DATA PROTECTION

EU-GDPR / EU-DSGVO / CH-DSG

Summary, Priorities and Implementation

Michael P. Hofmann
CEO 7iSolutions AG
MIT MS, dipl.Ing.ETH, lic.oec.HSG

About me

Who am I?

Michael P. Hofmann

15 years	7iSolutions AG, Rapperswil/Zurich CEO
4 years	Credit-Suisse Investment Bank, New York Financial Control / Global Project Director
5 years	Credit-Suisse, Zürich Head IT-Controlling
2001	MS Management MIT Business-School, Cambridge, USA
1991	lic. oec. HSG Hochschule St.Gallen, Schweiz
1989	dipl. Informatik-Ing. ETH ETH Zürich, Schweiz

7iSolutions AG

Focus	Modern e-business solutions Innovative projects
	Remote support and training
	Professional open-source solutions
	GDPR
Customers	Universities, Engineering, Startups
Since	2003

Connect ...

Mail: michael.hofmann@7isolutions.com
LinkedIn: www.linkedin.com/in/mphofmann

TABLE OF CONTENTS

Table of contents

Release Notes 2018-05

- Required for all websites
- Risk employees
- CH date 2019
- USA Privacy Shield

1 INTRODUCTION
Overview

EU General Data Protection Regulation - Everything at a glance

EU-GDPR
eur-lex.europa.eu

since 25.5.2018

99 articles and
173 recitals

Person with personal data (normal & special)

Is owner of its data and allows respective processing

Rights: 1. Right of information 2. Right of access 3. Right to object
4. Right to correct 5. Right to erasure 6. Right of data portability
May complain and is entitled to compensation for misdemeanors

Union, EU and CH

Union = EU + EU-equivalent + companies with EU model clauses

=> CH doesn't have a choice and needs to adapt quickly.

Company

DPO*
Controllers & responsibilities

Data breaches policy (72h)

Processing overviews*

Burden of proof e.g. consent

EU representative

Webseite About us Privacy policy Cookie law
Consent (with privacy by default)

Processes Consent Controller
Impact assessment (DPIA) Privacy by design

Endpoints
Pers.data
DPIA, Encryption?

Systems
Pers.data
DPIA, Encryption?

Processors
In Union
DPIA, Liability?

Backups Pers.data Encryption?

<30 days

Supervisory authority

Have large competences

Can impose high fines
(up to €20m or 4% of revenues)
and keep them

Market location principle

Appeals court

Unclear

Practice of jurisprudence in detail?
From entrepreneurial to picky
Risk from "Abmahner"?

* = with exceptions

1 INTRODUCTION
Overview

What is personal data and who does it concern?

It concerns the collection, processing and use of personal data of natural persons residing in the EU** or "resident" in the EU**.

since 25. May 2018

This applies to all companies / authorities with a seat, branch or a processor in the EU**. But also in all cases where data of EU citizens are processed by processors in connection with the sale of goods and services.

** Applies also to all natural persons in the CH from the end of 2019 at the latest (see parliament). Otherwise, CH will be listed on the "black list" of the EU.

Obvious	Less obvious	Special
Name	Car license plate	Videos
Address	Customer number	Political opinion
Employer	Processing number	Union membership
Phone and email	Transaction documents	Health data
Birthday, place of birth, nationality	Financial information	Biometric data
Credit card data, personal ids	Personal coupons	Genetic data
Social security numbers	IP- and MAC addresses	Ethnic origin

1 INTRODUCTION
Overview

The most important terms

English	Deutsch	Note
GDPR	**DSGVO / DSG**	General Data Protection Regulation / Datenschutz-Grundverordnung / Datenschutz-Gesetz
Regulation	**Verordnung**	Act that is immediately valid after its adoption. Implements a law.
Market location prin.	**Marktortprinzip**	The place where providers and recipients meet, respectively the destination country.
Union	**Union**	EU and countries with equivalent data protection (u.a. CH, CA, AR, IL, Privacy Shield). For third countries: Companies must fulfill EU model clauses and have them approved. Otherwise it is forbidden to store personal data there.
Rights	**Rechte**	The data subject (i.e. person) has rights that are protected by GDPR.
Privacy by default		Obtain a consent for each type of processing (z.B. empty checkboxes by terms).
Privacy by design		Processes and solutions must be designed and developed in accordance with GDPR.
Data Controller	**Verantwortlicher**	Is liable and liability is not delegable.
Data Processor	**Auftragsverarbeiter**	Is also liable if he has access to personal data (e.g., hosting provider).

1 INTRODUCTION
Overview

The most important summarized

Who does it concern?
- Affects all companies that process personal data.
- These are legal companies, public institutions, foundations, associations, etc.
  ... actually everybody, except natural persons.

What changes?
- So far data protection was a recommendation.
- Now it is a regulation from authorities with high fines that they can keep.

