WU Informationsveranstaltung

Die EU Datenschutz-Grundverordnung im Überblick

bkp
RECHTSANWÄLTE

Daten im Universitätsalltag

Neuer Datenschutz Rechtsrahmen

- EU Datenschutz-Grundverordnung
  - *„VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG“*
  - Gültig ab 25.05.2018
  - Neuer, einheitlicher europäischer Rechtsrahmen
  - Direkt anwendbar
  - Zahlreiche „Öffnungsklauseln“, die ergänzende nationale Regelungen erlauben

- Datenschutz-Anpassungsgesetz 2018
  - Kundgemacht am 31.07.2017 im BGBl. I Nr. 120/2017, abrufbar im RIS unter https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2017_I_120/BGBLA_2017_I_120.html
  - Anpassung des derzeit geltenden „DSG 2000“ (künftig „DSG“)

Kernpunkte der DSGVO

- Mehr Rechte für die betroffenen Personen
  - Mehr Transparenz
  - Erweiterte Informationspflichten
  - Recht auf „Vergessenwerden“
  - Recht auf Mitnahme der Daten, Datenportabilität
- Besserer Schutz der persönlichen Daten
  - Datenschutz durch Technik – „privacy by design“
  - Datenschutzfreundliche Voreinstellungen – „privacy by default“
- Dokumentationspflichten
  - „Persönliches Datenverarbeitungsregister“
  - Datenschutzfolgenabschätzung
  - Meldepflicht bei Datenschutzverstößen
- Größere Eigenverantwortung der Unternehmen – „Accountability“
  - Bestellung eines Datenschutzbeauftragten
- Förderung von Zertifizierungen, Datenschutzsiegeln und -prüfzeichen
- Strenge Sanktionen
  - Geldbußen bis zu 20 Mio EUR oder 4% des weltweiten Jahresumsatzes

Gliederung der DSGVO

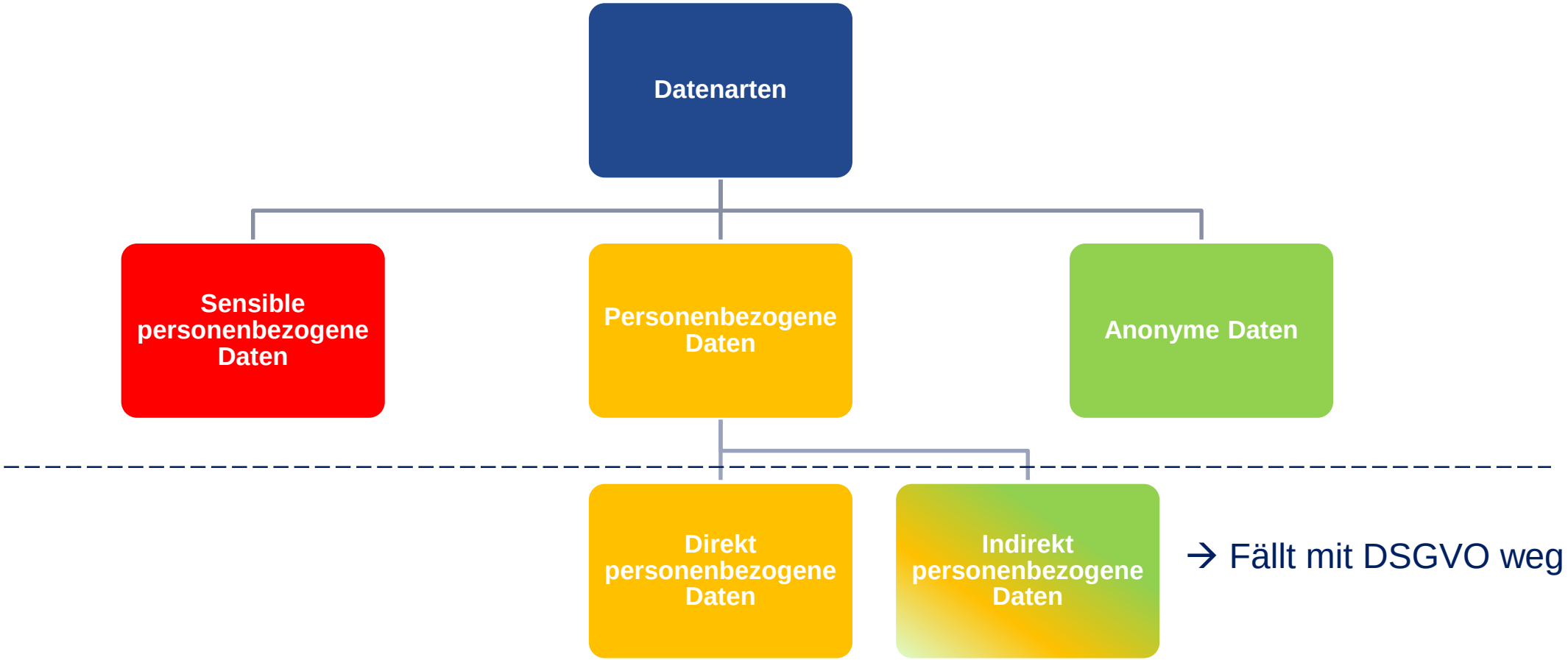
- Kapitel I Allgemeine Bestimmungen
  - Anwendungsbereich
  - Begriffsbestimmungen
- Kapitel II Grundsätze
- Kapitel III Rechte der betroffenen Person
- Kapitel IV Verantwortlicher und Auftragsverarbeiter
  - Allgemeine Pflichten
  - Sicherheit personenbezogener Daten
  - Datenschutz-Folgenabschätzung
  - Datenschutzbeauftragter
  - Verhaltensregeln und Zertifizierung
- Kapitel V Übermittlungen personenbezogener Daten an Drittländer / internat. Organisationen
- Kapitel VI Unabhängige Aufsichtsbehörden
- Kapitel VII Zusammenarbeit und Kohärenz
- Kapitel VIII Rechtsbehelfe, Haftung und Sanktionen
- Kapitel IX Vorschriften für besondere Verarbeitungssituationen
- Kapitel X Delegierte Rechtsakte und Durchführungsrechtsakte
- Kapitel XI Schlussbestimmungen

