

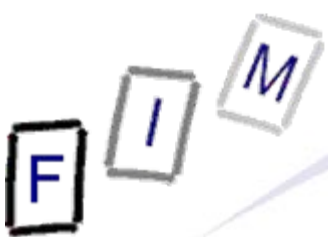


Datenschutzregister

Datenschutzrecht

Institut für Informationsverarbeitung und
Mikroprozessortechnik (FIM)
Johannes Kepler Universität Linz, Österreich

E-Mail: sonntag@fim.uni-linz.ac.at
<http://www.fim.uni-linz.ac.at/staff/sonntag.htm>



Wozu das Datenverarbeitungsregister (DVR) überhaupt?

- Alle Datenverarbeitungen (eigentlich: Datenanwendungen) persönlicher Daten müssen „öffentlich“ sein
 - **Achtung: Dass und welche Kategorien für welchen Zweck auf welche Weise, aber nicht der eigentliche Inhalt!**
- Dies erfolgt durch ein öffentliches Register
 - **Wird von der Aufsichtsbehörde geführt**
- Einsicht: Grundsätzlich für jeden und ohne Gebühr
- Allerdings wäre das auch viel (unnützer) Aufwand!
 - **Beispiel: Unternehmen verschickt Rechnungen**
 - » Auf dem Kuvert steht eine Adresse
 - » Daher Verarbeitung personenbezogener Daten
 - » Anmeldung „ Wir verschicken Rechnungen, darauf sind ...“
 - » Dies wäre nicht sehr sinnvoll!
 - **Viel Aufwand bei minimaler Gefährdung**



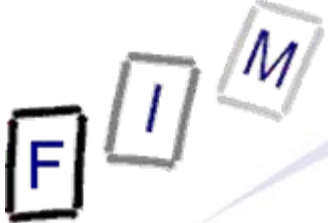
Wozu das Datenverarbeitungsregister (DVR) überhaupt?

- Daher existieren einige Ausnahmen:
 - Standard- & Musteranwendungen
 - » Siehe später!
 - Öffentliche Register, die per Gesetz eingerichtet sind und in die jeder Einsicht nehmen kann, auch wenn nur mit Nachweis eines berechtigten Interesses
 - » Gesetz → Kennt jeder und jeder weiß, was dort gespeichert ist
 - » Öffentlich → Jeder kann selbst nachschauen, was über ihn darin gespeichert ist
- Aber es existiert auch die Gegenrichtung:
Besonders gefährliche Datenanwendungen
 - Diese müssen zuerst registriert werden, und erst wenn dies erfolgreich durchgeführt wurde, darf begonnen werden
 - Beispiele: Informationsverbundsysteme, Bonität



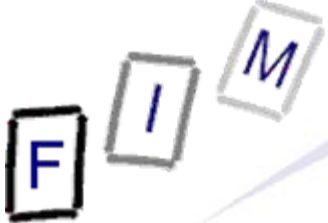
Wann besteht Meldepflicht?

- Jeder Auftraggeber muss seine Datenanwendung registrieren, außer er fällt in eine Ausnahme
 - Gilt gleichermaßen für Änderungen auf Einstellungen
 - » Sowohl der Datenanwendung wie auch der Person
 - Beispiel: Umbenennung/Schließung des Unternehmens
 - » Ebenso für die Rechtsgrundlage der Anwendung
 - Beispiel: Wegfall der nötigen Gewerbeberechtigung
- Ausnahmen:
 - Ausschließlich veröffentlichte Daten
 - Register/Verzeichnisse die per Gesetz eingerichtet sind
 - Nur indirekt personenbezogene Daten
 - Von natürlichen Personen ausschließlich für persönliche oder familiäre Tätigkeiten
 - Publizistische Zwecke
 - Standardanwendungen



Ausnahmen für staatliche Zwecke

- Besondere Ausnahmen von der Meldepflicht bestehen für staatliche Zwecke
 - Die gleichen Ausnahmen kommen im DSG öfters vor!
 - » Beispiele: Auskunft, Löschung
- Ausgenommen von der Meldepflicht sind, **sofern das für ihre Zweckverwirklichung notwendig** ist:
 - Schutz verfassungsm. Einrichtungen der Republik Österreich
 - Sicherung der Einsatzbereitschaft des Bundesheeres
 - » Z.B. Milizregister: Wer steht wofür zur Verfügung, welche Geräte (LKW, Baumaschinen, ...) sind im Einsatzfall abzuliefern
 - Sicherstellung der Interessen umfass. Landesverteidigung
 - Schutz wichtiger außenpolitischer, wirtschaftlicher oder finanzieller Interessen der Republik Österreich oder der Europäischen Union
 - Vorbeugung, Verhinderung oder Verfolgung von Straftaten



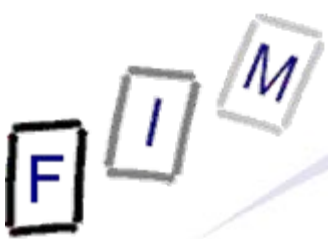
- Der Vorabkontrolle unterliegen folgende Anwendungen:
 - Verarbeitung sensibler Daten
 - Verarbeitung strafrechtlich relevanter Daten
 - Auskunft über die Erteilung der Kreditwürdigkeit der Betroffenen (Bonitätsauskunfteien)
 - Informationsverbundsysteme
- Ausnahme:
 - Sie entspricht einer Musteranwendung
 - » Beispiel: Für Informationsverbundsysteme existieren solche
 - Betrifft innere Angelegenheiten einer anerkannten Kirche oder Religionsgemeinschaft (z.B. Mitgliederverzeichnis)
 - Betrifft die Verwendung von Daten im Katastrophenfall
 - Bloß interner oder Testbetrieb
 - » Nur der „Vollbetrieb“ darf erst nach erfolgter Genehmigung aufgenommen werden!



