

# LUTIS 2008

Luzerner Tage der Informationssicherheit  
Information Security Refresher

3.- 5. Juni 2008

**Ursula Sury**  
Rechtsanwältin  
Professorin Informatikrecht

5. Juni 2008

# Neuerungen des Datenschutzgesetzes und der Verordnungen

in Kraft seit 1. Januar 2008

# Agenda

- Die wesentlichen Neuerungen des Datenschutzgesetzes (DSG) auf einen Blick
- Die wichtigsten Änderungen des DSG im Detail (Privatbereich)
- Die wesentlichen Neuerungen der Verordnung zum Datenschutzgesetz (VDSG)
- Die Verordnung über die Datenschutzzertifizierungen (VDSZ)

# Die wesentlichen Neuerungen auf einen Blick

- Informationspflicht bei Erhebung der Daten- erhöhte Transparenz
- Vereinfachung der Meldepflicht
- Förderung der Selbstregulierung durch Zertifizierung
- öffentlich-rechtlicher Bereich: Regulierung Pilotversuche, Bearbeitung von Personendaten durch Bundesorgane und Dritte, Mindeststandard in den Kantonen

# Aktive Informationspflicht: Erhöhung der Transparenz

Besonders schützenswerte Daten und Persönlichkeitsprofile: Information über:

- Identität des Inhabers der Datensammlung
- Zweck der Datensammlung
- Kategorien von Datenempfängern, falls Bekanntgabe der Daten vorgesehen ist: Art. 7a DSGVO

Andere Personendaten:

- Datenbeschaffung muss erkennbar sein: Art. 4 Abs.4 DSGVO

# Praktisches Beispiel zu Art. 4 Abs. 4 DSGVO

Wird eine Kundenkarte einer Bank beantragt, und sind dazu Personalien anzugeben, ist grundsätzlich klar, dass die Bank die Angaben für die Zustellung von eigener Werbung nutzen kann. Wenn aber beim Gebrauch der Kundenkarte Daten über die Konsumgewohnheiten beschafft und für die Erstellung von Konsumentenprofilen benutzt werden, so sind die Kunden in geeigneter Art und Weise darüber zu informieren.

# Vereinfachung der Meldepflicht

- Bekanntgabe von  
Personendaten ins  
Ausland gem. Art. 6  
Abs.1 DSGVO:
- Gesetzgebung muss **angemessenen Schutz** gewähren. Falls nicht vorhanden:
  - Art. 6 Abs. 2

- Anmeldung von  
Datensammlung bei  
Bearbeitung von bes.  
schützenswerten Daten  
oder  
Persönlichkeitsprofilen  
oder bei Bekanntgabe  
der Daten an Dritte:
- Meldepflicht wird **administrativ vereinfacht**

# Zertifizierung nach Art.11 DSGVO: Förderung der Selbstregulierung

- Zertifizierung für Produkte, Verfahren und Organisationen ist neu vorgesehen.
- Details werden in der Verordnung zum Zertifizierungsverfahren geregelt (VDSZ).

# Die wesentlichen Änderungen des DSGVO im Detail

Art. 4, 5, 6, 7a, 8, 11, 11a, 12, 17, 17a, 19

# Änderungen in Art. 4 DSGVO: Transparenz

## Abs.4

Die **Beschaffung** der **Personendaten** und insbesondere der **Zweck ihrer Bearbeitung** müssen für die betroffene Person **erkennbar** sein.

# Änderungen in Art. 4 DSGVO: Einwilligung

## Abs. 5

Ist für die Bearbeitung von Personendaten die **Einwilligung** der betroffenen Person erforderlich, so ist dies Einwilligung erst gültig, wenn sie **nach angemessener Information freiwillig** erfolgt. Bei der Bearbeitung von **besonders schützenswerten Personendaten** muss sie zudem **ausdrücklich** erfolgen.