- 88 Seiten
- 173 Erwägungsgründe
- 99 Artikel
- Viele unbestimmte Begriffe
- Nähere Ausgestaltung teilweise der EU Kommission und dem Europ. Datenschutzausschuss überlassen (ua. Erstellung von Leitlinien und Empfehlungen).

Welche Daten sind geschützt?

- Automatisierte Verarbeitung **personenbezogener Daten**
  - Informationen, die sich auf eine **identifizierte** oder **identifizierbare natürliche Person** („betroffene Person“) beziehen
    - Sämtliche Informationen über eine Person (z.B. Name, Wohnort, Geburtsdatum, Telefonnummer, Einkommen, Sozialversicherungsnummer, Krankenstände,…)
    - unabhängig davon, ob privat oder beruflich, vertraulich oder nicht!
  - Besondere Kategorien personenbezogener Daten (bisher **„Sensible Daten**“)
    - Daten über rassische und ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten, Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung
    - Verwendung nur unter strengeren Voraussetzungen zulässig (vgl. Art 9 DSGVO)
  - **Anonyme Daten** sind datenschutzrechtlich nicht relevant!
  - **Juristische Personen** (wie GmbH, AG) durch DSGVO nicht erfasst
    - Aber z.B. Sachbearbeiter, Organe einer juristischen Person
    - in Ö: Jurist. Person hat weiterhin Grundrecht auf Datenschutz (?)

Welche Daten sind geschützt?