Inhalt des Registers

- Das Register besteht aus drei Teilen:
 - Registrierte Meldungen über Auftraggeber und Datenanwendungen
 - » **Eigentliches Register: Wer macht Was**
 - **Gesondertes Verzeichnis der Informationsverbundsysteme**
 - » Da der Auftraggeber dort nur eine der zugriffsberechtigten Personen ist und diese „gefährlich“ sind
 - **Registrierungsakten: Schriftverkehr des Verfahrens etc.**
 - » Sonstige Beilagen zu Anträgen
 - » **Angaben zu Sicherheitsmaßnahmen**
 - » Genehmigungsbescheide, Auflagen, Änderungsbescheide
- **Achtung: Register enthält nur begrenzt historische Daten**
 - **Gestrichene oder nicht mehr meldepflichtige Anwendungen sind nicht Teil des Registers; Archiv nur für 7 Jahre**

Nur eingeschränkt öffentliche Einsicht!



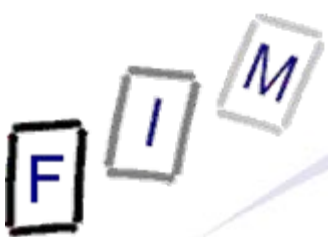
Form und Inhalt der Meldung

- Es sind die Formblätter des DSK zu verwenden
 - Diese sind auch el. verfügbar
 - Nur ausnahmsweise sind formlose Meldungen erlaubt
 - » Streichung einer Anwendung/eines Auftraggebers
 - » Namens-/Adressänderung
 - Namensänderung: Nachweis ist beizulegen
- „Angaben zum Auftraggeber“: Nur bei erster Meldung nötig!
- Sonderregelung für Informationsverbundsysteme
 - Keine Meldung aller anderen Teilnehmer, wenn der Betreiber verpflichtet wurde, jeweils aktuelle Teilnehmer zu melden
 - » Jeder Teilnehmer müsste sonst melden, wenn irgendwer dazu kommt: 100 Teilnehmer + 1 Neuer → 101 Meldungen!
 - Weitere Teilnehmer müssen nicht vollständig melden, sondern können auf existierende Meldung verweisen



Form und Inhalt der Meldung

- Meldung „kann“ per E-Mail (ungesichert, unsigniert) erfolgen
 - Bei Zweifel → Schriftlich + Unterschrift oder el. Signatur
 - Neues Gesetz (§ 17 Abs 1a DSGVO; gilt seit 1.1.2010): Einbringung **muss** elektronisch erfolgen!
 - **Sobald** der Bundeskanzler dafür eine Internetanwendung zur Verfügung stellt
 - » Derzeit gibt es diese (noch) nicht (Frist: 1.1.2012)!
 - » Also weiter auf Papier oder per E-Mail (= Alte Rechtslage)
 - Nähere Details regelt eine zukünftige Verordnung
 - » Soll insb. zur Identifizierung und Authentifizierung die Bürgerkarte verwenden (aber nicht nur)
 - Weiterhin E-Mail und auf Papier erlaubt
 - » Bei längerem Ausfall der Internetanw. + bei manuellen Dateien
 - » Die automatische Kontrolle lehnt die Meldung ab
- Achtung: Bis dahin gilt die alte Rechtslage!**

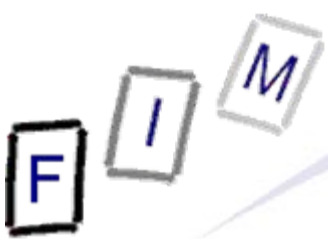


Wann darf ich mit der Anwendung beginnen?

- Grundsatz: Sofort nach der Meldung darf begonnen werden
 - Aber die Meldung muss dann auch genehmigt werden...
 - » Wird sie nicht, so hat man die Anwendung illegal betrieben!
- Ausnahme: Vorabkontrolle (siehe oben)
 - Hier: Melden → Genehmigung → Aufnahme
- Manuelle Prüfung (siehe unten) + 2 Monate ohne Reaktion
 - » Typischer Fall: Vorabkontrolle
 - Erfolgt kein Verbesserungsauftrag („liegenlassen“), so wird die Anwendung eingetragen und man darf beginnen



- Neuerung (1.1.2010/?12?): Meldungen werden nur mehr automationsunterstützt geprüft
 - Wenn sie laut Angabe des Melders nicht der Vorabkontrolle unterliegen
 - Prüfung: Nur Vollständigkeit und Plausibilität
 - Keine Beanstandung → Sofortige Registrierung
 - Fehler bei der Meldung:
 - » Verbesserung möglich
 - » Gilt als nicht eingebracht (→ Kein Beginn erlaubt!)
 - » Schriftlich + Fehlerausdruck einbringen, wenn man auf der Meldung in dieser Form besteht
- Manuelle Prüfung:
 - Vorabkontrollpflichtige Anwendungen
 - Zulässigerweise nicht-elektronisch eingebracht
 - Geprüft wird die „Mangelhaftigkeit“

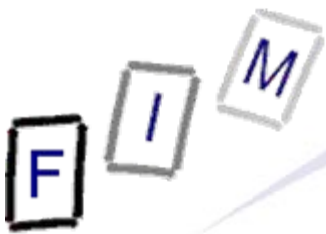


Wann ist eine Meldung „mangelhaft“?

- Angaben fehlen
 - Z.B. keine Rechtsgrundlage angegeben („Warum ich darf“)
- Angaben sind offenbar unrichtig oder unstimmgig
 - Unstimmigkeit = U.a. wenn der Inhalt der gemeldeten Datenanwendung durch die gemeldeten Rechtsgrundlagen nicht gedeckt ist
- Angaben sind so unzureichend, dass Einsichtnehmer im Hinblick auf die Wahrnehmung ihrer Rechte keine hinreichende Information darüber erhalten, ob durch die Datenanwendung ihre schutzwürdigen Geheimhaltungsinteressen verletzt sein könnten
 - Beispiel: Zu allgemeine Kategorien („Kundenklassifikation“ ohne nähere Angaben, wonach klassifiziert wird oder welche Klassen vorgesehen sind)

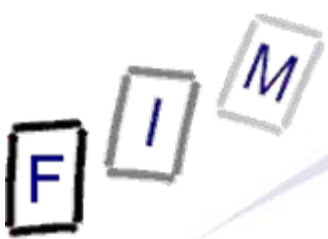


- Unterliegt die Meldung der Vorabkontrolle, so kann die DSK Auflagen, Bedingungen oder Befristungen festlegen
 - Bescheid → Rechtsweg möglich
 - Nur bei Vorabkontrolle!
- Keine Vorabkontrolle → Keine Auflagen möglich
 - Aber: Freiwillige Zusagen, die mit der Registrierung durch die DSK verbindlich werden
 - » Müssen so bestimmt sein, dass sie auch von der DSK ausgesprochen werden könnten
 - Achtung: DSK kann nichts verlangen, aber bei Fehlen kann sie die Registrierung ablehnen! → Verbotene Verarbeitung!