# Änderungen in Art. 5 DSGVO: Richtigkeit der Daten

## Abs. 1

Wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern. **Er hat angemessene Massnahmen zu treffen, damit die Daten berichtigt oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind.**

# Änderungen in Art. 6 DSGVO: Grenzüberschreitende Bekanntgabe

## Abs.1

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

# Änderungen in Art. 6 DSGVO: Grenzüberschreitende Bekanntgabe

## Abs. 2

**Fehlt eine Gesetzgebung**, die einen angemessenen Schutz gewährleistet, so können Personendaten ins Ausland nur bekannt gegeben werden, wenn:

- a. **hinreichende Garantien**, insbesondere durch Vertrag, einen angemessenen Schutz im Ausland gewährleisten;
- b. die betroffene Person im Einzelfall eingewilligt hat;

# Änderungen in Art. 6 DSGVO: Grenzüberschreitende Bekanntgabe

- c. die Bearbeitung in **unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags** steht und es sich um Personendaten des **Vertragspartners** handelt;
- d. die Bekanntgabe im Einzelfall entweder für die Wahrung eines **überwiegenden öffentlichen Interesses** oder für die **Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist**;

# Änderungen in Art. 6 DSGVO: Grenzüberschreitende Bekanntgabe

- e. die Bekanntgabe im **Einzelfall** erforderlich ist, um das **Leben** oder die **körperliche Integrität** der betroffenen Person **zu schützen**;
- f. die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat;

# Änderungen in Art. 6 DSGVO: Grenzüberschreitende Bekanntgabe

- g. die **Bekanntgabe innerhalb derselben juristischen Person** oder Gesellschaft oder zwischen juristischen Personen oder Gesellschaften, die einer **einheitlichen Leitung** unterstehen, stattfindet, sofern die **Beteiligten Datenschutzregeln unterstehen, welche einen angemessenen Schutz gewährleisten.**

# Neu: Informationspflicht gemäss Art. 7 a DSGVO

## Abs.1

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.

# Informationspflicht gemäss Art. 7a DSGVO

## Abs. 2

Der betroffenen Person sind **mindestens** mitzuteilen:

- a. der Inhaber der Datensammlung;
- b. der Zweck des Bearbeitens;
- c. die Kategorien der Datenempfänger, wenn eine Datenbekanntgabe vorgesehen ist.

# Informationspflicht gemäss Art. 7a DSG

## Abs. 3

Wenn Daten **nicht bei der betroffenen Person beschafft werden**, hat deren Information **spätestens bei Beginn der Speicherung der Daten** oder, wenn auf die Speicherung verzichtet wird, **mit der ersten Bekanntgabe an Dritte zu** erfolgen.

# Informationspflicht gemäss Art. 7a DSG

## Abs. 4

Die **Informationspflicht des Inhabers der Datensammlung entfällt**, wenn die **betreffene Person bereits informiert** wurde oder, in Fällen nach Absatz 3, wenn:

- a. die Speicherung oder die Bekanntgabe der Daten **ausdrücklich durch das Gesetz vorgesehen** ist; oder
- b. die **Information nicht** oder nur mit **unverhältnismässigem Aufwand möglich** ist.

# Verstärkung der Transparenz beim Auskunftsrecht Art. 8 DSGVO

## Abs. 2

Der Inhaber der Datensammlung muss der betroffenen Person mitteilen:

- a. alle über sie in der Datensammlung vorhandenen Daten **einschliesslich der verfügbaren Angaben über die Herkunft der Daten;**

# Zertifizierungsverfahren nach Art.11 DSGVO

- Hersteller von Datenbearbeitungssystemen oder -programmen, Private oder Bundesorgane können ihre Systeme, Verfahren und ihre Organisation durch eine unabhängige Stelle zertifizieren lassen
- Einzelheiten werden in der Verordnung über die Datenschutzzertifizierungen geregelt

# Anmeldung der Datensammlung nach Art. 11 a DSGVO:

- Regelmässige Bearbeitung von besonders schützenswerten Daten oder Persönlichkeitsprofilen
- Regelmässige Bekanntgabe von Personendaten an Dritte
- **Neu: Auch wenn die Bearbeitung für die betroffene Person erkennbar ist, muss angemeldet werden**

# Ausnahmen von dieser Anmeldepflicht

- Gesetzliche Bearbeitungspflicht
- Ausnahme durch Verordnung
- Veröffentlichung im red. Teil eines periodisch erscheinenden Mediums und keine Weitergabe an Dritte ohne Kenntnis der betroffenen Person
- Journalisten
- Datenschutzzertifiziert
- Ernennung eines unabhängigen Datenschutzbeauftragten und Meldung an EDÖB

# Persönlichkeitsverletzungen nach Art. 12 DSGVO

Abs. 2

Er darf insbesondere nicht:

- a. Personendaten entgegen den Grundsätzen der Artikel 4, 5 Absatz 1 und 7 Absatz 1 bearbeiten

**➔ kein Rechtfertigungsgrund mehr  
zugelassen!**

# Bekanntgabe von Personendaten durch Bundesorgane Art. 19 DSGVO

- Einwilligung der Person muss neu **ausdrücklich** vorliegen
- auch bei einem Zugänglichmachen ihrer Personendaten kann eine Person die Bekanntgabe durch Bundesorgane unterbinden

# Übergangsbestimmungen

Die Inhaber von Datensammlungen erhalten eine einjährige Frist ab Inkrafttreten des Gesetzes, um die erforderlichen Massnahmen zu ergreifen, welche die Neuerungen des DSG erfordern.