Deadlines?
- Since 25.5.2018: all companies that have any relation to the EU. That is ~ 75% of all companies of CH.
- From the end of 2019 at the latest: all companies of CH, when CH-DSG≅EU-GDPR applies (see parliament), with total revision of CH-DSG: minimal, punctual deviations.

Risk?
- High fines possible: up to € 20m or 4% of sales, whichever is higher.
- Is a regulation, i.e. the authority can issue the fine and keep the money directly.
- Market location principle (i.e. the physical location of processing is irrelevant).
- Could be a "paradise" for “Abmahner” (~German debt collector firms).
- The practice of the supervisory authorities is still unclear:
  - Interpretation of the regulation by the supervisory authorities.
  - How fast do the requirements have to be implemented exactly how?
- It is generally not possible to fulfill everything.

1 INTRODUCTION
EU-GDPR

What's in the EU-GDPR?

Ch. 1: General provisions

§1 Objective
- Protection of data of persons
- Respecting the rights of persons

§2/3 Scope
- Market location principle (extraterritorial).

§4 Definitions
- Data subject
- Personal data: very broad definition
  - Normal
  - Special (z.B. biometric, political)
- Processing (normal oder cross-border)
- Pseudonymization, profiling
- Consent
- Controller
- Processor
- Supervisory authority

Ch. 2: Principles

§5 Principles relating to processing
- **Lawfully** (fairness)
- **Transparent** (for data subject)
- **Data minimisation** (delete remaining data)

§6/7/8/9 Consent
- Required everywhere (for every process).
- Burden of proof
- Special data must be protected additionally.

1 INTRODUCTION
EU-GDPR

What's in the EU-GDPR?

Ch. 3: Rights of data subject

§12 Transparent information & communication
- Transparent.
- Easy to understand.
- First information for free. If excessive requests, then paid.
- Immediate execution (<30 Tage).

§13/14 Information to be provided
- Transparent what data is collected.

$15 Right of access
- Right to know what data is being processed.

$16 Right to rectification

$17 Right to erasure
- Legal requirements prevail.

§18 Right to restrict processing
- Consents can be withdrawn.

§19 Notification obligation
- Regarding corrections and deletions.

§20 Right to data portability
- Right to export his data.
- Export in an usual data format.

§21 Right to object
- Consents can be withdrawn.

§22/23 Special cases

1 INTRODUCTION
EU-GDPR

What's in the EU-GDPR?

Ch. 4: Controller and processor

§24/25/26 Responsibility, technology, "by default"
- Appropriate implementation (such as technology, pseudonymisation, data minimization)
- Shared responsibility

§27 Representatives of non-union controllers

§28/29 Processor
- Contract as basis (very restrictive)
- Model clauses

§30/31 Records of processing activities**
- System overview with apps, data types, organization, implementation of data protection

§32 Security of processing
- Appropriate measures relative to risk, such as pseudonymisation, encryption

§33 Notification of data breaches
- max. 72 h with description

§34 Communication of data breaches to subject
- Immediately if risk to affected person

§35 Data protection impact assessment (DPIA)

§36 Consultation with the supervisory authority
- If high risk, then seek advice.
- Especially if: automatic profiling, special data.

§37 Designation of data protection officer

§38 Position of the DPO

§39 Tasks of the DPO
- Designation by controllers/processors
- Common tasks such as contact point, advice, briefing, monitoring, etc.

§40/41 Codes of conduct and monitoring

§42/43 Certification and certification bodies
- Code of conduct and association work

** only if >250 employees or critical process or recurring usage … this is basically everything.

1 INTRODUCTION
EU-GDPR

What's in the EU-GDPR?

Ch. 5: Transfers of personal data

§44/45/46 General principle for transfers
- Only permissible if compliant with regulations.

§47 Binding corporate rules
- Will be approved by the supervising authority.

§48/49/50 Other

EU-GDPR Union: Personal data may be transmitted and processed from the Union if:

1. **EU country**
2. **Country with equivalent data protection** (u.a. CH, CA, AR, IL)
3. Companies from third countries (a.o. USA), if they fulfill the **EU model clauses** or corporate group with "Binding Corporate Rules".

Otherwise it is forbidden.

Ch. 6: Indep. supervisory authority

§51-56 Supervisory authority and competences
- Has to be set up per member state
- Cooperation and mutual assistance

§57 Tasks
- Application and monitoring of GDPR
- Raise awareness (public and controllers)
- Investigate complaints from data subjects
- Conduct investigations in companies

§58 Powers
- Conduct data protection audits
- Request access to all personal data
- Give instructions to controllers and processors

Remedy powers:
- Warn controllers and processors
- Impose restriction on processing
- Impose fines

§59 Activity report

1 INTRODUCTION
EU-GDPR

What's in the EU-GDPR?

