name (Vorname, Nachname, Titel):	Markus, Oman, Mag. Ing., SBH, CSE
Adresse:	M.-Corvinus-Str. 15, 4600 Wels, Österreich
E-Mail Adresse:	markus.oman@opp-beratung.com
Telefon:	069912518089

Beispiel DVR-Meldung

Zusammenfassung Datenanwendung	
Gemeldet am:	25.02.2014
Registriert am:	25.02.2014
Gestrichen am:	-
Bezeichnung/Zweck:	Kunden- und Interessentenverwaltung – Marketing
Bereich öffentlich/privat:	privater Bereich
Automationsunterstützt/manuell:	Automationsunterstützt
Angaben zur Vorabkontrolle:	Vorliegen keiner der Voraussetzungen
Rechtsgrundlagen:	Gewerbeberechtigung

Zusammenfassung Daten des Auftraggebers

Daten des Auftraggebers	
DVR-Nummer:	4011565
DAN-Nummer:	4011565/001
Bezeichnung des Auftraggebers:	Russmedia Service GmbH
Adresse:	Gutenbergstraße 1, 6858 Schwarzach, Vorarlberg, Österreich
Telefonnummer:	
E-Mail Adresse:	info@russmedia.com

Zuordnung betroffene Personengruppe(n) / Datenarten / Übermittlungsempfänger

Liste der Zuordnungen

Personenguppe	Datenart	Zugeordnete Übermittlungsempfänger
Eigene Kunden oder Interessenten	Ordnungsnummer	01
	Name bzw. Bezeichnung	01
	Anrede/Geschlecht	01
	Anschrift	01
	Telefon- und Faxnummer und andere zur Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben	01
	Sperrkennzeichen für Werbeaktionen des Auftraggebers	01
	Untersagung der Übermittlung der Daten an Adressverlage	01
	Berufs-, Branchen- und Geschäftsbezeichnung	01
	Firmenbuchdaten	01
	Korrespondenzsprache, sonstige Vereinbarungen und Schlüssel zum Datenaustausch	01
	Geburtsdatum, wenn vom Betroffenen angegeben	01
	Personenstand, wenn vom Betroffenen angegeben	01
	Nachfrageinteressen (auf Grund bisherigen Nachfrageverhaltens oder eigener Angaben des Kunden gegenüber dem Auftraggeber)	01
	Kaufkraftklassifizierung	01
	Betreuungsdaten (wie: zugesandtes Werbematerial, Besuchsrhythmus etc.)	01
	Kaufverhalten (Frequenz und Volumen)	01
	Sonstiges Antwortverhalten zu Werbeaktivitäten des Auftraggebers (Teilnahme an Gewinnspielen)	01
	Bonus- und sonstige Vorteilsdaten, die sich aus der Kunden- oder Interessenteneigenschaft ergeben	01
Kontaktpersonen bei Kunden oder Interessenten	Ordnungsnummer	01
	Name bzw. Bezeichnung, Anrede/Geschlecht	01
	Zugehöriger Kunde oder Interessent (Bezeichnung und Anschrift)	01
	Telefon- und Faxnummer und andere zur Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben	01
	Korrespondenzsprache	01
	Funktion oder betreutes Aufgabengebiet beim Kunden oder Interessenten	01
	Geburtstag, Personenstand und dgl., soweit die Verwendung vom Betroffenen für Zwecke der Kontaktpflege gestattet wird	01
	Betreuungsdaten (wie: zugesandtes Werbematerial, Besuchsrhythmus, etc.)	01

Übermittlungsempfänger

Liste der Übermittlungsempfänger

LfdNr	Bezeichnung	Rechtsgrundlage
01	Konzerngesellschaften und verbundene Gesellschaften	Vertragserfüllung (§ 8 Abs 3 Z 4 DSG) Zustimmungserklärung des Betroffenen (§ 8 Abs 1 Z 2 DSG)

Strafgesetzbuch (1)

§118 StGB Verletzung des Briefgeheimnisses

bestraft wird, wer ein nicht zu seiner Kenntnisnahme versandtes Schriftstück öffnet, oder verhindert, dass der rechtmäßige Empfänger dieses Schriftstück erhält (bis 3 Monate od. 180 Tagsätze)

