Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Informatik und Datenschutz im Bund

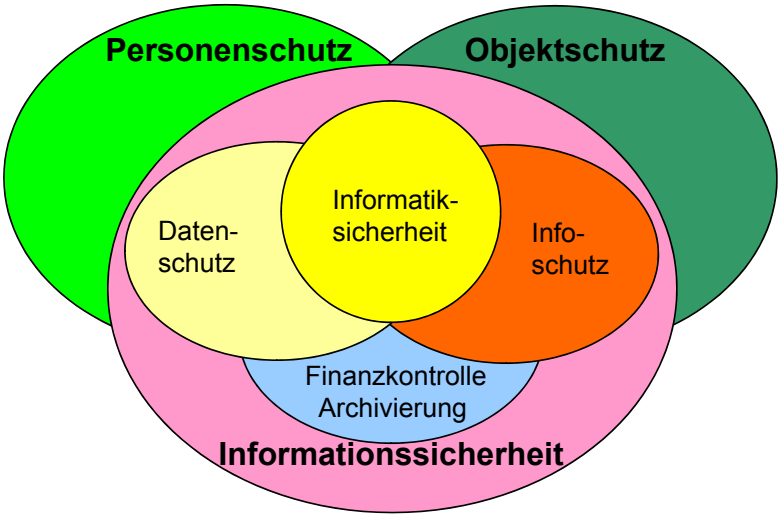
Peter Fischer, Delegierter für Informatikstrategie Bund

Zürich, 9. September 2008

Übersicht

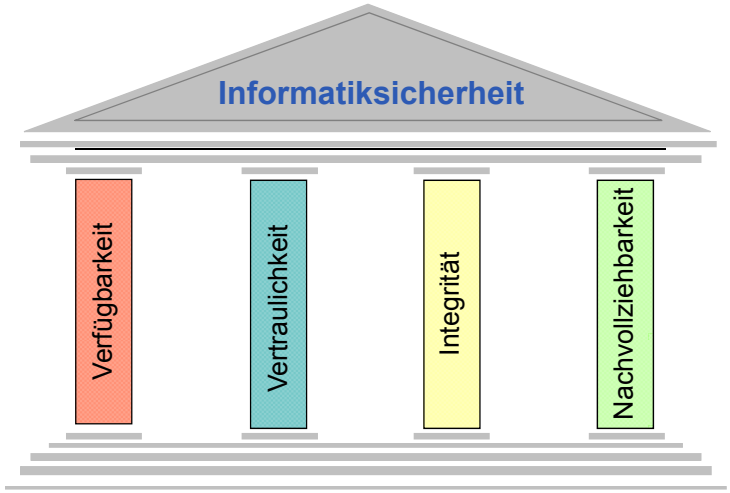
- **Datenschutz als Teil der Informatiksicherheit**
- Vorgaben des Datenschutzes (der Informatiksicherheit)
- Informatiksicherheit als Bestandteil jedes Informatikprojekts
- Rollen im Datenschutz/Informatiksicherheit
- Beispiel neuen materiellen Datenschutzrechts
- Datenschutz im E-Government Schweiz

Sicherheit im Spannungsfeld



Eidgenössisches Finanzdepartement EFD Informatik und Datenschutz / Peter Fischer / 2008-09-09 4

Die 4 Säulen der Informatiksicherheit



Eidgenössisches Finanzdepartement EFD Informatik und Datenschutz / Peter Fischer / 2008-09-09 5

Übersicht

- Datenschutz als Teil der Informatiksicherheit
- **Vorgaben des Datenschutzes (der Informatiksicherheit)**
- Informatiksicherheit als Bestandteil jedes Informatikprojekts
- Rollen im Datenschutz/Informatiksicherheit
- Beispiel neuen materiellen Datenschutzrechts
- Datenschutz im E-Government Schweiz

Vorgaben des Datenschutzes

- Straf- und Zivilgesetzbuch
- Datenschutzrecht (Bund, Kantone)
- Organisationsrecht (Personal-, Organisations-, Archiv-, Klassifikationsrecht, …)
- Öffentlichkeitsrecht
- Materielles Recht
- Fachweisungen

