Österreich - die EU-Datenschutzoase für Konzerne?

Hans G. Zeger, ARGE DATEN

Hamburg, IBS, 20. März 2014

Die ARGE DATEN als PRIVACY-Organisation

Aktivitäten der ARGE DATEN

Öffentlichkeitsarbeit, Informationsdienst:

- Web-Service: 60-80.000 Besucher/Monat
- Newsletter: rund 4.500 Abonnenten
- 2013: rund 500 Medienanfragen/-berichte

Mitgliederbetreuung Datenschutzfragen

- 2013: ca. 600 Datenschutz-Anfragen

Rechtsschutz, PRIVACY-Services

- 2013: in ca. 200 Fällen Mitglieder in Verfahren vertreten

Zahl der betreuten Mitglieder

- aktuell: ca. 15.000 Personen

Studien- und Beratungsprojekte

A-CERT - Zertifizierungsdienstleister gem. SigG

Datenschutz ist nicht der Schutz von Daten vor Menschen, sondern die **Sicherung** des **Grundrechts** auf **Privatsphäre**

ARGE DATEN

- **Datenschutz in Österreich**
- **Crashkurs DSG 2000**
- Registrierungsverfahren
- Standardanwendung Konzern
- Internationaler Datenverkehr

ARGE DATEN

© E-Commerce 2014

Entwicklung zum DSG 2000

1978 erstes Datenschutzgesetz - DSG (BGBl. Nr. 565/1978)
(Geltung 1.1.1980-31.12.1999)

1995 EG-Datenschutzrichtlinie 95/46/EG

1999 Datenschutzgesetz - DSG 2000 (BGBl. I Nr. 165/1999)

Wichtige Änderungen zum DSG 2000 (Auswahl)

2001 Euro-Umstellung der Verwaltungsstrafen (BGBl. I Nr. 136/2001)
2005 "Tsunami"-Bestimmung (BGBl. I Nr. 13/2005)
2008 Änderungen in Verfassungsbestimmungen (BGBl. I Nr. 2/2008)
2009 DSG 2000 - Novelle 2010 (BGBl. I Nr. 133/2009)
2012 Verwaltungsgerichtsbarkeits-Novelle 2012 (BGBl. I Nr. 51/2012)
2013 DSG 2000 - Novelle 2013 (BGBl. I Nr. 57/2013)
2013 DSG 2000 - Novelle 2014 (BGBl. I Nr. 83/2013)
20?? EU - Neuordnung des Datenschutzes

DSG 2000 - Grundlagen

Umsetzung der EU-Richtlinie "Datenschutz" (1995)

soll Privatsphäre (Art.1 Abs.1) und
Informationsaustausch innerhalb der EU (Art.1 Abs.2) sichern

Art. 1 Abs. 1 "Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten."

Art. 1 Abs. 2 "Die Mitgliedstaaten beschränken oder untersagen nicht den freien Verkehr personenbezogener Daten zwischen Mitgliedstaaten aus Gründen des gemäß Absatz 1 gewährleisteten Schutzes."

EU-RL gilt nur für "natürliche Personen"
DSG 2000 auch für "juristische und sonstige Personen"
damit vertritt Österreich EU-weit eine **exotische** Position

Bestimmungen betreffen alle Verwendungsformen persönlicher Daten, nicht nur automatisiert verarbeitete Daten

ARGE DATEN
© E-Commerce 2014

DSG 2000 § 1 (Verfassungsbestimmung):

"jede Verwendung persönlicher Daten ist verboten"

umfassender Geheimhaltungsanspruch

Grundlage ist Art. 8 EMRK ("Achtung des Privatlebens")

Einschränkungen des Verbots
(= Nutzungsmöglichkeiten für Daten):

- mit der Zustimmung des Betroffenen
- zur Vollziehung von Gesetzen (gesetzlichen Verpflichtungen)
- zur Wahrung überwiegender Interessen Auftraggeber/Dritter
- bei "allgemeiner" Verfügbarkeit von Daten
- bei lebenswichtigen Interessen des Betroffenen/Dritter

