12th Symposium on Privacy and Security

Datenschutz nach der Revision des eidg. Datenschutzgesetzes – ein Überblick

Dr. James T. Peter
Aschwanden Del Fabro & Partner, Zürich

Inhalt:
Die wesentlichen Änderungen im Überblick

1. Stand der Gesetzgebungsarbeiten
2. Grundsätzliches zur Revision
3. Erkennbarkeit der Datenbearbeitung (Art. 4 IV)
4. Information der betroffenen Personen (Art. 7a)
5. Grenzüberschreitende Bekanntgabe (Art. 6)
6. Einwilligung (Art. 4 V)
7. Zertifizierungsverfahren (Art. 11)
8. Betrieblicher Datenschutzverantwortlicher (Art. 11a V lit. e)

Stand der Gesetzgebungsarbeiten

- 24. März 2006 werden DSG-Änderungen vom Parlament verabschiedet
- Verordnung zum DSG (VDSG): Änderung vom 28. September 2007
- Verordnung über die Datenschutzzertifizierungen (VDSZ) vom 28. September 2007
- 1. Januar 2008: Inkraftsetzung DSG mit Ausführungsbestimmungen

Grundsätzliches zur Revision

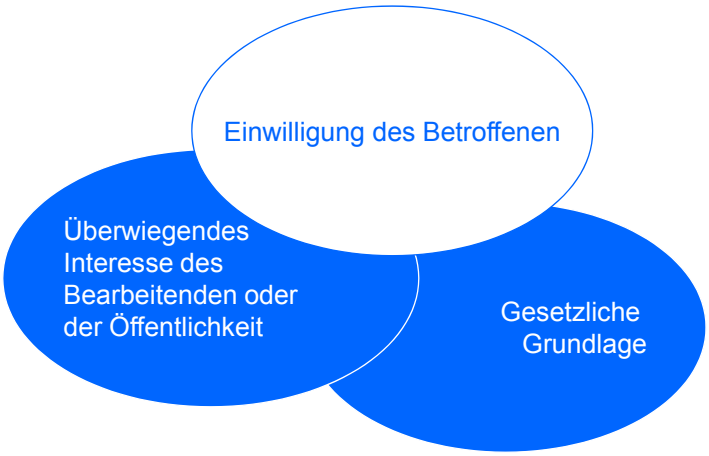
- DSG (des Bundes) betrifft Bundesorgane und Private
- Subsidiäre Auswirkung auf kantonale Organe beim Vollzug von Bundesrecht (→ Art. 37 DSG)
- Schwerpunkt der Revision betrifft die für Bundesorgane und Private gültigen allgemeinen Grundsätze (Art. 4 – 11a)

Erkennbarkeit (Art. 4 IV)

«Die Beschaffung von Personendaten und insbesondere der Zweck ihrer Bearbeitung müssen für die betroffene Person erkennbar sein»

- Gilt für alle Daten und alle Bearbeitungsvorgänge
- Hinweis auf regelmässige oder mögliche Datenbearbeitungen z.B. mittels Anmerkungen in Formularen, Vertragsklauseln/AGB, Website, Serienbrief, E-Mail oder SMS
- Vornahme der erforderlichen Massnahmen innert einem Jahr seit Inkraftsetzung

Bedeutung der Neuerung



Erkennbarkeit (Art. 4 IV)

- Bezieht sich auf den Bereich der ohne Einwilligung erfolgt

  Wobei die Transparenzpflicht gemäss den Ausnahmetatbeständen von Art. 7a und 9 entfällt

Einschränkungen der Transparenzpflicht

Die Anwendung der Einschränkungen von Art. 7a und 9 ergibt sich durch Auslegung:

- Art. 7a IV: Datenbearbeitung *ausdrücklich* im Gesetz vorgesehen oder Transparenz führt zu unverhältnismässigem Aufwand
- Art. 9: Einschränkung ausdrücklich in einem formellen Gesetz vorgesehen
- Art. 9: Überwiegende Drittinteressen
- Art. 9: Überwiegende öffentliche Interessen oder wo erforderlich bei Strafuntersuchungen (für Bundesorgane)
- Art. 9: Überwiegende eigene Interessen (der Privatperson) soweit Daten nicht Dritten bekannt gegeben werden

Einschränkungen der Transparenzpflicht

Handlungsbedarf betreffend Transparenzpflicht (Art. 4 IV)

1. Prüfen, ob für den Betroffenen nicht erkennbare Datenbearbeitungen vorgenommen werden.
2. Prüfen, ob eine Einschränkung der Transparenzpflicht vorliegt (Art. 7a & 9).
3. Sinnvollste Kommunikationsform evaluieren, die zur Erkennbarkeit der Datenbearbeitung führt.