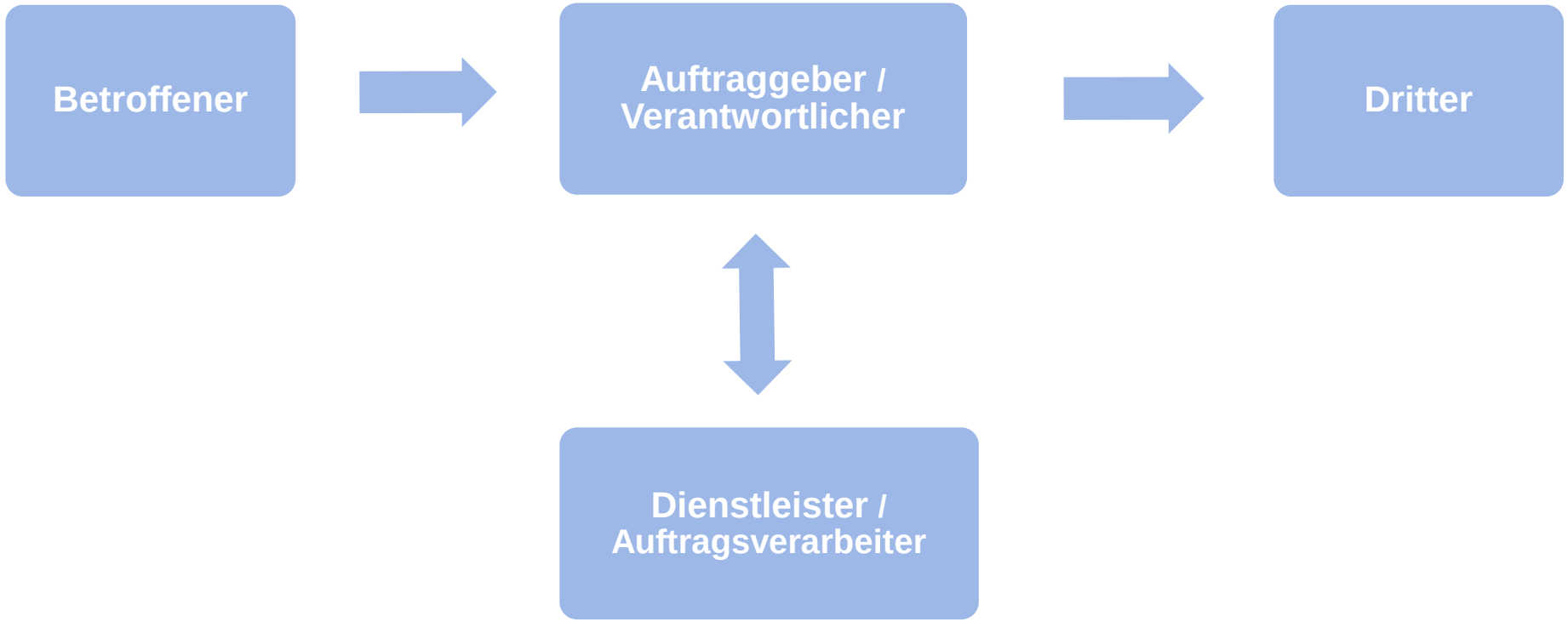
Welche Daten sind geschützt?

- Automatisierte Verarbeitung

- Nicht automatisierte Verarbeitung in Form eines Dateisystems
  - Nach bestimmten Kriterien strukturierte Sammlung personenbezogener Daten

- „Haushaltsausnahme“: Datenverarbeitung zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten ausgenommen
  - z.B. private Aktivitäten in sozialen Medien

Die datenschutzrechtlichen Akteure



Grundsätze für die Datenverarbeitung (Art 5)

- wie bisher gelten die allgemeinen Grundsätze der „Rechtmäßigkeit“, Verarbeitung nach „Treu und Glauben“, „Transparenz“
- Zweckbindungsgrundsatz
  - Für festgelegte, eindeutige und legitime Zwecke erhoben
  - Neu: Daten dürfen für andere, kompatible Zwecke weiterverwendet werden
- Grundsatz der „Datenminimierung“ – Wesentlichkeitsgrundsatz
  - Nur Daten verarbeiten, die für Zweck notwendig sind
- Grundsatz der sachlichen „Richtigkeit“ und Aktualität
- Grundsatz der „Speicherbegrenzung“
  - Daten nur so lange in personenbezogener Form aufbewahren, wie erforderlich
  - Gesetzliche Aufbewahrungsfristen in diversen Materiengesetzen (ua. Steuerrecht, Buchhaltung)
- Grundsatz der Datenintegrität und Vertraulichkeit
  - Pflicht angemessene Datensicherheitsmaßnahmen zu treffen
- Rechenschaftspflicht
  - Der Verantwortliche muss die Einhaltung der Grundsätze nachweisen

Rechtmäßigkeit der Verarbeitung (Art 6 ff)

- Verbot mit Erlaubnisvorbehalt!
- Mögliche Rechtsgrundlagen
  - **Einwilligung**
  - Erfüllung eines **Vertrags** mit der betroffenen Person
  - Erfüllung einer **gesetzlichen Verpflichtung**
  - **Berechtigte Interessen** des Verantwortlichen oder eines Dritten (Interessenabwägung)
    - Gilt nicht für sensible Daten!
  - Aufgabe im **öffentlichen Interesse**
  - Verarbeitung zu **wissenschaftlichen Forschungszwecken**
    - Vgl. §§ 7, 8 DSG neu (ähnlich §§ 46, 47 DSG 2000)