Das DSG 2000 - Crash-Kurs für Profis

- Österreich hat ein Bundes- + 9 Landesdatenschutzgesetze
- Geheimhaltung ist im DSG 2000 verfassungsrechtlich verankert
- Betroffenenrechte ("subjektive" Rechte) sind innerhalb von fixen Fristen zu erfüllen
- eigene Sprachschöpfungen:
  Auftragsdatenverarbeiter ⇨ Dienstleister
  Datenverarbeitung ⇨ Datenanwendung
  Daten mit bestimmbaren Personenbezug ⇨ "indirekt" personenbezogene Daten
  "sensible" Datenanwendungen, die nicht sensibel genannt werden ⇨ besonders schutzwürdige Daten
- Daten juristischer Personen sind wie Daten natürlicher Personen geschützt (gilt nicht bei sensiblen Daten)
- Anspruch auf immateriellen Schadenersatz

Das DSG 2000 - Crash-Kurs für Profis II

- Konstruktion des "Informationsverbundes": gemeinsame Datenverwendung verschiedener österreichischer Auftraggeber
- Sonderregelung für Datenverwendung zu "Verständigungszwecke"
- ausführliche Regelung zur Videoüberwachung
- Grundsatz der Meldepflicht mit Ausnahmen
  aber: Genehmigungspflicht bei besonders "heiklen" Datenanwendungen (⇨ "Vorabkontrollverfahren")
- wesentlichste Ausnahme von Meldepflicht für Unternehmen sind "Standardanwendungen" (werden per Verordnung vorgegeben)
- für internationalen Datenverkehr gilt Genehmigungspflicht mit Ausnahmen
- sehr moderate Verwaltungsstrafen (max. 25.000,- Euro)
- komplexes (kompliziertes) System der Zuständigkeit

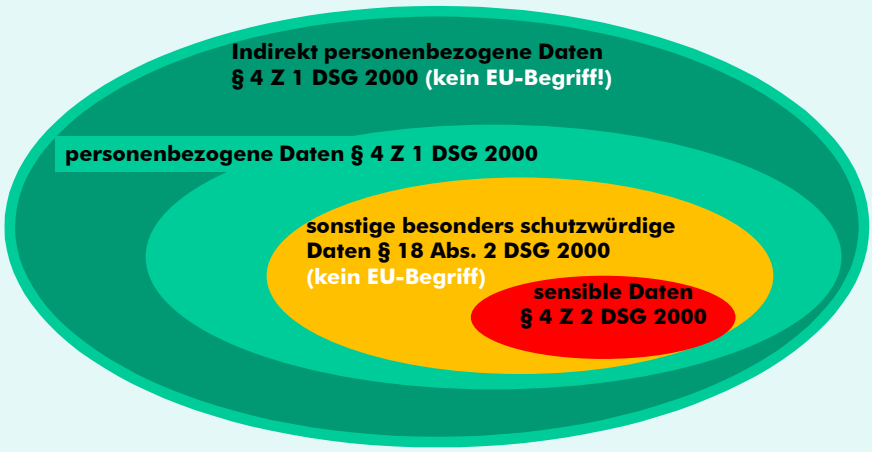
Das DSG 2000 - Crash-Kurs für Profis III

- **Datenschutzbehörde (bis 31.12.2013 Datenschutzkommission)**
  Melde- und Genehmigungsstelle für Registrierung und internationalen Datenverkehr
  Aufsichtsstelle für öffentliche Auftraggeber + Datenanwendungen auf Grund von Gesetzen
  zuständig für Beschwerden Betroffener zu Auskunftsbegehren für alle Auftraggeber + zu allen anderen Punkten im öffentlichen Bereich
  Ombudsstelle für alle Arten vermuteter Datenschutzverletzungen (für private Datenverarbeiter können jedoch nur Empfehlungen abgegeben werden)
  keine Strafbefugnis!

Das DSG 2000 - Crash-Kurs für Profis IV

- **Bundesverwaltungsgerichtshof (BVwG, seit 1.1.2014)**
  Beschwerdeinstanz gegen Entscheidungen der Datenschutzbehörde
  nicht mit dem VwGH verwechseln!
- **16 Landesgerichte**
  zuständig für Beschwerden Betroffener soweit diese nicht in den Zuständigkeitsbereich der Datenschutzbehörde fallen
  Landesgerichte nicht mit Bundesländern ident!
- **120 (ca.) Strafbehörden**
  zuständig für Verwaltungsstrafen nach DSG 2000
- **9 Landesverwaltungsgerichte (seit 1.1.2014)**
  zuständig für Beschwerden gegen Strafbehörden