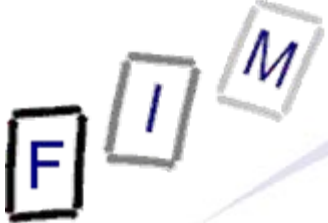


Verbesserungsverfahren

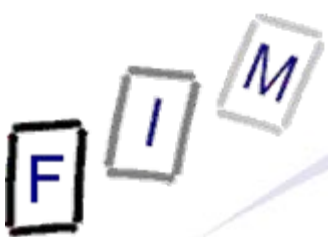
- Ist eine Meldung mangelhaft
 - Binnen zwei Monaten ist Verbesserung aufzutragen
 - » Sonst: 2 Monate keine Reaktion → Genehmigt!
 - Angemessene Fristsetzung
 - Hinweis auf die Rechtsfolgen einer Nichtbeachtung
- Verbesserung wurde durchgeführt
 - Mitteilung an die DSK
 - Anwendung wird registriert
- Was passiert bei ignorieren?
 - Schriftliche Mitteilung der Ablehnung der Registrierung
 - » Wo wurden die Verbesserungsaufträge nicht erfüllt
 - » Verbesserungen nach Absender der Mitteilung sind egal
 - Binnen zwei Wochen Antrag auf Bescheid möglich
 - » Nur ein Bescheid kann bekämpft werden, nicht die Mitteilung!



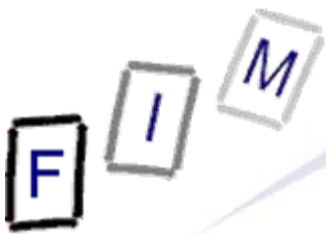
- Erhält man bei der ersten Registrierung
 - Wer nur **nur** Standardanwendungen betreibt, hat **keine!**
 - Jeder Auftraggeber besitzt nur eine Nummer
 - » D.h., Nummer spezifiziert Person, nicht Datenanwendung
- Aussehen: „DVR: 0000000“ (7-stellige Nummer)
 - Führende Nullen sind anzugeben!
- Wann ist sie anzugeben?
 - Bei Übermittlungen an den Betroffenen
 - Vorsichtshalber: Fix in jedem Schreiben anführen
 - » Gleich wie Firmenbuchnummer
- Fehlende Angabe: Verwaltungsstrafe bis € 10.000



- Die erfolgte Registrierung wird schriftlich bestätigt
- Erfolgte die Eingabe elektronisch, so ist auch die Bestätigung elektronisch, z.B. per E-Mail!
- Streichungen oder Namens-/Adressänderungen:
 - Nur Mitteilung der Kenntnisnahme
- Dient als eigener Nachweis, dass die Registrierung erfolgte

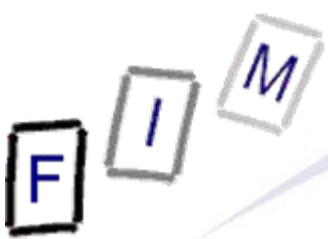


- Spezielles Verzeichnis mit folgenden Informationen:
 - Bezeichnung und Zweck
 - Rechtsgrundlagen
 - Name, Anschrift, Telefon-/Faxnummer und E-Mail Adresse des Betreibers
 - Liste der teilnehmenden Auftraggeber
 - Angaben zu
 - » Rechtsgrundlage, priv./öff. Bereich, manuell/automatisiert
 - » Kreise der Betroffenen und verarbeitete Datenarten
 - » Daten zu beabsichtigten Übermittlungen (→ an Dritte!)
 - Sonstige Informationen auf Anordnung der DSK
 - Übertragung von Rechtspflichten auf den Betreiber
 - » Diese sind gegenüber Dritten nur wirksam, wenn sie hier eingetragen sind!



Register-Richtigstellungen

- Amtlicherseits bei Kenntnis aus amtlichen Verlautbarungen
 - Firmenlöschung, Tod des Auftraggebers, Wegfall der Rechtsgrundlage, Ablauf befristeten Betriebs, Kenntnis der dauerhaften Einstellung → Streichung
 - Adressänderung → Berichtigung
- Schreibfehler oder ähnliche Fehler, die offenbar aus einem Versehen oder ausschließlich auf einem techn. Fehler beruhen, können jederzeit amtswegig berichtigt werden
 - Verpflichtende Verständigung des Auftraggebers
- Verdacht der Nichterfüllung der Meldepflicht
 - Fehlerhaft oder unterlassen → Berichtigungsverfahren
- Änderungen sind 7 Jahre lang ersichtlich zu machen



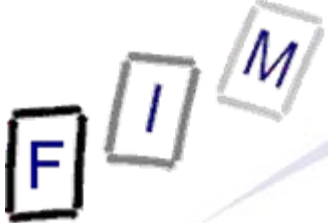
Übernahme der Anwendungen bei Rechtsnachfolge

- Der Rechtsnachfolger eines Auftraggebers kann einzelne oder alle registrierten Meldungen übernehmen
 - Binnen 6 Monaten Antrag + Glaubhaftmachung
 - Kann auch die Registernummer des Vorgängers übernehmen
 - » Zusätzlicher Antrag nötig
 - » Voraussetzung: Vorgänger stellt jede Verarbeitung ein
 - Ansonsten gäbe es zwei Auftraggeber mit gleicher Nummer!
- Vorteil: Kein Genehmigungsverfahren nötig