# Die wesentlichen Neuerungen der VDSG

- Einführung elektronisches Auskunftsrecht
- Regelung der Ausnahmen der Anmeldepflicht von Datensammlungen
- Regelung der Stellung des Datenschutzverantwortlichen eines Unternehmens oder eines Bundesorgans

# Elektronisches Auskunftsrecht nach Art. 1 VDSG

## **Elektronisches Auskunftsrecht nach Art. 1 VDSG**

- Voraussetzungen dafür sind:
- Der Inhaber der Datensammlung sieht dies ausdrücklich vor und trifft angemessene Massnahmen, um
- die Identifizierung der betroffenen Person sicherzustellen (lit a.); und
- die persönlichen Daten der betroffenen Person bei der Auskunftserteilung vor dem Zugriff unberechtigter Dritter zu schützen (lit. b).

# Ausnahmen von der Anmeldepflicht von Datensammlungen

Folgende Datensammlungen sind  
ausgenommen:

- Von Lieferanten und Kunden, falls keine besonders schützenswerte Daten oder Persönlichkeitsprofile enthalten sind
- mit nicht personenbezogenen Zwecken
- archivierte DS, falls Aufbewahrung aus historischen oder wissenschaftlichen Gründen erfolgt

# Ausnahmen von der Anmeldepflicht von Datensammlungen

- falls Daten enthalten sind, die schon veröffentlicht oder die betroffene Person allgemein zugänglich gemacht und deren Bearbeitung sie nicht untersagt hat
- Daten, die der Erfüllung nach Art. 10 VDSG dienen
- Buchhaltungsunterlagen
- Hilfsdatensammlungen für die Personalverwaltung, soweit sie keine besonders schützenswerten Personendaten oder Persönlichkeitsprofile enthalten.

# Datenschutzverantwortlicher nach Art. 12a VDSG

- Ernennung eines Datenschutzverantwortlichen, der gewisse Anforderungen erfüllt (Art. 12 Abs.2, 12b DSGVO)
- Meldung an EDÖB

⇒ Befreiung von der Anmeldepflicht

# Anforderungen an Datenschutzbeauftragten

Der Inhaber einer Datensammlung kann einen Mitarbeiter oder einen Dritten als Datenschutzverantwortlichen bezeichnen. Dieser darf keine anderen Tätigkeiten ausüben, welche mit seinen Aufgaben als Datenschutzverantwortlicher unvereinbar sind und muss über die notwendigen Fachkenntnisse verfügen.

# Unabhängigkeit (1)

- Gliederung innerhalb der Hierarchie des Unternehmens nicht entscheidend, besser aber direkt der Geschäftsleitung des Inhabers der Datensammlung unterstellt.
- Datenschutzaufgaben dürfen nicht mit anderen Aufgaben kollidieren: Grundsätzlich ist Kumulation mit Amt Informatiksicherheitsbeauftragter oder Leiter Rechtsdienst aber denkbar

# Unabhängigkeit (2)

- Datenschutzbeauftragter muss selber auch für Einhaltung der Unabhängigkeit besorgt sein: Verzicht auf Tätigkeiten, welche mit seinen datenschützerischen Aufgaben in Konflikt stehen könnten.

# Aufgaben des Datenschutzbeauftragten Art. 12 b VDSG

- Prüfung der Bearbeitung von Personendaten
  - Empfehlung von Korrekturmaßnahmen bei Verletzung von Datenschutzvorschriften
  - Führung einer Liste der Datensammlungen
  - Schulung des Personals, Begutachtung Projekte, Erlass von Weisungen
- ⇒ keine Haftung des Datenschutzbeauftragten falls Inhaber der Datensammlung DSGVO verletzt

# Fachkenntnisse

- Datenschutzgesetzgebung
- technische Standards
- Organisation des Inhabers der Datensammlung
- Einzelheiten der Bearbeitung von Personendaten

# Neu: Die VDSZ

Regelt das Zertifizierungsverfahren für:

- Organisation und Verfahren des Datenschutzes  
(Datenschutzmanagementsysteme)
- Produkte (Hardware, Software, Systeme für automatisierte Datenbearbeitungsverfahren)
- Es ist je eine separate Akkreditierung notwendig!