Einwilligung (Art 7)

- *„jede **freiwillig** für den bestimmten Fall, **in informierter Weise** und unmissverständlich angegebene Willensbekundung in Form einer **Erklärung** oder einer sonstigen eindeutigen **bestätigenden Handlung**, mit der die betroffene Personen zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist“*
- freiwillig
  - Möglichkeit Einwilligung zu verweigern, ohne Nachteile zu erleiden
  - Eine Einwilligung bietet keine Rechtsgrundlage für die Verarbeitung, wenn zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen ein klares Ungleichgewicht besteht
  - Kopplungsverbot
- in informierter Weise
- schriftliche / elektronische (z.B. Checkbox) / mündliche Erklärung
  - Aktives Tun erforderlich
  - Schweigen, vorab angeklickte Checkbox oder Untätigkeit der Betroffenen ist keine Einwilligung
- verständlich, leicht zugänglich, in klarer und einfacher Sprache
- jederzeit widerrufbar
- Verantwortliche trägt die Beweislast für die Erteilung der Einwilligung

Rechte der Betroffenen (Art 12 - 23)

- Informationspflicht gegenüber Betroffenen (Art 13)
- Auskunftsrecht (Art 15)
- Recht auf Berichtigung (Art 16)
- Recht auf Löschung und „Vergessenwerden“ (Art 17)
- Recht auf Einschränkung der Verarbeitung (Art 18)
- Mitteilungspflicht (Art 19) neu!
  - jede Berichtigung oder Löschung bzw. Einschränkung der Verarbeitung ist nach Möglichkeit jedem Empfänger der Daten mitzuteilen
- Recht auf Datenübertragbarkeit (Art 20) neu!
  - Recht des Betroffenen, seine Daten in einem strukturieren, gängigen und maschinenlesbaren Format zu erhalten
- Widerspruchsrecht (Art 21)
- Automatisierte Entscheidungen im Einzelfall u. Profiling (Art 22)

Informationspflicht (Art 13 und 14)

- Information der betroffenen Person bei Erhebung der Daten
  - Namen und Kontaktdaten des Verantwortlichen und eines (allfälligen) Datenschutzbeauftragten
  - Zwecke der Datenverarbeitung
  - **Rechtsgrundlagen**
    - Erläuterung der berechtigen Interessen des Verantwortlichen
  - **Allfällige Empfänger / Empfängerkategorien**
  - Hinweis auf Datenübermittlung in Drittländer ohne angemessenes Datenschutzniveau
  - **Speicherdauer** oder Kriterien für Bestimmung der Speicherdauer
  - Betroffenenrechte
  - Beschwerderecht bei der Aufsichtsbehörde
  - Gesetzliche oder vertragliche Verpflichtung oder Notwendigkeit zur Bereitstellung der Daten und Folgen der Nichtbereitstellung der Daten
- Vor geplanter Weiterverarbeitung zu einem anderen (kompatiblen) Zweck erneute Informationspflicht!

➡ Prüfen wie Informationspflichten in der Praxis umgesetzt werden können

Auskunftsrecht (Art 15)

bkp RECHTSANWÄLTE

Neu: DSGVO

- Mündliches, schriftliches oder elektronisches Auskunftsersuchen
- Auskunft über
  - Verarbeitungszwecke
  - Datenkategorien
  - Empfängerkategorien
  - **Speicherdauer**
  - Herkunft
- Hinweis auf Betroffenenrechte, einschließlich Beschwerderecht
- Frist: 1 Monat (max. 3 Monate)
- Strafen: bis zu EUR 20 Mio./ 4% des letztjährigen weltweiten Jahresumsatzes

⇒ Geeignete Prozesse implementieren

Bisher: DSG 2000

- Schriftliches Auskunftsersuchen (mündlich nur mit Zustimmung)
- Auskunft über
  - Verarbeitungszweck
  - Verarbeitete Daten
  - Empfängerkreise
  - Herkunft
  - Rechtsgrundlagen
- Frist: max. 8 Wochen
- Strafen: bis zu EUR 500,-

Recht auf Löschung / „Vergessenwerden“ (Art 17)