§119 StGB Verletzung des Telekommunikationsgeheimnis

bestraft wird, wer sich unbefugt Kenntnis vom Inhalt elektronisch übermittelter Nachrichten (zB E-Mails) verschafft (bis 6 M od. 360 TS)

§118a Widerrechtlicher Zugriff auf ein Computersystem

bestraft wird (bis 6 M od. 360 TS):

- **wer sich** oder andern vorsätzlich und **unbefugt Zugang** zu elektronisch gespeicherten Daten **verschafft** und
- unter **Bereicherungsvorsatz** diese **Daten** selbst **verwendet**, veröffentlicht oder anderen zugänglich macht und
- **dabei Sicherheitsvorkehrungen** im Computersystem **überwindet** (zB Passwort, die Eingabe eines fremden Passwortes stellt hierbei schon ein „Überwinden“ dar)

Strafgesetzbuch (2)

§ 122 StGB Verletzung eines Geschäfts- oder Betriebsgeheimnisses

Bestraft wird

- wer ein Geheimnis verwertet,
- zu dessen Geheimhaltung er durch Gesetz verpflichtet ist und
- dessen Preisgabe geeignet ist, ein berechtigtes Interesse des Betroffenen zu verletzen

Strafmaß:

- bis 6 Monate od. 360 Tagsätze
- bei Bereicherungsvorsatz bis 1 Jahr od. 360 Tagsätze

§123 StGB Auskundschaften eines Geschäfts- und Betriebsgeheimnisses

Bestraft wird, wer derartige Geheimnisse vorsätzlich auskundschaftet um es zu verwerten oder anderen zur Verwertung zu überlassen. (bis 2 Jahre oder 360 TS)

§124 StGB

pönalisiert das Auskundschaften von Geschäfts und Betriebsgeheimnissen, bzw. die Weitergabe derselben zur Verwendung oder Verwertung im Ausland (bis 3 Jahre **und** 360 TS)

Aktuelle Entwicklungen iZmd EU-Datenschutz-Grundverordnung

DS-GVO

Highlights des konsolidierten Entwurfs

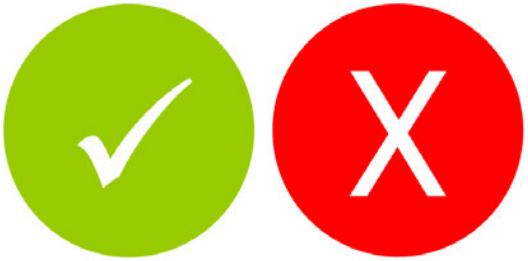
- (Pflicht zur Bestellung eines Datenschutzbeauftragten)
- Pflicht zur Durchführung von Folgenabschätzungen
- Erweiterte Dokumentationspflichten
- Pflicht zur Gestaltung von entsprechenden Prozessen um Betroffenenrechte bzw. Informationsrechte der Behörde entsprechen zu können
- Strafen bis zu 1.000.000 € oder 2% vom weltweiten Umsatz

Änderungen der Erwägungsgründe

ErwGr 29 → besonderer Schutz iZm mit der Verarbeitung von Daten über Kinder (neu ist hier die Definition von „Kind“ → bis zum vollendeten 13. Lebensjahr), insbesondere bei der Verarbeitung iZm mit Angeboten von Waren oder Dienstleistungen. → Einwilligung (Zustimmung der Eltern erforderlich), Verwendung einer kindgerechten Sprache iZm der Information über Zweck und Inhalt der Datenverarbeitung.

ErwGr 48 → wenn der Betroffene im Rahmen der Nutzung einer Datenanwendung seine Zustimmung zur Verwendung der ihn betreffenden Daten erteilt, so sind zur Darstellung des Verwendungsumfanges standardisierte ICONS zu verwenden. Dadurch soll für den Betroffenen erkennbar sein auf welcher Basis seine Daten nach dem Grundsatz von „Treu und Glauben“ verwendet werden. (Artikel 13 a + Anhang).