Personenbezogene Daten



Was ist ein Informationsverbundsystem (IVS)? (§ 50)

gemeinsame Verwendung von Daten in einer DA durch mehrere [österreichische] Auftraggeber

geeigneter Betreiber ist zu bestellen

Betreiber ist zwecks Eintrag im DVR zu melden

Betreiber hat Auskünfte über Auftraggeber zu geben (12 Wochenfrist!) es können weitere Auftraggeberpflichten an den Betreiber abgetreten werden

Meldepflichten des Informationsverbundsystems können an Betreiber formlos übertragen werden (Abs. 2)

Erleichterungen der Meldung zusätzlicher Teilnehmer an Informationsverbundsystem: es genügt Verweis auf andere Meldung (Abs. 2a)

Stand lt. DVR-Online: 103 Anwendungen gemeldet, davon ca. 80% aus dem öffentlich-rechtlichen Bereich, 20% private

Dienstleister im Sinne des DSG 2000 (§§ 10f)

- Dienstleistung liegt vor, wenn ein Verantwortlicher jemanden Dritten für die Durchführung bestimmter Verarbeitungsaufgaben betraut
- Geeignete Vereinbarungen sind zu treffen
- Vereinbarungen sind zu überprüfen/überwachen ["überzeugen"] ⇨ wie bei Cloud-Computing umsetzen?
- Meldepflicht an DSK bei Datenverarbeitungen des öffentlichen Bereichs, die der Vorabkontrolle unterliegen (z.B. bei Verwendung von Gesundheitsdaten), jedoch keine Meldepflicht bei verbundenen Unternehmen
- Subdienstleister nur mit Billigung des Auftraggebers

Schriftliche Vereinbarung notwendig!
(§ 11 Abs. 2 DSG 2000)

Datenschutz in Österreich

Crashkurs DSG 2000

Registrierungsverfahren

Standardanwendung Konzern

Internationaler Datenverkehr

DSG 2000 - Standard- und Musterverordnung

Registrierung von Datenanwendungen (§§ 16ff)

- Grundsätzlich besteht für jede Datenanwendung Registrierungspflicht, aber: es sind nicht alle Datenanwendungen zu registrieren (§ 17)
- Jede Registrierung erfolgt für eine bestimmte Datenanwendung, für bestimmte Datenarten, bestimmte Personengruppen und bestimmte Zwecke (§ 17)
- Verordnungsermächtigung des Bundeskanzlers: kann Datenanwendungen zum "Standard" zu erklären, die
  - von einer großen Anzahl von Auftraggebern in gleichartiger Weise vorgenommen werden und
  - angesichts des Zwecks und der Datenarten die Gefährdung von Geheimhaltungsinteressen Betroffener unwahrscheinlich ist. (§ 17 Abs. 2 Z 6)

⇨ **Datenanwendung ist Registrierungsfrei**

- derzeit gültig: StMV 2004 BGBl. II 312/2004

DVR – Wozu? und Warum?

Was muss gemeldet werden (§ 19 DSG 2000)

- Wer (Name und Anschrift des Auftraggebers),
- warum (Rechtsgrundlage),
- wozu (Zweck der Datenanwendung),
- welche Daten,
- von welchen Personen (Betroffenenkreise) verarbeitet und
- an wen diese gegebenenfalls übermittelt (Empfängerkreise) werden.

Betrieb einer gemeldeten Datenanwendung unmittelbar nach Meldung bzw. nach Abschluss eines Vorabkontrollverfahrens (sensible / strafrechtliche Daten, Auskunft über Kreditwürdigkeit oder Informationsverbundsystem).