- Daten sind unverzüglich zu löschen, wenn
  - Sofern die Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet werden, nicht mehr notwendig sind
  - betroffene Person ihre Einwilligung widerruft und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung
  - betroffene Person hat Widerspruch eingelegt (vgl. Art 21).
  - Daten unrechtmäßig verarbeitet wurden
- Neu: Wurden Daten vom Verantwortlichen veröffentlicht, muss er nach Möglichkeit Dritte, welche die veröffentlichen Daten verarbeiten (z.B. verlinken, kopieren) über das Löschungsbegehren informieren.
- Ausnahmen:
  - freie Meinungsäußerung,
  - gesetzliche Verpflichtung zur Verarbeitung (insb. Aufbewahrungspflichten)
  - öffentliche Interessen einschließlich wissenschaftliche Forschungszwecke und
  - zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Datenschutz durch Technik und Voreinstellungen (Art 25)

- „**Privacy by design**“: Geeignete technische und organisatorische Maßnahmen wie z.B. Pseudonymisierung, um Datenschutzgrundsätze wie Datenminimierung wirksam umzusetzen und Rechte der Betroffenen zu schützen
  - Berücksichtigung des Stands der Technik, der Implementierungskosten, Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risken

- „**Privacy by default**“: Datenschutzfreundliche Voreinstellungen, damit nur jene Daten verarbeitet werden, deren Verarbeitung für den jeweiligen Zweck erforderlich ist.
  - Bezieht sich auf Menge der Daten, Umfang der Verarbeitung, Speicherfrist und Zugänglichkeit der Daten
  - Daten dürfen ohne Eingreifen der Person nicht einer unbestimmten Zahl von Personen zugänglich gemacht werden
  - Verpflichtung gilt ohne Rücksicht auf wirtschaftliche Vertretbarkeit oder Unternehmensgröße

➡ Handlungsbedarf / Verbesserungsmöglichkeiten prüfen!

Auftragsverarbeiter (Art 28)

- Bisher „Dienstleister“
- Verantwortlicher darf nur Auftragsverarbeiter heranziehen, die „**hinreichend Garantien**“ bieten, dass geeignete **technische und organisatorische Maßnahmen** durchgeführt werden
- Abschluss eines schriftlichen (bzw. elektronischen) **Dienstleistervertrags**
  - Gegenstand und Dauer sowie Art und Zweck der Verarbeitung
  - Art der personenbezogenen Daten, Kategorien betroffener Personen
  - Rechte und Pflichten
- **Subdienstleister** nur mit Zustimmung oder Einspruchsmöglichkeit des Verantwortlichen
- Haftung des Dienstleisters für seine Subdienstleister
- Haftung des Verantwortlichen für alle seine Dienstleister
- Dienstleister daher sorgfältig auswählen!

➡ Bestehende Dienstleisterverträge prüfen und allenfalls anpassen, neuer Mustervertrag, Verzeichnis der Dienstleisterverträge erstellen

Verzeichnis von Verarbeitungstätigkeiten (Art 30)

- Jeder Verantwortliche und jeder Auftragsverarbeiter muss ein Verzeichnis aller Verarbeitungsvorgänge führen
- **„persönliches Datenverarbeitungsregister“ statt DVR-Meldungen**
  - Name und Kontaktdaten des Verantwortlichen und eines (allfälligen) Datenschutzbeauftragten
  - Zwecke der Verarbeitung
  - Kategorien betroffener Personen und Daten
  - Empfängerkategorien
  - Fristen für die Löschung (neu)
  - Beschreibung der Datensicherheitsmaßnahmen
- Zurverfügungstellung des Verzeichnisses an die Aufsichtsbehörde auf Anfrage

zu prüfen, welche Verarbeitungstätigkeiten durchgeführt werden,
in Verarbeitungsverzeichnis der WU aufzunehmen

Meldepflicht bei Datenmissbrauch

bkp RECHTSANWÄLTE

www.kleinezeitung.at/steiermark/chronik/4899864/Nicht-gehackt_Datenleck-an-Grazer-Uni_472-Gigabyte-gestohlen

Startseite › Steiermark › Chronik

NICHT GEHACKT

Datenleck an Grazer Uni: 47,2 Gigabyte gestohlen

Daten aus den Jahren 2011 bis 2013 wurden offenbar vom Computer einer Professorin entwendet, darunter Prüfungsdaten und persönliche Daten. Anzeige wurde erstattet. *Norbert Swoboda*

18.18 Uhr, 07. Jänner 2016

Keine ruhigen Tage erlebte die Universität Graz zum Jahreswechsel. Beim großen Treffen des Computer Chaos Club in Hamburg mit 15.000 Teilnehmern wurde auch ein Fallbeispiel gezeigt, das in Graz für Erschrecken sorgte: Offenbar wurden 47,2 Gigabyte von der Universität Graz an Daten entwendet, darunter auch Prüfungsnoten und andere private Daten.