Informationspflicht (Art. 7a)

Der Inhaber der Datensammlung ist verpflichtet, die betroffene Person über die Beschaffung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen zu informieren; diese Informationspflicht gilt auch dann, wenn die Daten bei Dritten beschafft werden.

Unterschied von Art. 7a zu Art. 4 IV

Art. 7a bezieht sich nur auf:

- *Beschaffung* von
- besonders schützenswerten Daten und Persönlichkeitsprofilen (*sensitiven Daten*) wenn deren
- Bearbeitung in *Datensammlungen* erfolgt.
- *Aktive Information ist verlangt! Die vorsätzliche Unterlassung ist mit Strafe bedroht (Art. 34 Abs. 1)*

Zahlreiche offene Fragen zu Art. 7a

Beispiele:

- Darf aus der Verwendung des Begriffes «speichern» geschlossen werden, dass nur elektronische Datensammlungen gemeint sind?
- Gilt die Informationspflicht auch für öffentlich zugänglich gemachte «sensitive Daten»?
- Gilt diese Regel auch für bestehende (altrechtliche) Datensammlungen, die allenfalls noch mit aktualisierten Daten ergänzt werden?

Informationspflicht (Art. 7a II)

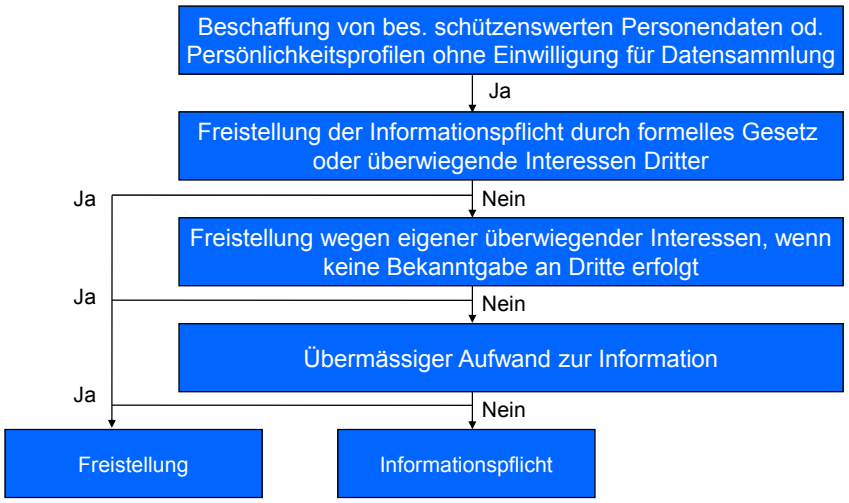
- Inhaber der Datensammlung
- Zweck des Bearbeitens
- Kategorien der (möglichen) Datenempfänger

- Hinsichtlich der Form besteht keine Voraussetzung. Aber: Strafandrohung verlangt eine gewisse Vorsicht!
- Übergangsfrist: 1 Jahr seit Inkrafttreten des Gesetzes

Informationspflicht entfällt

- Wenn die betroffene Person bereits informiert wurde. (Das positive Wissen um die Möglichkeit der Beschaffung muss reichen.)
- Wenn ein Gesetz im formellen Sinn die Einschränkung vorsieht.
- Wenn überwiegende Interessen Dritter eine Geheimhaltung erforderlich machen.
- Wenn überwiegende Interessen des Inhabers die Geheimhaltung erforderlich machen und die Daten nicht an Dritte (auch Konzern-gesellschaften?) bekannt gegeben werden.

Schematische Darstellung



Grenzüberschreitende Bekanntgabe (Art. 6)

«Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet.»

Art. 5 VDSG: Werden Personendaten mittels automatisierter Informations- und Kommunikationsdienste zwecks Information der Öffentlichkeit allgemein zugänglich gemacht, so gilt dies nicht als Übermittlung ins Ausland.