DSG 2000 - Registrierung

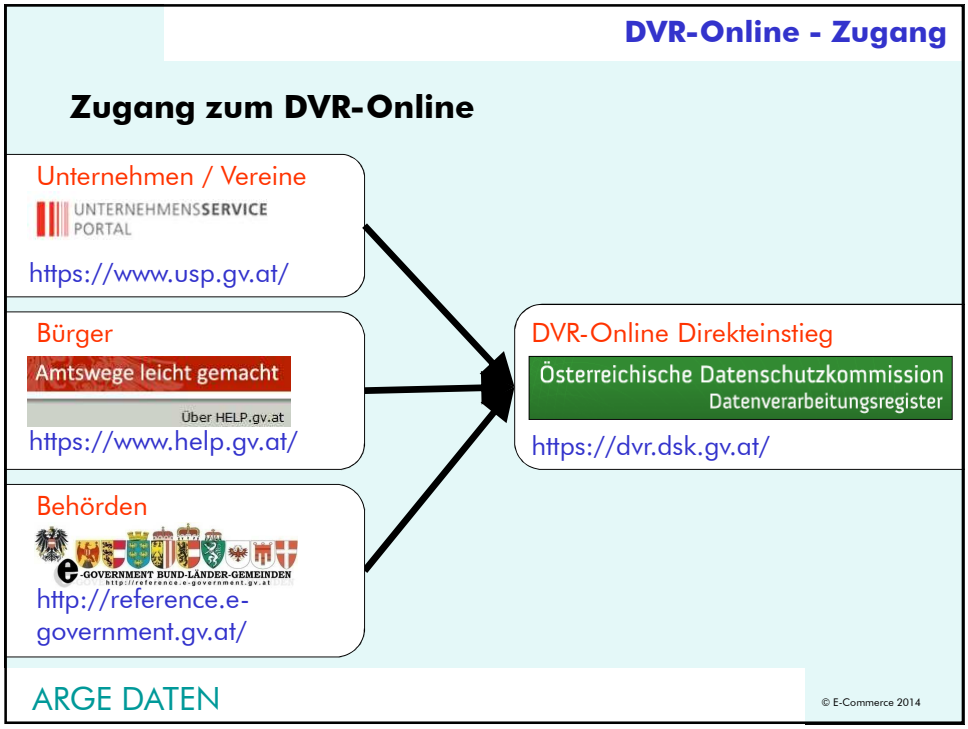
Registrierungsverfahren (seit 1.9.2012)

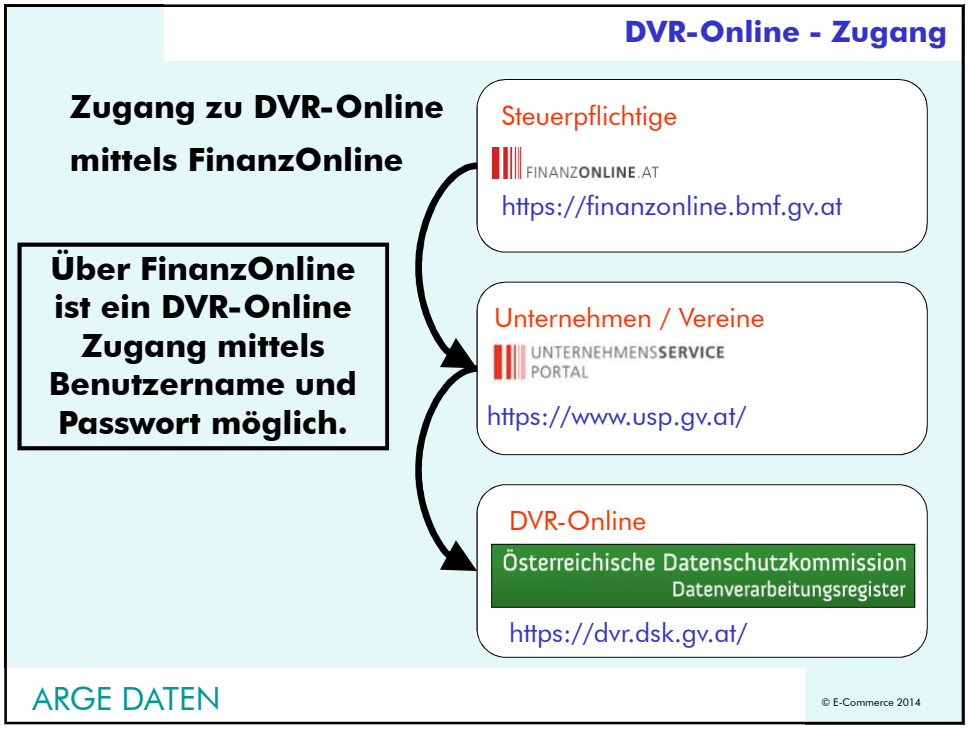
(DSG 2000 § 17 Abs. 1a)

- Meldungen haben über Internetanwendung zu erfolgen
- Authentifizierung erfolgt durch Bürgerkarte, Handy-Signatur oder USP
- eMail-Meldung und nicht-elektronische Meldung bei manuellen Dateien und bei längerem technischen Ausfall der Internetanwendung möglich
- Details sind in der Verordnung des BKA nach § 16 Abs. 3 geregelt

(DSG 2000 § 19 Abs. 3a)