Daten an Uni Graz entwendet © Jürgen Fuchs

"Es gab auch ein Bekennerschreiben, das uns zugespielt wurde", erklärte Vizerektor Peter Riedler, der unter anderem auch für die IT der Universität zuständig ist. Am 28. Dezember wurde das Datenleck in Graz bekannt. Relativ rasch habe

MEIST GELESEN

Datenleck bei der Uni Basel fördert persönliche Dokumente ins Netz

Datenleck an der Uni Göttingen betraf rund 26.000 Studenten [Update]

Datenleck: 400.000 vertrauliche Schülertests im Internet aufgetaucht

"Die Presse" exklusiv: Geheime Testergebnisse österreichischer Schüler sowie die E-Mail-Adressen von 37.000 Lehrern liegen ungeschützt auf einem rumänischen Internetserver. Das zuständige Bundesinstitut für Bildungsforschung wusste es – und handelte nicht.

Meldepflicht bei Datenmissbrauch

bkp RECHTSANWÄLTE

SPIEGEL ONLINE DER SPIEGEL SPIEGEL TV Anmelden

Online-Speicherdienst

Dropbox räumt riesiges Datenleck ein

Mehr als 68 Millionen Passwörter sind betroffen: Ein Datenleck beim Online-Speicherdienst Dropbox aus dem Jahr 2012 hat größere Dimensionen als bisher bekannt. Jetzt sollen die Nutzer aktiv werden.

Hackerangriff von 2013 traf alle drei Mrd. Yahoo-Nutzer

Der Hackerangriff auf den US-Internetanbieter Yahoo im Jahr 2013 hat nach Angaben des Unternehmens alle drei Milliarden Nutzerinnen und Nutzer getroffen - und somit zwei Milliarden mehr als bisher bekannt. Die Betroffenen würden per E-Mail informiert, teilte das Unternehmen gestern mit. Zugleich versicherte Yahoo, dass die Hacker weder Passwörter noch Bankdaten entwendet hätten.

...on hatte Yahoo Anfang ... das Ausmaß und die ...n einmal überprüft.

Datenleck

Mehr als 100 Millionen LinkedIn-Passwörter gehackt

Rund vier Jahre nach dem Datenleck bei LinkedIn muss das Onlinenetzwerk zugeben, dass wesentlich mehr Passwörter betroffen sind als zunächst angegeben.

Seitensprung-Plattform zahlt nach Datenleck 11,2 Millionen Dollar

17. Juli 2017, 08:22

54 POSTINGS

Die Webseite Ashley Madison einigt sich mit Nutzern, deren persönliche Informationen ins Netz gelangten

Vorgehen bei Datenmissbrauch an der WU

- Betroffene sind von der WU zu informieren, wenn bekannt wird, dass ihre Daten *systematisch* und *schwerwiegend unrechtmäßig* verwendet wurden und den Betroffenen ein Schaden droht (§ 24 DSG 2000).

- Innerhalb der WU festgelegter Prozess:
  - Bei tatsächlich erfolgten Datenmissbrauch/Verdacht
  - A.) Unverzügliche Information der/des Vorgesetzten und Kontaktaufnahme mit der/dem Datenschutzbeauftragten durch die/den Vorgesetzten.
  - B.) Bei Nichterreichen der/des Vorgesetzten bzw. der/des Datenschutzbeauftragten Information an die Rechtsabteilung.
  - Bei Kontaktversuchen durch Medien: Verweis an Involviertes Rektoratsmitglied und die/den Pressesprecher/in zu verweisen.
  - https://www.wu.ac.at/datenschutz/

Meldepflicht bei Datenmissbrauch (Art 33)

- Meldepflicht bei **jedem** Datenmissbrauch an Datenschutzbehörde binnen 72 Stunden, außer es besteht voraussichtlich kein Risiko für die Rechte und Freiheiten betroffener Personen.
  - Art der Verletzung
  - Kategorien und Zahl der betroffenen Personen
  - Kategorien und Zahl der betroffenen Datensätze
  - Wahrscheinliche Folgen der Verletzung
  - Maßnahmen zur Behebung bzw. zur Schadensminderung
- Unverzügliche Information der Betroffenen oder öffentliche Bekanntmachung, sofern hohes Risiko für die persönlichen Rechte der Betroffenen
- Verpflichtende Dokumentation aller Verletzungen