Freier Datenfluss

- Gewährleistet in allen EU-Ländern sowie Signatarstaaten der Datenschutzkonvention Nr. 108 des Europarates
- Von der EU als gleichwertig anerkannte Drittstaaten (z.B. Argentinien)

Grenzüberschreitender Datenfluss ohne gleichwertigen Datenschutz (Art. 6 II)

1. «Safe Harbor» zertifizierte Unternehmen: Empfänger hat sich zur Einhaltung von gleichwertigem Datenschutz verpflichtet (lit. a)
2. Datenschutz-Vereinbarung, die angemessenen Schutz gewährleisten (lit. a) [→Mitteilungspflicht]
3. Konzerninterner Datenfluss: Empfänger untersteht genehmigten internen Datenschutzregeln (lit. g) [→ Mitteilungspflicht]
4. Rechtfertigungsgrund: Einwilligung (lit. b), Vertragsabschluss (lit. c), überwiegende öffentliche Interessen (lit. d), Gerichtsverfahren (lit. d), allgemein zugängliche gemachte Daten (lit. f)

Prüfung der Zulässigkeit (Art. 6 III)

- EDÖB muss über die Datenschutzgarantien oder Datenschutzregeln informiert werden (unter Strafandrohung: Art. 34)
- EDÖB prüft die ihm gemeldeten Garantien und Datenschutzregeln (Art. 31 I lit. e) innert 30 Tagen (Art. 6 V VDSG)

Anforderungen an die Einwilligung (Art. 4 V)

- Einwilligung erst nach *angemessener Information* gültig:
  - Angemessene Information: Abhängig von der Bekanntheit/Erkennbarkeit einer Datenbearbeitung
  - Evtl. Hinweis auf welche Daten, zu welchem Zweck bearbeitet werden und u.U. welche Verbreitung im Unternehmen oder Konzern erfolgt
- Bearbeiten von «sensitiven Daten» setzt *ausdrückliche Einwilligung* voraus

Zertifizierung (Art. 11)

- Bundesorgane und Private können ihre Systeme, Verfahren und Organisation zertifizieren lassen.
- Bundesrat erlässt die Verordnung über die Datenschutzzertifizierung (VDSZ) vom 28. September 2007
- Datenschutzzertifizierungs-Stellen müssen akkreditiert sein. EDÖB wird beigezogen.

Zertifizierung von Organisation & Verfahren

- Gesamtheit oder einzelne Datenbearbeitungs-verfahren
- Gegenstand ist das Datenschutzmanagement-system:
  - Datenschutzpolitik
  - Dokumentation von Zielen und Massnahmen
  - Organisatorische und technische Massnahmen zur Behebung festgestellter Mängel

Zertifizierung von Produkten

- Prüfung der produktimmanenten Gewährleistung:
  - von Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der Daten
  - der Vermeidung von Bearbeitung nicht erforderlicher Daten
  - von Transparenz und Nachvollziehbarkeit der Datenbearbeitung
  - von technischen Massnahmen zur Unterstützung der Einhaltung der Datenschutzgrundsätze

Nutzen der Zertifizierung

- Zertifizierte Inhaber von Datensammlungen müssen ihre Sammlungen nicht registrieren lassen (Art. 11a V lit. f), wenn sämtliche Datenbearbeitungsverfahren, denen eine Datensammlung dient, zertifiziert sind.
- Eine Zertifizierung schafft eine (widerlegbare) Vermutung des datenschutzkonformen Verhaltens: z.B. kann «angemessene Information» für Einwilligung reduziert werden

Betrieblicher Datenschutzverantwortlicher (DV)

- Inhaber einer Datensammlung kann einen Datenschutzverantwortlichen bezeichnen
- Entweder Mitarbeiter oder Dritter (Art. 12a II VDSG)
- DV darf keine Aufgaben übernehmen, die mit der Aufgabe als DV unvereinbar wären
- Übt seine Funktion fachlich unabhängig aus (Art. 12b VDSG)

Nutzen des DV

- Datensammlungen müssen nicht registriert werden (Art. 11a V lit. e)
- Erhöht Glaubwürdigkeit in die Einhaltung der erforderlichen Datenschutzregeln

Herzlichen Dank für Ihre Aufmerksamkeit