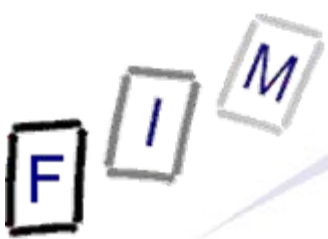
Überprüfungsverfahren

- DSK kann jederzeit die Erfüllung der Meldepflicht prüfen
 - Mangelhaftigkeit genauso wie Nicht-Meldung
 - » D.h., die kann bei jedem vor der Tür stehen und prüfen, ob/welche Datenanwendungen erfolgen!
- Bei Verdacht ist ein Verfahren zu eröffnen
 - Mitteilung an Auftraggeber mit Verbesserungs- oder Nachmeldungsaufrag unter Fristsetzung
 - Einleitung und Stand wird im Register (→ öffentlich!) vermerkt
- Wird dem Verbesserungsauftrag nicht entsprochen, so ist die Streichung aus dem Register zu verfügen
 - Auch teilweise, wenn möglich und sinnvoll
- Wird dem Nachmeldungsaufrag nicht entsprochen, so ist der Betrieb zu untersagen und Anzeige zu erstatten
 - § 52 Abs 2 Z 1 DSGVO: Unerlaubter Betrieb
 - » Verwaltungsstrafe bis € 10.000



Einsicht in das DVR

- Jeder kann Einsicht in das Register nehmen
 - Keine Begründung notwendig; keine Kosten
 - Keine DVR-Nummer (selbst/Frage) nötig
 - Nach Möglichkeit im Internet
 - » Suche eingeschränkt: Nur Name/DVR bzw. Name des Informationsverbundsystems/Name des Betreibers/Name des Auftraggebers
 - » Derzeit allerdings nicht möglich!
- Dies betrifft aber nur die Datenanwendungen und das Informationsverbundsystem-Verzeichnis
- Der Registerakt erfordert zusätzlich:
 - Glaubhaftmachung dass man Betroffener ist
 - Keine überwiegenden schutzwürdigen Geheimhaltungsinteressen des Auftraggebers oder Dritter
- **Niemals** gibt es Einsicht in die **Datensicherheitsmaßnahmen!**



Archivierung des Registers

- Ist Papier und el. Version vorhanden, so wird nur die digitale Variante aufbewahrt
- Meldungen, die gestrichene oder nicht mehr meldepflichtige Anwendungen betreffen, werden nur drei Jahre nach Streichung/Wegfall der Meldepflicht archiviert
- Dies betrifft auch die zugehörigen Registrierungsakten
- Es existiert daher keine Archivierung!
 - Drei/Sieben Jahre lang zurück verfolgbar
 - Was aktuell ist, aber kein historischer Bestand
 - » Anders als etwa beim Grundbuch!



Formblatt: Auftraggeber

- Registernummer
- Name, Firmenbuchnummer
- Telefon, Fax, E-Mail Adresse
- Kontaktdaten eines Zustellbevollmächtigten
 - **Optional; z.B. Rechtsanwalt**
- Kontaktdaten eines Vertreters, falls der Auftraggeber keine Niederlassung in der EU besitzt
 - **Verarbeitung in AT von USA aus**
- Kontaktdaten eines Sachbearbeiters beim Auftraggeber
- Rechtsgrundlagen (warum **überhaupt**)

REPUBLIK ÖSTERREICH DATENSCHUTZKOMMISSION DVR: 0000027 Stand: 1. August 2004	Datenverarbeitungsregister A-1010 Wien, Hohenstaufengasse 3 Tel. (01) 531 15 / 4043 Fax: (01) 531 15 / 4016 E-Mail: dvr@dsk.gv.at
--	--

Angaben zum Auftraggeber (gemäß Anlage 1 DVRV 2002 BGBl II Nr. 24/2002)

1. Registernummer <small>(bitte eintragen, falls eine solche bereits zugeteilt wurde)</small>	DVR:
---	-------------

2. Name (sonstige Bezeichnung) und Anschrift des Auftraggebers

3. Telefon- und Faxnummer sowie E-Mail-Adresse

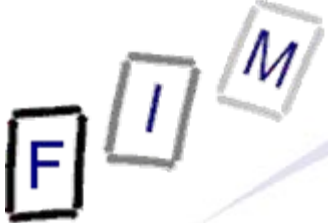
4. Name, Anschrift, Telefon- und Faxnummer sowie E-Mail-Adresse eines Zustellbevollmächtigten

5. Name (sonstige Bezeichnung) und Anschrift des Vertreters eines Auftraggebers, der keine Niederlassung in der Europäischen Union hat

6. Name und Telefonnummer des Sachbearbeiters beim Auftraggeber (für allfällige Rückfragen zu den Angaben im Formblatt)

7. Rechtsgrundlage(n) für die Verwendung von Daten (rechtliche Befugnis im privaten Bereich, gesetzliche Zuständigkeit im öffentlichen Bereich)

8. Firmenbuchnummer des Auftraggebers (falls vorhanden)



Formblatt: Auftraggeber

- Art der Meldung: Erst-/Änderungs- / Streichungsmeldung
- Angaben über Unterlagen der Meldung
- Datum, Unterschrift, Stempel
 - Variante 1: Einscannen
 - Variante 2: Grafik hineinkopieren
 - Variante 3: Text hinschreiben
- Varianten 2+3: Werden akzeptiert und nur bei Zweifeln wird eine echte Unterschrift verlangt
 - § 5 Abs 7 DVR-VO 2002

9. Anlass der Meldung:

9.1. Erstmeldung

9.2. Änderungsmeldung

Änderung des Namens (der Bezeichnung) oder Anschrift des Auftraggebers

Änderung infolge Rechtsnachfolge (Der Rechtsnachfolger muss alle von ihm durchgeführten Datenanwendungen neu melden, auch wenn die Registernummer vom Rechtsvorgänger übernommen werden soll)