Änderungen der Erwägungsgründe



Dabei müssen unter Verwendung dieser Symbole Informationen bereitgestellt werden, ob durch die betroffene Anwendung:

a) mehr personenbezogene Daten erhoben werden, als für den jeweiligen Zweck der Verarbeitung erforderlich;

b) mehr personenbezogene Daten gespeichert werden, als für den jeweiligen Zweck der Verarbeitung erforderlich sind;

c) personenbezogene Daten zu anderen als den Zwecken verarbeitet werden, für die sie erhoben wurden;

d) personenbezogene Daten an gewerbliche Dritte weitergegeben werden;

e) personenbezogene Daten verkauft oder gegen Entgelt überlassen werden;

f) personenbezogene Daten verschlüsselt gespeichert werden.

Änderungen der Erwägungsgründe

ErwGr 53 aus dem „Recht auf Vergessenwerden“ wurde ein „Recht auf Löschung“ das Inhaltlich den bestehenden Bestimmungen des DSG zum Recht auf Richtigstellung bzw. Löschung entspricht.

ErwGr 55 „Datenportabilität“ → die bisherige Forderung nach einer verpflichtenden Bereitstellung von Daten zum Zwecke der Übertragung von Daten aus einer Anwendung in eine andere Anwendung (explizit erwähnt „soziale Netzwerke“) wurde daurch zu einer „SOLL“-Bestimmung.

ErwGr 58+59: Besondere Bestimmungen iZm mit Profiling, insbesondere im Zusammenhang mit deren Zulässigkeit. Generelle Erleichterungen bei Profiling auf Basis „pseudonymisierter“ Daten.

ErwGr 60 Besondere Pflichten des Auftraggebers sollen im Gesetz verankert werden, insbesondere iZm mit der erforderlichen Dokumentation, Maßnahmen zur Datensicherheit, Durchführung von Folgenabschätzungen, Einsetzung eines Datenschutzbeauftragten. Zudem sollen entsprechende Kontrollrechte der Aufsichtsbehörden verankert werden.

ErwGr 62 beschreibt ein Szenario, das dem bestehenden „Informationsverbundsystem“ nicht unähnlich ist (gemeinsam Verarbeitung durch mehrere Auftraggeber). Hierbei forderte die DS-GVO eine explizite Klärung der Aufgabenverteilung, sowie Klärung der Rechte und Pflichten jedes Beteiligten.

Änderungen der Erwägungsgründe

ErwGr 65 beschreibt eine erweiterte Protokollierungspflicht für alle Auftraggeber bzw. Dienstleister, die in vielen Fällen über die bisherigen Protokollierungsgepflogenheiten nach § 14 Abs 3 DSG hinausgehen.

ErwGr 67 die Verpflichtung zur Benachrichtigung bei Verletzungen des Datenschutzes beinhalten nunmehr auch die Pflicht zur Benachrichtigung der Aufsichtsbehörde binnen 72 Stunden.

ErwGr 75 stellt dem Auftraggeber eine weitere Person zur Seite, der diesen bei der Einhaltung der gesetzlichen Bestimmungen unterstützt (den Datenschutzbeauftragten). Für öffentliche Auftraggeber grundsätzlich verpflichtend, für private Auftraggeber bei

a. Verarbeitung von Daten von mehr als 5000 Personen im Kalenderjahr (Daten die sich in reinen Archivspeichern befinden sind hier nicht zu berücksichtigen)
b. Verwendung sensibler Daten als Kerntätigkeit
c. Datenverarbeitungsvorgängen, die als Kerntätigkeit ausgeübt werden und einer regelmäßigen und systematischen Überwachung bedürfen (dies bedarf wohl noch genauerer Spezifikation in Form eines delegierten Rechtsaktes)

ErwGr 75a erläutert die Anforderungen an einen Datenschutzbeauftragten:

- umfassende Kenntnisse des Datenschutzrechts und seiner Anwendung, einschließlich technischer und organisatorischer Maßnahmen und Verfahren;
- Beherrschung der fachlichen Anforderungen an den Datenschutz durch Technik, die datenschutzfreundlichen Voreinstellungen und die Datensicherheit;
- sektorspezifisches Wissen entsprechend der Größe des für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters und der Sensibilität der zu verarbeitenden Daten;
- die Fähigkeit, Überprüfungen, Konsultationen, Dokumentationen und Protokolldateianalysen durchzuführen;
- sowie die Fähigkeit, mit Arbeitnehmervertretungen zu arbeiten.