WIsB, wichtigste Aspekte 1/2

- Art. 2 Zuständigkeiten, Aufgaben
  ISBD/O, LB, LE, Operative Ebene
- Art. 3 Sicherheitsverfahren
  - Ablauf nach HERMES-Phasen
  - Sicherheitsmassnahmen nach internationalen Standards wie ISO/IEC 27001/2, BSI IT-Grundschutz-Kataloge, etc.
  - Verfahren
  - Dokumentation
  - Kontrolle

WIsB, Verfahren und Hilfsmittel

- Art. 3.3
  Schutzbedarfsanalyse (nach HERMES)
  → Hilfsmittel: Excel-Sheet **Schuban**
  - Genereller Schutzbedarf
    → Anforderungen gemäss **Anhang-1** der WIsB
  - Erhöhter Schutzbedarf
    - Vertiefte Beurteilung des Schutzbedarfs
      → Hilfsmittel: **ProtAn**
    - Erstellen von Sicherheitskonzepten
      → Hilfsmittel: **ISDS-Konzept**

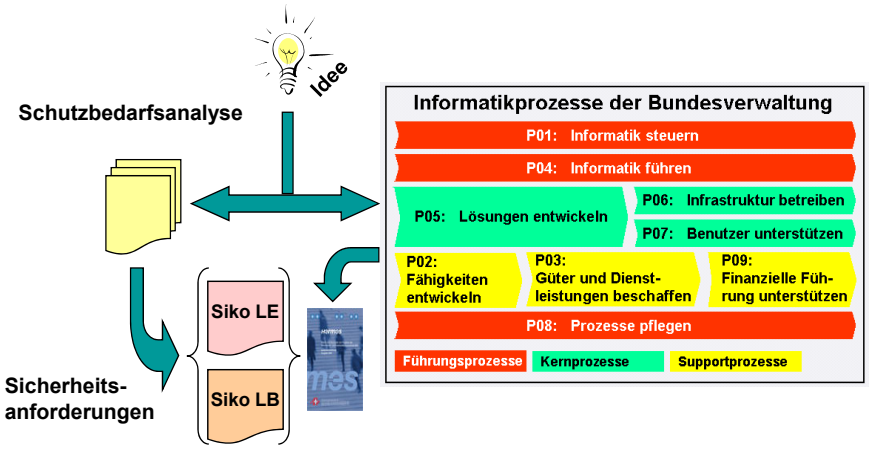
Übersicht

- Datenschutz als Teil der Informatiksicherheit
- Vorgaben des Datenschutzes (der Informatiksicherheit)
- **Informatiksicherheit als Bestandteil jedes Informatikprojekts**
- Rollen im Datenschutz/Informatiksicherheit
- Beispiel neuen materiellen Datenschutzrechts
- Datenschutz im E-Government Schweiz

Datenschutz ist integraler Bestandteil jedes Informatiksystemprojekts

Abbildung 3: Ergebnisübersicht Projekttyp «Systemadaption»

Bedürfnisse / Anforderungen



Sicherheit in HERMES und P05

	Initialisierung	Voranalyse	Konzept	Realisierung	Einführung	Abschluss
Studien-controlling (SCO) erstellen	Zuständige(n) Sicherheits- und Datenschutzbeauftragte(n) kontaktieren	Analysieren und bewerten vom Schutz-bedarf	Erarbeiten und bewerten der Schutzmass-nahmen, Erstellen ISDS Konzept	Umsetzen der Schutzmass-nahmen, Umsetzen ISDS Konzept	Kontrolle der umgesetzten Schutzmass-nahmen, Abnahme ISDS Konzept	Informations-sicherheit und Datenschutz abschliessen
	P05.01 Informatik-vorhaben initialisieren	P05.02 Grobe Lösungs-vorschläge skizzieren	P05.03 Lösung designen	P05.04 Lösung realisieren	P05.05 Lösung einführen	P05.06 „Lösungen entwickeln“ abschliessen
Tools	Schuban Schutzbedarfsanalyse	ProtAn Risikoanalyse	ISDS Sicherheitskonzept	ISDS Sicherheitskonzept	ISDS Sicherheitskonzept	ISDS Sicherheitskonzept

Legende: Studiencontrolling | HERMES | Informationssicherheit | P05 „Lösungen entwickeln“ | Tool