- Erklärung des Auftraggebers ob es sich um vorabkontrollpflichtige Datenanwendung handelt


DVR-Online - Zugang
Zugang zum DVR-Online
Unternehmen / Vereine
UNTERNEHMENSSERVICE PORTAL
https://www.usp.gv.at/
Bürger
Amtswege leicht gemacht
Über HELP.gv.at
https://www.help.gv.at/
Behörden
e-GOVERNMENT BUND-LÄNDER-GEMEINDEN
http://reference.e-government.gv.at
http://reference.e-government.gv.at/
DVR-Online Direkteinstieg
Österreichische Datenschutzkommission
Datenverarbeitungsregister
https://dvr.dsk.gv.at/
ARGE DATEN
© E-Commerce 2014


DVR-Online - Zugang
Zugang zu DVR-Online mittels FinanzOnline
Über FinanzOnline ist ein DVR-Online Zugang mittels Benutzername und Passwort möglich.
Steuerpflichtige
FINANZONLINE.AT
https://finanzonline.bmf.gv.at
Unternehmen / Vereine
UNTERNEHMENSSERVICE PORTAL
https://www.usp.gv.at/
DVR-Online
Österreichische Datenschutzkommission
Datenverarbeitungsregister
https://dvr.dsk.gv.at/
ARGE DATEN
© E-Commerce 2014

DSG 2000 - Standard- und Musterverordnung

Systematik der Standardanwendungen nach StMV 2004

- Standardanwendung behandelt bestimmtes "Thema"
- detaillierte Zweckbeschreibung(en) inkl. Angaben zu
  - gesetzlichen Grundlagen / rechtlichen Voraussetzungen
  - Beschreibung der betroffenen Personen, der zulässigen Verarbeitungen und Übermittlungen
  - Höchstdauer der Datenspeicherung
- Darstellung der Datenarten (analog einer individuellen DVR-Meldung) mit Angabe
  - der betroffenen Personengruppe
  - der Datenarten (inkl. historische Datenführung)
  - Empfängerkreise (betrifft nur Übermittlungen, nicht Überlassung an Dienstleister oder auftraggeberinterne Verwendung!)
- Sicherheitsvorgaben [nicht in allen Fällen!]

ARGE DATEN

DSG 2000 - Standardanwendungen

Die wichtigsten Standardanwendungen für Unternehmen (gem. StMV 2004, StF BGBl. II Nr. 312/2004)

SA001 Rechnungswesen und Logistik ("Buchhaltung")
SA002 Personalverwaltung für privatrechtliche Dienstverhältnisse ("Mitarbeiterverwaltung") + "Bewerberdaten" **(seit 30.3.11)**
SA007 Verwaltung von Benutzerkennzeichen
SA022 Kundenbetreuung und Marketing für eigene Zwecke
SA032 Videoüberwachung für bestimmte Branchen
SA033 **Datenübermittlung in Konzernen**

Die wichtigste Musteranwendung bei Unternehmen

MA002 Zutrittskontrollsysteme

ARGE DATEN

Datenschutz in Österreich

Crashkurs DSG 2000

Registrierungsverfahren

Standardanwendung Konzern

Internationaler Datenverkehr

ARGE DATEN

StMV - Standard- und Musterverordnung

SA033 Datenübermittlung im Konzern

- **Konzerndefinition:** Konzernverband liegt vor, wenn ein rechtlich selbständiges Unternehmen auf Grund von Beteiligungen oder sonst unmittelbar oder mittelbar unter dem beherrschenden Einfluss eines anderen Unternehmens steht
- vier Detailthemen ("Zwecke")
  - A. Konzernweite Kontakt- und Termindatenbank
  - B. Karrieredatenbank
  - C. Verwaltung von Bonus- und Beteiligungsprogrammen eines Konzerns
  - D. Technische Unterstützung

alle anderen Zwecke eines Konzern-Datenverkehrs oder andere Unternehmensverbindungen (z.B. Joint-Ventures, Projektpartnerschaften usw.) fallen NICHT darunter!