Änderungen im Gesetzestext

Artikel 3 →

- räumliche Anwendbarkeit auf die Verarbeitung personenbezogener Daten für die **Zwecke von Auftraggebern und Dienstleistern in der EU**
- unabhängig davon, ob die Verarbeitung tatsächlich in der EU stattfindet,
- sowie für die Verarbeitung von **in der EU ansässigen Personen** im Zusammenhang mit dem **Anbieten von Waren und Dienstleistungen,** sowie mit dem Ziel der **Überwachung** dieser Personen

Änderungen im Gesetzestext

Artikel 9 → die Gruppe der sensiblen Daten wurde erweitert:

- **Rasse oder ethnische Herkunft,**
- **politische Meinungen,**
- **religiöse oder philosophische Überzeugungen,**
- **sexuelle Orientierung oder Geschlechtsidentität**
- **Mitgliedschaft und Betätigung in einer Gewerkschaft**
- **genetischen oder biometrischen Daten**
- **Daten über die Gesundheit,**
- **Daten über das Sexualleben,**
- **Daten über verwaltungsrechtliche Sanktionen, Urteile, Straftaten oder mutmaßliche Straftaten, Verurteilungen oder damit zusammenhängende Sicherungsmaßregeln**

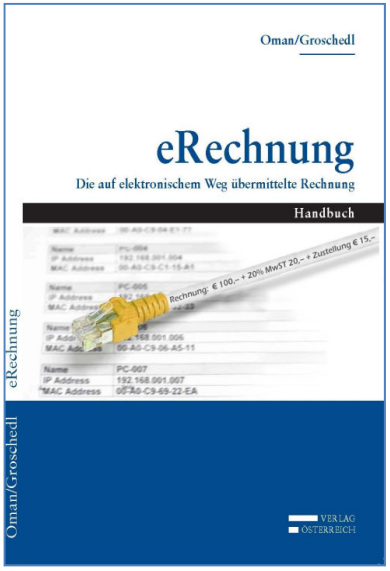
Änderungen im Gesetzestext

- Artikel 10a → verpflichtet die Auftraggeber zur Bereitstellung klarer und leicht verständlicher Informationen über die Verarbeitung der personenbezogenen Daten der betroffenen Person, das Recht auf Zugang, Berichtigung und Löschung ihrer Daten, das Recht auf Herausgabe von Daten, das Recht, dem Profiling zu widersprechen, das Recht auf Beschwerde bei der zuständigen Aufsichtsbehörde und Klageerhebung sowie das Recht auf Ersatz des Schadens, der durch eine rechtswidrige Verarbeitung entsteht.
- Artikel 12 → für das Recht auf Auskunft wird die Frist auf 40 Kalendertage verkürzt (bisher 8 Wochen)
- Artikel 14 → erweitert die Informationspflichten über Datenverarbeitungssysteme erheblich. Informationen über Datenverarbeitungssysteme müssen den Betroffenen zur Verfügung gestellt werden (insb. Zweck der Verarbeitung, Aufbewahrungsdauer, Übermittlungsempfänger, etc.).

Änderungen im Gesetzestext

- Artikel 20 → beschreibt den datenschutzrechtlichen Begriff „Profiling“ und die Voraussetzungen der Zulässigkeit von Profiling
- Artikel 22 → der Auftraggeber ist dazu verpflichtet, die Wirksamkeit der von ihm ergriffenen Datensicherheitsmaßnahmen nachzuweisen.
- Artikel 28 → Enthält umfassende Dokumentationspflichten für Auftraggeber und Dienstleister
- Artikel 30 → enthält Bestimmungen über die Durchführung von Datenschutz-Folgenabschätzungen (hier sind noch weitere Rechtsakte zur detaillierten Umsetzung erforderlich).
- Artikel 32 → beschreibt wann eine derartige Folgenabschätzung durchzuführen ist.
  - insb. Anzahl verarbeiteter Daten,
  - Verarbeitung sensibler Daten, Profiling,
  - Verarbeitung von Standortdaten,
  - Daten iZm mit der Erbringung von Gesundheitsdiensten.

DANKE !



Fragen...

- gerne jetzt

  oder

- per eMail:

  markus.oman@opp-beratung.com

  oder

- per Tel.: 06991-2518089

  oder