Schutzbedarfsanalyse Schuban

Projektname : Webzugriff auf Amtsdaten
Studien / Projekt Nr. : 608.123.456
Departement : EFD
Amt : ISB
Dienststellen Nr. : 987.654
Geschäftsprozess Hans Muster
Klassifizierung : Intern (siehe neue IschV)
Datum der Einstufung : 01. Mrz 08
Interview Teilnehmer : Projektleiter, GPV, ISBD,ISBO, DSB

Drucken

Einstufung

Kriterien	Fragen	Antwort	Kommentar, Begründung
Vertraulichkeit	**Was für Daten werden bearbeitet ?** **Ist die Bearbeitung von personenbezogenen Daten bei welchem die Betroffenen in irgend einer Weise beeinträchtigen wirklich notwendig ?** **Kann evtl. darauf verzichtet werden**	Personenbezogene Daten, deren Bearbeitung keine besondere Beeinträchtigung der Persönlichkeit erkennen lassen sowie Personendaten, die ihre Öffentlichkeit bereits erreicht	
		Personenbezogene Daten, deren Bearbeitung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann	
		Personenbezogene Daten, deren Bearbeitung den Betroffenen in seiner gesellschaftlichen Stellung oder seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen oder eine Gefahr für Leib und Leben sein kann. (Bspw. besonders schützenswerte Personendaten, Persönlichkeitsprofile,...)	*Die Religionszugehörigkeit ist beispielsweise ein Merkmal für besonders schützenswerte Personendaten, ebenfalls können Arbeitslosendaten schützenswert sein.Bei dieser Frage ist auch der Aspekt der 'normaler' Vertraulichkeit der zu berarbeitenden Daten und Informationen zu berücksichtigen. Bei Unklarheiten kontaktieren Sie am besten Ihren DSB*
Verfügbarkeit	**Max. Ausfalldauer ?**	Ausfalldauer mehr als einen Tag	
		Ausfalldauer maximum 1 Tag	*Die Ausfalldauer sollte in der Regel einen Tag nicht überschreiten (z.B. Vorbereitung für wichtige BR Sitzung)*
	Katastrophenvorsorge ?	Kein Ausfall (0 Std.) In einem Katastrophenfall müssen die Daten nicht verfügbar sein	
		In einem Katastrophenfall müssen die Daten verfügbar sein	*Die Amtsdaten respektive Teile davon müssen in einem K-Fall verfügbar sein.*
Integrität	**Können Datenveränderungen die Aufgabenerfüllung derart einschränken, dass sie Handlungsunfähig wird ?**	Eine unbeabsichtigte Datenveränderung führt zu keiner erheblichen Einschränkung in der	*Die Anwendung stellt nur den Zugriff auf die Amtsdaten und Informationen sicher.*
		Eine unbeabsichtigte Datenveränderung führt zu einer erheblichen Einschränkung in der Aufgabenerfüllung, evtl. sogar bis zur	
Nachvollziehbarkeit	**Was passiert, wenn die Nachvollziehbarkeit nicht gewährleistet werden kann ?**	Es führt zu keiner erheblichen Einschränkung in der	
		Es führt zu einer erheblichen Einschränkung des Aufgabenbereiches. Verstösse gegen geltende Gesetze, Vorschriften oder Verträge bis hin zum Imageverlust der BV sind möglich.	*Die Nachvollziehbarkeit ist in diesem Projekt auf folgende Punkte festgelegt: WER hat WANN mittels dieser Anwendung auf die Amtsdaten zugegriffen*

Informationssicherheit und Datenschutz Konzept (ISDS, nach Hermes)

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Informatikstrategieorgan Bund ISB

ISDS-Konzept

Klassifizierung *	Nicht klassifiziert / Intern / Vertraulich
Status **	In Arbeit / In Prüfung / Abgeschlossen
Projektname	Sichereit 1
Projektabkürzung	Projektabkürzung
Projektnummer	
Projektleiter	Peter Fischer
Auftraggeber	Auftraggeber
Autor	Herr Tom
Initiale	Initiale
Bearbeitende	Bearbeitende
Prüfende	
Genehmigende	
Verteiler	Verteiler

ISDS Konzept (nach Hermes)

Projektname	Sicherheit 1	Eidgenössisches Finanzdepartement: EFD
Ergebnisname	ISDS-Konzept	Informatikstrategieorgan Bund ISB