Sonstige Änderungen von Angaben zum Auftraggeber in diesem Formblatt

9.3. Streichungsmeldung

Streichung der Registernummer (nur, wenn der Auftraggeber keine meldepflichtige Datenanwendung mehr durchführt, z.B. wenn das Unternehmen erloschen ist)

10. Beilagen zur Meldung

Nachweis der Rechtsgrundlagen für die Verwendung von Daten (in Übereinstimmung mit Punkt 7) im privaten Bereich z.B. durch Vorlage einer Kopie

* des Gewerbescheines

* der Bestellsurkunde

* der genehmigten/hinterlegten Satzung;

im öffentlichen Bereich durch Nachweis der gesetzlichen Zuständigkeit, soweit dies nicht außer Zweifel steht

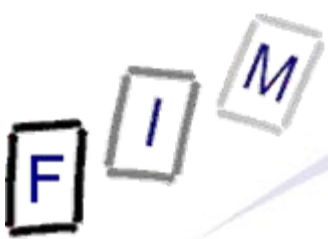
Nachweis bei Änderungen (z.B. Kopie des aktuellen Firmenbuchauszuges bei einer Firmenwortlautänderung)

Begründung, weshalb ein Nachweis nicht erbracht werden muss:

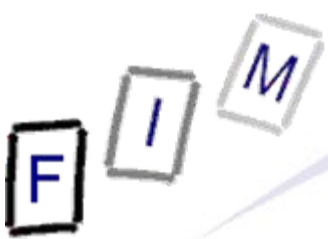
Anzahl der Beilagen:

11. Bestätigung der Richtigkeit und Vollständigkeit der Angaben in diesem Formblatt

Datum, Unterschrift, Stempel



- Automationsunterstützt oder Manuell
- Vorabkontrolle:
 - **Sensible/Strafrecht/Bonität**
 - **Informationsverbundsystem**
 - » Gesamtbezeichnung
 - » Betreiber + Kontaktdaten
 - » Rechtsgrundlage für Informationsverbundsystem
- Geschäftszahlen von Bescheiden der DSK mit Auflagen
- Geschäftszahl der Genehmigung der DSK für internationalen Datenverkehr
- Angaben über Beilagen



- Angaben zum Inhalt der Datenanwendung
 - Kreise der Betroffenen: Über wen wird gespeichert
 - Verarbeiteten Datenarten: Welche Kategorien werden gespeichert („Spaltenüberschriften“ der Tabelle)
- Falls Übermittlungen geplant sind:
 - Kreise der Betroffenen: Wessen Daten werden übermittelt
 - Übermittelten Datenarten: Was wird weitergegeben
 - Empfängerkreise: An wen wird geschickt
 - » Inkl. Empfängerstaaten falls im Ausland
 - » Besondere Hervorhebung falls Empfänger zum gleichen Informationsverbundsystem gehören
 - Rechtsgrundlagen der Übermittlung



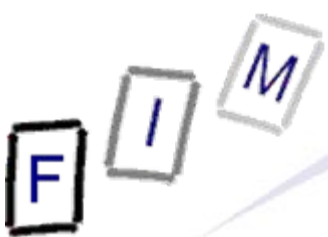
Sicherheitsmaßnahmen

- Der Auftraggeber muss die Daten absichern
 - gegen zufällige oder unrechtmäßige Zerstörung, Verlust oder Veränderung
 - » Unveränderte Existenz muss sichergestellt werden
 - Gegen unbefugten Zugriff oder Veröffentlichung
 - » Geheimhaltung der Daten
- Mittels angemessener Mittel
 - Technisch und organisatorisch: Siehe nächste Folie!
- Der Auftraggeber haftet hierfür; er muss diese Aufgaben auch an alle Dienstleister weitergeben
 - Erfordert einen rechtlich bindenden Akt
 - » Dienstleister ist an Anweisungen des Auftraggebers zu binden
 - » Dienstleister muss alle Sicherheitsmaßnahmen erfüllen
 - **Schriftlichkeit** nötig!
 - AG muss sich von tatsächlichen Maßnahmen überzeugen



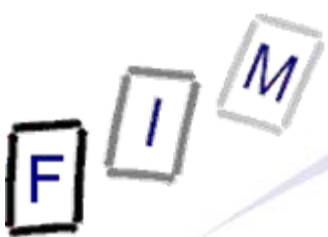
Sicherheitsmaßnahmen: Typische Minimalanforderungen

- Das minimale Schutzniveau beinhaltet:
 - Unabhängig von Wert/Gefährlichkeit der Daten
 - » Aber das Ausmaß des Schutzes hängt sehr wohl davon ab!
 - Explizite Regeln, wer mit den Daten was tun darf
 - In Verträge mit Mitarbeitern:
 - » Verarbeitung nur aufgrund gültiger Aufträge
 - » Information über die Verschwiegenheitspflicht
 - » Wer welche Datenverarbeitungssysteme benutzen darf
 - Zutrittsberechtigungen zu Räumen mit Daten regeln
 - Medien mit Daten müssen gesichert werden
 - Protokollierung aller Verarbeitungsschritte, soweit erforderlich
 - » Beispiele für unterschiedliche Niveaus
 - Marketingadressen → Pro Datei/Datenbank
 - Gesundheitsdaten → Jeder einzelne Lese-/Schreibzugriff auf einen Datensatz; ev. sogar pro Datenfeld
 - Dokumentation aller Sicherheitsmaßnahmen



Sicherheitsmaßnahmen : Typische Minimalanforderungen

- Technisch ev. einzuführen:
 - Verschlüsselung: Alle Übertragungen öffentlicher Netzwerke
 - » Z.B. SSL: Kreditkartenfirmen verlangen dies, wenn man Online Kreditkarten akzeptiert (ansonsten kein Vertrag mit diesen)
 - Partitionierung (Pseudonyme): Sofern möglich/sinnvoll
 - Zugriffsrechte: Für jedes persönlicher Datum nötig
 - » Beinhaltet sichere Identifikation der Benutzer!
 - Daten auf separatem und separat abgesicherten Server
 - » Webserver werden immer wieder gehackt → Eigener DB-Server
 - Konfigurierbares Logging
 - Speicherung von Text + Datum/Zeit einer Zustimmung
 - » Um diese später nachzuweisen zu können!
 - Backup speziell beachten: Verschlüsselt/gesichert lagern
 - » Der Sicherheitsmaßstab gilt für alle „Kopien“ gleichermaßen