ARGE DATEN

A. Konzernweite Kontakt- und Termindatenbank

- **Zweck:** Führung & Übermittlung von Kontaktdaten der Mitarbeiter zu einer gemeinsamen konzernweiten Termindatenbank
- **Rechtsgrundlage:** DSG 2000 §§ 8 Abs. 1 Z 4 und 12 Abs. 3 Z 8
- **Speicherdauer:** bis drei Jahre nach Beendigung eines Arbeitsverhältnisses (nach Ende: beschränkt auf korrekte Behandlung noch eintreffender Nachrichten)
- **Betroffene:** [breit gefasst] Arbeitnehmer, arbeitnehmerähnliche Gruppen, Leiharbeitnehmer, freie Dienstnehmer (Werkverträge), Lehrlinge, Volontäre, Ferialpraktikanten
- **Datenarten (Auswahl):** Identifikations- und Organisationsdaten, Funktion gegenüber Kunden/Geschäftspartnern, Kontaktdaten, Verfügbarkeit (Urlaube, sonstige Abwesenheiten), Informationen zur Weiterleitung von Nachrichten
  bei ehemaligen Beschäftigten: reduzierter Datenumfang!
- **Übermittlungen:** andere Konzernunternehmen weltweit

StMV - Standard- und Musterverordnung

A. Konzernweite Kontakt- und Termindatenbank II

- **Sicherheitsvorgaben:** direkter Bezug auf Art. 25 oder ausreichende Garantien in Form von EU-Standardvertragsklauseln Art. 26 Abs. 2 iVm Abs. 4 der Datenschutz-Richtlinie 95/46/EG

Welche Schritte vereinfacht die SA033 / A. ?

- Konzern-Mitarbeiterverzeichnisse waren registrierungspflichtig
- gemeinsame Verwendung bedeutete Vorliegen eines genehmigungspflichtigen Informationsverbundes
- Übermittlung in Drittstaaten ohne angemessenes Schutzniveau war DSK-genehmigungspflichtig

B. Karrieredatenbank

- **Zweck:** Verwaltung freiwillige Teilnahme an Karriereprogramme
- **Rechtsgrundlage:** DSG 2000 §§ 8 Abs. 1 Z 2 und 12 Abs. 3 Z 5 und/oder Z 8
- **Speicherdauer:** Ende der Bewerbung (Zurückziehung oder Beschäftigungsende)
- **Betroffene:** [breit gefasst] wie bei A.
- **Datenarten (Auswahl):** Identifikations- und Organisationsdaten, Kontaktdaten, Qualifikationen, Sprachkenntnisse, Leistungsbeurteilung, Karrierewünsche/Gehaltsvorstellungen
- **Übermittlungen:** andere Konzernunternehmen weltweit die neue Mitarbeiter suchen, externe Beratungsunternehmen die in Personalangelegenheiten beraten

B. Karrieredatenbank II

- **Sicherheitsvorgaben:** wie A.

Welche Schritte vereinfacht die SA033 / B. ?

- analog zu A.: Registrierung/Informationsverbund/int. Datenverkehr

C. Verwaltung von Bonus- und Beteiligungsprogrammen eines Konzerns

- **Zweck:** Verwaltung von Bonuszahlungen und Beteiligungen (Stock-Options)
- **Rechtsgrundlage:** DSG 2000 §§ 8 Abs. 1 Z 2 und 12 Abs. 3 Z 5 und/oder Z 8 (erfordert Zustimmung des Betroffenen)
- **Speicherdauer:** bis Ausscheiden aus Progamm oder Ende von Garantie-, Gewährleistungs-, Verjährungs- und gesetzlichen Aufbewahrungspflichten; Ende von Rechtsstreitigkeiten
- **Betroffene:** [breit gefasst] wie bei A., jedoch ohne Praktikanten und Volontäre, inkl. ehemalige Beschäftigte
- **Datenarten (Auswahl):** Identifikations- und Organisationsdaten, Kontaktdaten, private Wohn- und Kontaktdaten, Brutto- und Nettoentgelt, sonstige Leistungen, Teilnahmedaten am Programm, Bankverbindung, Steuerdaten

C. Verwaltung von Bonus- und Beteiligungsprogrammen eines Konzerns II

- **Übermittlungen:** an Konzernunternehmen, die Programm durchführen, Steuerbehörden und Banken zur Abwicklung des Zahlungsverkehrs
- **Sicherheitsvorgaben:** wie A.

Welche Schritte vereinfacht die SA033 / C. ?