➡ Bestehenden Prozess bei Datenmissbräuchen anpassen

Datenschutz-Folgenabschätzung (Art 35)

- Pflicht zur Datenschutz-Folgenabschätzung
  - wenn insbesondere bei Verwendung neuer Technologien aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung ein hohes Risiko für die Rechte und Freiheiten von natürlichen Personen besteht
    - Bei systematischer und umfassender Bewertung persönlicher Aspekte durch automatisierte Verarbeitung einschließlich Profiling
    - Umfangreiche Verarbeitung sensibler Daten und Daten über Straftaten
    - Systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche
- **Mindestinhalt**: Beschreibung der Verarbeitungsvorgänge, Zwecke, Notwendigkeit, Verhältnismäßigkeit, Bewertung der Risken und Abhilfemaßnahmen
- Konsultation mit der Aufsichtsbehörde, wenn Folgenabschätzung ergibt, dass eine Verarbeitung ohne Risiko mindernde Maßnahmen ein hohes Risiko zur Folge hätte.

Bestellung eines Datenschutzbeauftragten (Art 39)

- **Behörden** oder öffentliche Stellen müssen zwingend eine/n Datenschutzbeauftragte/n bestellen
- Sonstige Organisationen / Unternehmen, wenn deren Kerntätigkeit eine **umfangreiche regelmäßige und systematische Überwachung** von Betroffenen oder eine umfangreiche Verarbeitung **sensibler oder strafrechtlich relevanter Daten** beinhaltet
- Datenschutzbeauftragte/r ist in alle mit dem Datenschutz zusammenhängenden Fragen einzubinden
- Unterrichtung und **Beratung** des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten über Pflichten nach der DSGVO
- **Überwachung** der Einhaltung der Datenschutzvorschriften
- Beratung bei Datenschutz-Folgenabschätzung und Überwachung der Durchführung
- Sensibilisierung und **Schulung** der Mitarbeiter
- **Ansprechperson** der Aufsichtsbehörde, Zusammenarbeit mit der Aufsichtsbehörde

Rechtsbehelfe, Haftung und Sanktionen (Art 77 - 84)

- Recht auf **Beschwerde** bei seiner Aufsichtsbehörde (Wohnsitz, Arbeitsplatz)
- Recht auf wirksamen **gerichtlichen Rechtsbehelf**
  - Klage gegen Verantwortlichen oder Auftragsverarbeiter an dessen Sitz oder wahlweise am Aufenthaltsort des Betroffenen
- **Schadenersatzforderungen**
  - Jeder an der Verarbeitung beteiligte Verantwortliche haftet solidarisch für den gesamten Schaden
  - Haftung auch für Verschulden eines Dienstleisters
  - Beweislastumkehr
    - Nachweis, dass er in keinerlei Hinsicht für den Schaden verantwortlich ist
- **Geldbußen**
  - bis zu **20 Mio. EUR** oder **4% des gesamten weltweit erzielten Jahresumsatzes**
  - derzeit nach DSG 2000 bis zu 25.000 EUR
  - Bemessung der Geldbuße im Einzelfall nach Art, Schwere und Dauer des Verstoßes, Schadenshöhe, Verschulden etc.
  - Ausnahmen für Behörden und öffentliche Stellen

Fragen?

Weitere Datenschutz-Schulungen an der WU

- Thematischer Schwerpunkt: wissenschaftlicher Bereich, akademische Einheiten
  - Mittwoch, 20.12.2017, 09:00 bis 13:00 Uhr oder
  - Freitag, 12.01.2018, 09:00 bis 13:00 Uhr

- Thematischer Schwerpunkt: Dienstleistungseinrichtungen
  - Dienstag, 23.01.2018, 09:00 bis 13:00 Uhr oder
  - Mittwoch, 31.01.2018, 09:00 bis 13:00 Uhr

Danke für Ihre Aufmerksamkeit!

Georg Fellner

Brauneis Klauser Prändl Rechtsanwälte GmbH
Bauernmarkt 2, 1010 Wien
T + 43.1.532 12 10
F + 43.1.532 12 10 20
E g.fellner@bkp.at
datenschutz@wu.ac.at