Sicherheitsmaßnahmen : Ausmaß des Schutzes

- Entsprechend dem Stand der techn. Möglichkeiten
 - Neue Technologie: Muss **sofort** berücksichtigt werden!
- Entsprechend der wirtschaftlichen Vertretbarkeit
 - Aber nicht alles (techn.) mögliche ist auch **verpflichtend!**
- Sicherheitsniveau muss den Gefahren durch die Art der Daten und Umfang & Zweck ihrer Verarbeitung entsprechen
 - Allgemeine Beurteilung: Wie „gefährlich“ ist Veröffentlichung, Löschung, ... solcher Daten für den typischen Betroffenen
 - » Einzelne Personen stärker gefährdet → Keine Berücksichtigung!
- Ergebnis:
 - ① Bewertung von Daten und Risiko
 - ② Vergleich der Sicherungsmethoden und ihrer Kosten
 - ③ Auswahl und Umsetzung entsprechenden Schutzniveaus



- DSK kann bei Verdacht auf eine fehlende oder falsche Meldung prüfen
 - Unangemessenheit oder Nichteinhaltung der Sicherheitsmaßnahmen?
 - » Feststellung per Bescheid
 - » Frist zur Herstellung ausreichender Maßnahmen
 - » Mitteilung von Details der getroffenen Maßnahmen an die DSK innerhalb der Frist
 - » Erfolgt dies nicht oder sind diese nicht ausreichend, so muss die Meldung gestrichen werden!
 - Kein Betrieb mehr erlaubt!
- Strafraumen:
 - Gröbliche Außerachtlassung: Verwaltungsstrafe bis € 10.000
 - » Außer es handelt sich um eine gerichtliche Angelegenheit



Datensicherheitsmaßnahmen

- Standard-Kopf mit Referenzen auf die Datenanwendung

REPUBLIK ÖSTERREICH
DATENSCHUTZKOMMISSION
 DVR: 0000027
 Stand: 1. August 2004

Datenverarbeitungsregister
 A-1010 Wien, Hohenstaufengasse 3
 Tel. (01) 531 15 / 4043
 Fax: (01) 531 15 / 4016
 E-Mail: dvr@dsk.gv.at

Allgemeine Angaben zu ergriffenen Datensicherheitsmaßnahmen
 (gemäß Anlage 4 DVRV 2002 BGBl. II Nr. 24/2002)

1. **Registernummer** DVR:
 (bitte eintragen, falls eine solche bereits zugeteilt wurde)

2. **Name (sonstige Bezeichnung) des Auftraggebers:**

3. **Bezeichnung der Datenanwendung:**

Kreuzen Sie bitte in den nachstehenden Rubriken an, welche Datensicherheitsmaßnahmen Sie für die gemeldete Datenanwendung getroffen oder nicht getroffen haben. Sofern von Ihnen vorgesehene Datensicherheitsmaßnahmen in der Auflistung nicht angeführt sind, geben Sie bitte unter „Sonstige“ an, welche Datensicherheitsmaßnahmen Sie für die gegenständliche Datenanwendung getroffen bzw. zusätzlich getroffen haben.

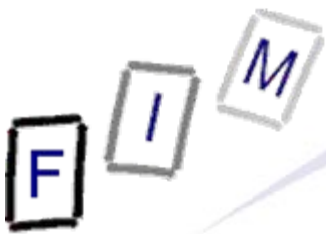
4. **Folgende Datensicherheitsmaßnahmen wurden für diese Datenanwendung ergriffen / nicht ergriffen: (Zutreffendes bitte ankreuzen)**

	JA	NEIN	
1.	<input type="checkbox"/>	<input type="checkbox"/>	Die Aufgabenverteilung bei der Datenverwendung zwischen den Organisationseinheiten und zwischen den Mitarbeitern wurde ausdrücklich festgelegt;



Datensicherheitsmaßnahmen

	JA	NEIN	
1.	<input type="checkbox"/>	<input type="checkbox"/>	Die Aufgabenverteilung bei der Datenverwendung zwischen den Organisationseinheiten und zwischen den Mitarbeitern wurde ausdrücklich festgelegt;
2.	<input type="checkbox"/>	<input type="checkbox"/>	die Verwendung von Daten wurde an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter gebunden;
3.	<input type="checkbox"/>	<input type="checkbox"/>	jeder Mitarbeiter wurde über seine nach dem DSG 2000 und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten belehrt;
4.	<input type="checkbox"/>	<input type="checkbox"/>	die Zutrittsberechtigung zu den Räumlichkeiten des Auftraggebers oder Dienstleisters wurde geregelt und Maßnahmen gegen den Zutritt Unbefugter ergriffen;
5.	<input type="checkbox"/>	<input type="checkbox"/>	die Zugriffsberechtigung auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte wurde geregelt;
6.	<input type="checkbox"/>	<input type="checkbox"/>	die Berechtigung zum Betrieb der Datenverarbeitungsgeräte wurde festgelegt und jedes Gerät durch Vorkehrungen bei den eingesetzten Maschinen oder Programmen gegen die unbefugte Inbetriebnahme abgesichert;
7.	<input type="checkbox"/>	<input type="checkbox"/>	es wird Protokoll geführt, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können;
8.	<input type="checkbox"/>	<input type="checkbox"/>	es wird eine Dokumentation über die nach Z 1. bis 7. getroffenen Maßnahmen geführt, um die Kontrolle und Beweissicherung zu erleichtern.
9.	<input type="checkbox"/>		Sonstige Datensicherheitsmaßnahmen:



Standard- und Musteranwendungen

- Erleichterungen für „übliche“ Anwendungen
 - Standardanwendung: Werden von einer großer Anzahl von Auftraggebern gleichartig vorgenommen und angesichts des Verwendungszwecks und der verarbeiteten Datenarten ist die Gefährdung schutzwürdiger Geheimhaltungsinteressen der Betroffenen unwahrscheinlich
 - » Beispiel: Geschäftskorrespondenz, Buchhaltung, ...
 - Musteranwendung: Werden von großer Anzahl von Auftraggebern gleichartig vorgenommen, sind aber nicht „harmlos“
- Werden beide per Verordnung festgelegt
 - Aufbau: Ähnlich wie eine normale Meldung
 - Beinhalten auch „rund-um“ Elemente: Freier Text und maschinenlesbare Bilddateien mit diesen Daten + Archivierung dieser Daten
 - » Muss also nicht eine „echte“ Datenbank sein

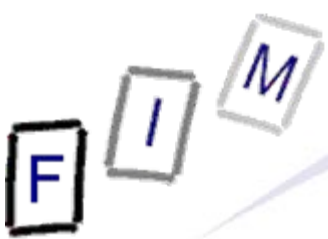


- In der Verordnung werden festgelegt:
 - Zulässigen Datenarten
 - Betroffenen- und Empfängerkreise
 - » Solche Übermittlungen müssen **nicht** protokolliert werden!
 - Höchstdauer zulässiger Datenaufbewahrung
- Weil diese Anwendungen nicht im Register stehen:
 - Der Auftraggeber muss diese Informationen jeder Person auf Anfrage hin mitteilen (oder dass keine erfolgen)
 - » Das erfordert **nicht**, dass es sich um einen Betroffenen handelt!
 - D.h. auch dann, wenn die Daten dieser Person nicht enthalten sind
 - » Keine Begründung der Anfrage erforderlich
- Kosten: Wohl gratis
 - Kein nennenswerter Aufwand und gesetzliche Verpflichtung



Übersicht Standardanwendungen

- Derzeit 31 Standardanwendungen
- Wichtigsten:
 - SA001 Rechnungswesen und Logistik
 - SA002 Personalverwaltung für privatrechl. Dienstverhältnisse
 - SA003 Mitgliederverwaltung
 - SA007 Verwaltung von Benutzerkennzeichen
 - SA022 Kundenbetreuung und Marketing für eigene Zwecke
- Weitere für spezielle Berufsgruppen (Ärzte, Apotheker) sowie öffentliche Einrichtungen (Wirtschaftskammer, Ministerien)
 - Beispiele: Melderegister, Wählerevidenz, Lehrstellenbörse der Wirtschaftskammer, Verrechnung ärztlicher Verschreibungen für Rechnung begünstigter Bezieher durch Apotheken



Beispiel Standardanwendung

SA 22: Kundenbetreuung und Marketing

Zweck: Verwendung von eigenen oder zugekauften Kunden- und Interessentendaten für die Geschäftsanbahnung betreffend das eigene Lieferungs- oder Leistungsangebot, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in dieser Angelegenheit.

Höchstdauer zulässiger Aufbewahrung: Die Daten dürfen bis zum Ablauf des dritten Jahres nach dem letzten Kontakt mit dem Auftraggeber aufbewahrt werden.

Rechtsgrundlage: Nicht angegeben (wohl alle Gewerbetreibenden, Selbständigen, ...)

3 Gruppen von Betroffenen:

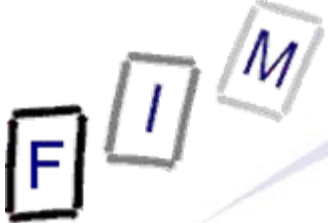
- Eigene Kunden, Interessenten, die an den Auftraggeber selbst herangetreten sind
- Kontaktpersonen beim Kunden oder Interessenten
- Potenzielle Interessenten; von Adressverlagen zugekauft (gemietet) oder selbst ermittelt

2 Empfängerkreise:

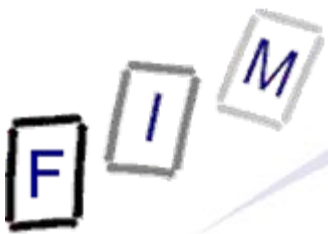
- Adressverlage und Direktwerbeunternehmen gem. § 151 GewO 1994
- Konzernleitung bei gewerblichen Kunden und Großkunden

Daten (Nur Auswahl!):

- Name, Titel, Anrede, Geschlecht, Anschrift, Telefon, Fax, E-Mail, Sperrkennzeichen, Untersagung der Übermittlung an Adressverlage, Branchenbezeichnung, Geburtsdatum, Familienstand, Interessen, Kaufkraftklassifizierung, Betreuungsdaten, Kaufverhalten (Frequenz und Volumen), Antwortverhalten, Bonus-/Vorteilsdaten, ...



- Grundidee: Vorausgefülltes Meldungsformular
 - Hier wird keine besondere Prüfung durchgeführt
 - Wird es wie im Muster vorgegeben betrieben, so besteht „keine“ Gefahr und die Meldung muss genehmigt werden
 - » Ist aber nicht harmlos, daher soll sie im Register enthalten sein!
- In der Verordnung werden festgelegt:
 - Zulässigen Datenarten
 - Betroffenen- und Empfängerkreise
 - » Solche Übermittlungen müssen **nicht** protokolliert werden!
 - Höchstdauer zulässiger Datenaufbewahrung
- Auskunft: Wie bei allen „sonstigen“ Anwendungen
 - Nur für Betroffene, Mitwirkungspflicht, ev. Kosten, ...