# Mindestanforderungen an das Zertifizierungsverfahren

- Vorhandensein eines Begutachtungs- und Prüfungsrasters
- Festlegung des Ablaufs des Verfahrens:  
Regelung des Vorgehens bei festgestellten Unregelmässigkeiten
- Verweis auf Art. 4-6 VDSZ und Anhang 2 der Akkreditierungs- und Bezeichnungsverordnung (SR 946.512)

# Zertifizierung von Organisation und Verfahren (Art. 4 VDSZ)

- Es können einzelne oder die Gesamtheit der Datenbearbeitungsverfahren zertifiziert werden.
- Gegenstand der Zertifizierung bildet das Datenschutzmanagementsystem

# Datenschutz- managementsysteme

Dieses umfasst:

- die Datenschutzpolitik
- Dokumentation von Zielen und Massnahmen, mit denen der Datenschutz und die Datensicherheit gewährleistet werden sollen
- org. und technische Vorkehrungen zur Verwirklichung der festgelegten Ziele und Massnahmen insbes. Vorkehrungen zur Behebung festgestellter Mängel

# Definition Datenschutzpolitik

Grundlagendokument, welches die Grundzüge des Datenschutzes in der betreffenden Organisation vorgibt und die entsprechende Selbstverpflichtung aufzeigt. Der Ansatz der organisatorischen Massnahmen wird darin beschrieben, mit welchen die datenschutzrechtlichen Vorgaben eingehalten werden sollen.

# Achtung!

Die Ausnahme von der Pflicht zur Anmeldung von Datensammlungen nach Art. 11 a Abs. 5 lit. f DSGVO ist nur anwendbar, wenn sämtliche Datenbearbeitungen, denen eine Datensammlung dient, zertifiziert sind.

# Zertifizierung von Produkten nach Art. 5 VDSZ

Zertifizierbar sind Produkte, die hauptsächlich der Bearbeitung von Personendaten dienen oder bei deren Benutzung Personendaten generiert werden.

# Gegenstand der Prüfung von Produkten (1)

Produktimmanente Gewährleistung von:

- Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der bearbeiteten Personendaten
- Vermeidung nicht zweckerforderlicher Generierung, Speicherung oder anderer Bearbeitung von Personendaten

# Gegenstand der Prüfung von Produkten (2)

- Transparenz und Nachvollziehbarkeit der automatisierten Bearbeitung von Personendaten, die im Rahmen der v. Hersteller festgelegten Funktionalität eines Produktes erfolgt
- technischen Massnahmen zur Unterstützung des Anwenders bei der Einhaltung weiterer Datenschutzgrundsätze und -pflichten

# Gültigkeit der Datenschutz Zertifizierung

- Datenschutzmanagement: während drei Jahren gültig. Jährliche summarische Überprüfung der Zertifizierungsvoraussetzungen.
- Produkte: zwei Jahre gültig. Ein Produkt muss neu zertifiziert werden, sobald daran wesentliche Änderungen vorgenommen werden.

# Sanktionen Art. 9 VDSZ

Sistierung oder Entzug der Zertifizierung bei vorliegen schwerer Mängel:

- wesentliche Voraussetzungen der Datenschutzzertifizierung nicht mehr erfüllt
- Zertifizierung wird in irreführender/missbräuchlicher Art und Weise verwendet

Beurteilung und Verfahren im Falle von Streitigkeiten richtet sich nach den anwendbaren Bestimmungen des Zivilrechts. Meldung an EDÖB durch Zertifizierungsstelle

# Ich danke für Ihre Aufmerksamkeit

HINWEISE AUF PUBLIKATIONEN

[www.dieadvokatur.ch](http://www.dieadvokatur.ch)

[www.itandlaw.ch](http://www.itandlaw.ch)

WEITERBILDUNGSMÖGLICHKEITEN  
AUCH IT-RECHT

[www.hslu.ch](http://www.hslu.ch)

**Prof. Ursula Sury**

**Rechtsanwältin**

**Alpenquai 4**

**6005 Luzern**