1 Allgemeines
2 Zusammenfassung
3 Zweck des Dokuments
4 Sicherheitsrelevante Systembeschreibung
5 Risikoanalyse
6 Sicherheitsbedürfnisse
7 Schutzvorschläge
8 Schutzmassnahmen
9 Notfallkonzept
10 Abdeckung der Risiken durch die Massnahmen
11 Restrisiken
12 Einhaltung / Überprüfung der Schutzmassnahmen
13 Test / Abnahme der Informationssicherheitsfunktionen
14 Verzeichnis der sicherheitsrelevanten Dokumente
15 Anhang
- Datenschutzbearbeitungsreglement

Eidgenössisches Finanzdepartement EFD Informatik und Datenschutz / Peter Fischer / 2008-09-09 16

Datenschutzbearbeitungsreglement

1. **Allgemeines**
2. **Zweck des Dokuments**
3. **Gesetzliche Grundlagen**
   Dieser Abschnitt fasst die gesetzlichen Grundlagen zusammen, auf die sich die Bearbeitung der Daten stützt.
4. **Angaben zur Meldepflicht**
   Definiert die Meldepflicht.
   Hier wird die Datensammlung-Anmeldung festgehalten und dokumentiert. Das ausgefüllte Anmeldungsformular wird als Anhang beigelegt.
5. **Datensammlung**
   Beschreibt die Datensammlung. Folgende Angaben sind zwingend:
   das für den Datenschutz und die Datensicherheit verantwortliche Organ
   die Herkunft der Daten
6. **Datenbearbeitung**
   Beschreibt die Bearbeitung der Daten:
   der Bearbeitungszweck
   die Kontrollverfahren und insbesondere die technischen und organisatorischen Massnahmen
   die Beschreibung der Datenfelder und die Organisationseinheiten, die darauf Zugriff haben
   die Art und der Umfang des Zugriffs der Benutzer der Datensammlung
   die Datenbearbeitungsverfahren, insbesondere die Verfahren bei der Berichtigung, Sperrung, Anonymisierung, Speicherung, Aufbewahrung, Archivierung oder Vernichtung der Daten.
   die Konfiguration der Informatikmittel
   das Verfahren zur Ausübung des Auskunftsrechts
6. **Anhang**
   - Datensammlung-Anmeldung

Eidgenössisches Finanzdepartement EFD Informatik und Datenschutz / Peter Fischer / 2008-09-09 17

Übersicht

- Datenschutz als Teil der Informatiksicherheit
- Vorgaben des Datenschutzes (der Informatiksicherheit)
- Informatiksicherheit als Bestandteil jedes Informatikprojekts
- **Rollen im Datenschutz/Informatiksicherheit**
- Beispiel neuen materiellen Datenschutzrechts
- Datenschutz im E-Government Schweiz

Rollen im Datenschutz in der Informatik

- Datenschutz-Informatiksicherheit-Risikomanagement
- Leistungsbezüger/in, Auftraggeber/in
  - Geschäftsprozessverantwortliche/r
  - Anwendungsverantwortliche/r
  - Datenverantwortliche/r
  - Datenschutzbeauftragte/r
  - Informatiksicherheitsbeauftragte/r
- Leistungserbringer/in
  - Systemverantwortliche/r

Übersicht

- Datenschutz als Teil der Informatiksicherheit
- Vorgaben des Datenschutzes (der Informatiksicherheit)
- Informatiksicherheit als Bestandteil jedes Informatikprojekts
- Rollen im Datenschutz/Informatiksicherheit
- **Beispiel neuen materiellen Datenschutzrechts**
- Datenschutz im E-Government Schweiz

34 Artikel Sportförderungsgesetz und …

415.0

Bundesgesetz
über die Förderung von Sport und Bewegung
(Sportförderungsgesetz)

vom

Die Bundesversammlung der Schweizerischen Eidgenossenschaft,
gestützt auf Artikel 68 der Bundesverfassung[1],
nach Einsicht in die Botschaft des Bundesrates vom …[2],
beschliesst:

1. Kapitel: Allgemeine Bestimmungen

Art. 1 Ziele

Dieses Gesetz strebt im Interesse der Leistungsfähigkeit und Gesundheit der Bevölkerung, der ganzheitlichen Bildung und des gesellschaftlichen Zusammenhalts folgende Ziele an:

a. Steigerung der Sport- und Bewegungsaktivitäten der Menschen aller Altersstufen;
b. Erhöhung des Stellenwerts des Sports in Erziehung und Ausbildung;
c. Schaffung geeigneter Rahmenbedingungen zur Förderung des leistungsorientierten Nachwuchs- und des Spitzensports;
d. Förderung von Verhaltensweisen, mit denen die positiven Werte des Sports in der Gesellschaft verankert und Auswüchse und Missbräuche bekämpft werden.

29 Artikel ISG …

Bundesgesetz
über die Informationssysteme des Bundes im Bereich Sport (ISG)

vom

Die Bundesversammlung der Schweizerischen Eidgenossenschaft,
gestützt auf Artikel 68 der Bundesverfassung[1],
nach Einsicht in die Botschaft des Bundesrates vom …[2],
beschliesst:

1. Kapitel: Allgemeine Bestimmungen

Art. 1 Gegenstand

Dieses Gesetz regelt die Bearbeitung von Personendaten (Daten) in Informationssystemen des Bundesamtes für Sport (BASPO) durch:

a. Behörden des Bundes und der Kantone;
b. Sport- und Jugendverbände, die nach dem Sportförderungsgesetz vom yy.xx.zzzz[3] unterstützt werden;
c. Dritte, die Aufgaben im Zusammenhang mit der Sportförderung des Bundes übernehmen.

Art. 2 Grundsätze der Datenbearbeitung

[1] Soweit es zur Erfüllung ihrer gesetzlichen oder vertraglichen Aufgaben notwendig ist, dürfen die Stellen und Personen nach Artikel 1:

Bsp. ISG …

3. Abschnitt: Reservations- und Bestellungssysteme

Art. 12 Zweck

Die Reservations- und Bestellungssysteme dienen der Verwaltung der Infrastruktur und der effizienten Abrechnung der bezogenen Leistungen.

Art. 13 Daten

Die Systeme enthalten folgende Daten:

a. Namen, Adresse und Telefonnummer der Benutzerinnen und Benutzer;
b. personenbezogene Offerten und Abrechnungen.

Art. 14 Datenbeschaffung

Das BASPO beschafft die Daten für die Systeme bei den betroffenen Personen.

Art. 15 Datenbekanntgabe

Das BASPO macht die Daten der Systeme durch Abrufverfahren zugänglich:

a. der betroffenen Person für die sie betreffenden Daten;
b. den für die Abrechnung zuständigen Stellen und Personen.

Übersicht

- Datenschutz als Teil der Informatiksicherheit
- Vorgaben des Datenschutzes (der Informatiksicherheit)
- Informatiksicherheit als Bestandteil jedes Informatikprojekts
- Rollen im Datenschutz/Informatiksicherheit
- Beispiel neuen materiellen Datenschutzrechts
- **Datenschutz im E-Government Schweiz**

Datenschutz im E-Government

- Vertrauen in E-Government Anwendungen ist ein Schlüssel für den Erfolg: Vertrauen basiert auf Daten- und Informationsschutz
- Methode Hermes auch im E-Government Schweiz empfohlen: Datenschutz ist integriert im Informatikprojekt
- E-Government bedingt und bringt grössere Vernetzung der Produktions- und Distributionsprozesse: Datenherrschaft und damit Datenschutzverantwortung über mehrere Verwaltungseinheiten und föderale Ebenen zu klären
- Daten- und Informatikschutz über die ganze Prozesskette zu betrachten

Datenschutz im E-Government

- Benutzer/innenfreundlichkeit steht häufig im Spannungsfeld mit dem individuellen Datenschutz
- Datenschutz steht im Spiegel der gesellschaftlichen Entwicklung: Spannungsfeld zwischen individuellem persönlichem Verhalten und öffentlicher Erwartung, auch im E-Government?
- Verknüpfung von Datensätzen ist technisch möglich, auch ohne einheitlichen Personenidentifikator
- Zugriffs- und Berechtigungsregelung sowie deren Umsetzung auf Datensätze ist entscheidend: Selektion nach Rollen und Anwendung/Produkt