Übersicht Musteranwendungen

- Derzeit 5 Musteranwendungen:
 - MA001 Personentransport- und Hotelreservierung
 - » Gew. Flugreservierung, Hotels, ... → Reisebüros
 - MA002 Zutrittskontrollsysteme
 - » Siehe nächste Folie!
 - MA003 KFZ-Zulassung durch beliehene Unternehmen
 - » Erfolgt inzwischen durch Versicherungen
 - „Beliehen“ = Privatunternehmen tritt wie Staat auf (z.B. Bescheid)
 - MA004 Teilnahme am Informationsverbundsystem
www.fundamt.gv.at
 - » Österreichisches Fundwesen; Gemeindeaufgabe; Gemeinden können daran teilnehmen, wenn sie möchten
 - MA005 Teilnahme am Informationsverbundsystem
FundInfo.at
 - » Konkurrenzplattform zu oben; auch in DE und IT angeboten



Beispiel Musteranwendung: MA002: Zutrittskontrollsysteme

- **Zweck der Datenanwendung:**
 - Kontrolle der Berechtigung des Zutritts zu Gebäuden und abgegrenzten Bereichen durch den Eigentümer oder Benutzungsberechtigten mit Hilfe von Anlagen, die personenbezogene Daten automationsunterstützt ermitteln und speichern, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in dieser Angelegenheit.
- **Rechtsgrundlagen:** § 96a Abs 1 Z 1 ArbVG und § 9 Abs 2 lit f PVG
 - Zustimmungserfordernis des Betriebsrates/Personalvertretung bei Verarbeitung personenbezogener Daten vor Arbeitnehmern in bestimmten Fällen (???)
- **Betroffene Personengruppen:** Zutrittsberechtigte
- **Datenarten:**
 - Ordnungsnummer, Bereichsspez. Personenkennzeichen; Personalverwaltung (PV)
 - Vor- und Familienname, akad. Grad/Standesbezeichnung, Geschlecht
 - Beziehung des Betroffenen zum Auftraggeber (Mitarbeiter, Kunde, Besucher)
 - Telefon-, Faxnummer, und andere zur Adressierung erforderliche Informationen, die zur raschen Verständigung des Betroffenen erforderlich sind
 - Lichtbild des Betroffenen, sofern als zusätzliche Sicherheitsmaßnahme erforderlich
 - Zutrittscode
 - Vom Berechtigten einzugebender Berechtigungscode
 - Daten der Zutrittsberechtigung, insbesondere Bereiche und Zeiten
 - Gültigkeitsdauer der Zutrittsberechtigung

← Weitergabe an Stammzahlenregisterbehörde erlaubt



Formblatt: Meldung einer Musteranwendung

- Registernummer
- Name, Kontaktdaten
 - Auftraggeber, Sachbearbeiter
- Bezeichnung der Musteranwendung
 - + Informationsverbundsystem Ja/Nein
 - » MA1, MA2 → Möglich
 - » MA3 - MA5 → Immer
- Art der Meldung: Neu, Änderung, Streichung
- Informationen zu Beilagen

REPUBLIK ÖSTERREICH DATENSCHUTZKOMMISSION DVR: 0000027 Stand: 1. August 2004	Datenverarbeitungsregister A-1010 Wien, Hohenstaufengasse 3 Tel.: (01) 531 15 / 4043 Fax: (01) 531 15 / 4016 E-Mail: dvr@dsk.gv.at
--	---

Meldung einer Musteranwendung (gemäß Anlage 3 DVRV 2002 BGBl. II Nr. 24/2002)

1. Registernummer
(bitte eintragen, falls eine solche bereits zugeteilt wurde) **DVR:**

2. Name (sonstige Bezeichnung) und Anschrift des Auftraggebers

3. Telefon- und Faxnummer sowie E-Mail-Adresse

4. Name und Telefonnummer des Sachbearbeiters beim Auftraggeber

5. Bezeichnung(en) der Musteranwendung(en) gemäß BGBl. II Nr. 312/2004
(Zutreffendes bitte ankreuzen: ☒)

	Vorliegen eines Informationsverbundsystems:	
	JA	NEIN
<input type="checkbox"/> MA001 Personentransport- und Hotelreservierung	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> MA002 Zutrittskontrollsysteme	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> MA003 KFZ-Zulassung durch beliehene Unternehmen	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> MA004 Teilnahme am Informationsverbundsystem www.fundamt.gv.at	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> MA005 Teilnahme am Informationsverbundsystem FundInfo.at	<input checked="" type="checkbox"/>	<input type="checkbox"/>

6. Falls durch eine gemeldete Musteranwendung eine bereits registrierte Datenanwendung ersetzt wird
Laufende Nummer oder Bezeichnung der betreffenden Datenanwendung:

7. Streichung einer registrierten Musteranwendung
Laufende Nummer oder Bezeichnung der Musteranwendung sowie Grund der Streichung:

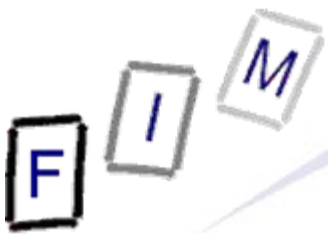
8. Beilagen zur Meldung

Formblatt "Allgemeine Angaben zu ergriffenen Datensicherheitsmaßnahmen" gem. Anlage 4 DVRV 2002

Nachweis der Rechtsgrundlage, soweit diese dem Datenverarbeitungsregister noch nicht vorgelegt wurde (z.B. Kopie der Gewerbeberechtigung, Nachweis der Zustimmung des Betriebsrates nach dem Arbeitsverfassungsgesetz, Ermächtigungsbescheid des Landeshauptmannes gemäß § 40a KFG).

Begründung, weshalb ein Nachweis nicht erbracht werden muss:

Anzahl der Beilagen:



- Für viele Unternehmen wichtig:
 - Was keine Standardanwendung ist, muss gemeldet werden
 - » Manche Unternehmen haben mehrere hundert gemeldet!
 - Praktisch nicht so bedeutsam
 - » Gefahr bei Nicht-Meldung (derzeit?) nicht sonderlich hoch
 - » Potentiell gefährlich: UWG!
 - Ähnliches gilt für die Datensicherheitsmaßnahmen
 - » Könnten jetzt aber wichtiger werden
 - § 24 Abs 2a DSGVO: Mitteilungspflicht an potentiell Betroffene!
- Musteranwendungen sind trivial zu melden
 - Aber nicht sehr hilfreich, da nur 1 (2) praktisch relevant sind!
- Besonders wichtig: Änderungsmeldungen
 - Wird SEHR oft vergessen: Neue Funktion in der Software → Mehr Daten verarbeiten → Meldung müsste geändert werden!

F I M

Fragen?

Vielen Dank für Ihre Aufmerksamkeit!