- analog zu A.: Registrierung/Informationsverbund/int. Datenverkehr

D. Technische Unterstützung

- **Zweck:** Helpdesk/Wartungsdienste zur Unterstützung der Mitarbeiter durch andere Konzernfirmen oder externe Unternehmen
- **Rechtsgrundlage:** DSG 2000 §§ 8 Abs. 1 Z 4 und 12 Abs. 3 Z 8
- **Speicherdauer:** bis zur Bereinigung eines technischen Problems oder bis Ablauf der für den Auftraggeber geltenden Aufbewahrungsfristen bzw. bis Ende eines Rechtsstreites
- **Betroffene:** [breit gefasst] wie bei C.
- **Datenarten (Auswahl):** Identifikations- und Organisationsdaten, Kontaktdaten, technische Ausstattung, Kostenstelle, Probleme und Lösungen
- **Übermittlungen:** andere Konzernunternehmen, die Helpdesk-Aufgaben übernehmen oder mit Beschaffung technischer Ausstattung betraut sind, externe Unternehmen mit Helpdesk-Aufgaben

D. Technische Unterstützung II

- **Sicherheitsvorgaben:** wie A.

Welche Schritte vereinfacht die SA033 / A. ?

- analog zu A.: Registrierung/Informationsverbund/int. Datenverkehr

Datenschutz in Österreich

Crashkurs DSG 2000

Registrierungsverfahren

Standardanwendung Konzern

Internationaler Datenverkehr

DSG 2000 - Internationaler Datenverkehr

Internationaler Datenverkehr (§§ 12, 13, 55)
Genehmigungsfreiheit (EU: "Datenexport")

- innergemeinschaftlicher Datenverkehr
- gleichwertige Datenschutzgesetzgebung
- im Inland zulässigerweise veröffentlichte Daten
- notwendige Grundlage zur Vertragserfüllung mit Betroffenen
- persönliche oder publizistische DA's
- mit Zustimmung des Betroffenen
- wenn Datenverkehr in Standard- und Musteranwendungen vorgesehen
- bei Akten und Dokumenten (Entscheidung DSK K178.074/13-DSK/00 "gegenseitige Information zu Waffenexporten")
- Theoretisch: bei Verwendung der EU-Standardvertragsklauseln (jedoch fehlt Verordnung des Bundeskanzlers!)

Genehmigungsfrei (weil gleichwertig)

- **gleichwertig auf Grund EWR-Verträge**
  Island, Norwegen, Liechtenstein
- **gleichwertig gem. Kommissionsentscheidung**
  Schweiz (27.7.2000), Kanada (15.1.2002)
  Argentinien (30.6.2003), Australien (30.6.2008)
  Israel (31.1.2011), Uruguay (23.8.2012)
  Neuseeland (30.1.2013)
  Andorra, Färöer Islands, Guernsey, Isle of Man, Jersey
- **USA** (nur bereichs- oder unternehmensbezogen, etwa wenn SafeHarbour-Vereinbarung beigetreten, SWIFT- oder PassengerNameRecord-Abkommen)

bei allen anderen Staaten hat sich der Betroffene bzw. der Auftraggeber um den Datenschutz zu kümmern

DSG 2000 - Internationaler Datenverkehr

Internationaler Datenverkehr II (§§ 12, 13, 55)
Genehmigungspflicht

in allen anderen Fällen besteht Genehmigungspflicht (§ 13) die Genehmigung hat die DSB zu erteilen:

- die Feststellungen der Europäischen Kommission sind zu beachten (Abs. 2)
- im konkreten Genehmigungsfall besteht ein angemessenes Schutzniveau (Abs. 2 Z 1)
  [z.B. Verwendung von EU Mustervereinbarungen]
- Antragsteller macht den Schutz der Geheimhaltungsinteressen des Betroffenen glaubhaft (Abs. 2 Z 2)
- Novelle 2010: Möglichkeit einseitiger verbindlicher Zusagen des Auftraggebers für internationalen Datenverkehr (*Abs. 2 Z 2*)
- seit 1.1.2003 sind vor 1.1.2000 erteilte Genehmigungen zu erneuern (sofern weiterhin Genehmigung erforderlich)

Ich danke für Ihre Aufmerksamkeit

Dr. Hans G. Zeger
ARGE DATEN
A-1160 Wien, Redtenbachergasse 20

Tel.:	**+43 676 / 9107032**
Fax.:	**+43 1 / 53 20 974**
Mail persönlich:	**hans.zeger@argedaten.at**
Verein:	**http://www.argedaten.at**
Web2.0:	**http://web2.0.freenet.at**
Personal Page:	**http://www.zeger.at**