Ch. 8: Cooperation & consistency

§77 Right to lodge a complaint
- Submission by affected person

§78 Right to an effective judicial remedy against supervisory authority

§79 Right to an effective judicial remedy against controller or processor

§80/81 Representation and suspension

§82 Right to compensation and liability

§83 Conditions for imposing fines
- Depending on the circumstances of the case
- Up to €20m or 4% or revenues, whichever is higher
- Mainly: §5-9, §12-22, §44-49, §58, §85-91

§84 Penalties

Ch. 7-11

Ch.7: Cooperation and consistency

Ch.9: Provisions relating specific situations

Ch.10: Delegated acts and implementing acts

Ch.11: Final provisions

1 INTRODUCTION
Other

What else is to be considered?

EU vs. USA

Europa	USA
EU-GDPR Subject to EU rules and regulations	Data protection weakly implemented (“Privacy Shield” only) “Patriot Act” with the greatest possible freedom of action
Rights of data subjects and supervisory authority Data usually remains within the Union	Self-regulation of market participants and no authority Data is transmitted without restriction
Fines	No consequences, respectively loss of image only

The **EU model clauses** regulate the exchange of data between the Union and companies.

ePrivacy Regulation (EU)

Content:

- Online tracking (z.B. shop cart, Google-Analytics)
- Right to encryption
- Addressing consumers for advertising purposes

~2019

Other

Cloud Act
APEC Privacy Framework
China Regulations
Russian Regulations

2 ANALYSIS
Requirements

What do you have to do?

A Public requirements

Websites (all - customer oriented and technical)
- About us (or imprint)
- Privacy policy (company specific)
- Cookie consent (only if used)
- Privacy by default (empty checkboxes, no coupling)

Newsletter
- Subscriptions with double opt-in
- Mailings only with consent
- Implement unsubscriptions

Customer accounts
- Consent per processing purpose
- Empty checkboxes everywhere
- Simple language
- Implement unsubscriptions

Email in Germany
- Signature is required for business mails.

B Corporate requirements

General
- Separate private and business data
  - Example: Audit by supervisory authority: “I would like to have access to all customer data.”

Data protection officer
- Assign with appropriate competences
- Tasks: Training and control

Policy
- Controllers and processors
- Behavior in case of data breaches (72 h)

Processing overviews
- Identification of personal data
- Data security and impact assessment

Partner respectively processors
- Check
- Clarify liability

Michael P. Hofmann / michael.hofmann@7isolutions.com / +41 78 796 4010

2 ANALYSIS
Requirements

What do you have to do?

C Process requirements

General
- Use GDPR compatible solutions only
- Check processors (a.o. liability)

Process
- Identification of personal data
- List of used apps per process
- Risk and data protection impact assessment
  - If high, implement measure

Per endpoint (PC, notebook, mobiles)
- Identification of personal data
- Separate private and business data
- Encryption, if high risk

Supported measures
- Encryption
- Pseudonymization
- Data minimization

D App & infra requirements

Per App, Infra, Backup
- Identification of personal data
- Location of personal data
- Implementation of rights
  - Response within 30 days, if request is appropriate

  1 Right to be informed
  - In advance with consent

  2 Right of access
  - What data about my person exists?

  3 Right to object
  - Consents can be withdrawn.

  4 Right to rectification
  - Data must be corrected.

  5 Right to erasure/restrict
  - If not possible, restrict processing
  - Legal requirements prevail

  6 Right to data portability
  - Data must be exportable.
- Privacy by design

Michael P. Hofmann / michael.hofmann@7isolutions.com / +41 78 796 4010

2 ANALYSIS
“Trouble makers”

If a company does nothing: Who could make trouble?

Supervising authority

Will become active if:

- receiving complaints (from customers, former employees, rejected applicants) e.g. due to false information from employees
- periodic audits

Scope: All requirements

Priority: medium

“Abmahner”**

Can become active if:

- Visible or easy to check items are not ok
- Due to false information provided by employees

Scope: See “A Public requirements”

Priority: high

Current and new customers

If the company is a processor for a customer requesting immediate GDPR compliance.

Scope: All requirements (a.o. liability)

Priority: case by case

Unclear is the practice of the supervisory authorities:

- Interpretation of the regulation by the supervisory authorities.
- How fast do the requirements have to be implement and how precisely?

** ~German debt collector firms

3 IMPLEMENTATION
Priorities

What has to be done by when?

For small companies in CH without relevant EU connection

Implement the most important now

1. **Management and employees**: raise awareness

2. **Everything that can be check from outside**
   - A Public requirements

3. **Strategy:** ensure for later
   - B Corporate requirements
   - C Process requirements
   - D App and infra requirements

Plus:
- **follow data protection discussion** and
- **be ready** to implement additional measures quickly (<30 days), if needed.

For medium companies in CH and/or with a clear EU connection

Implement everything now

See items 1 to 3 on the left, plus:

4. **Organization**
   - B Corporate requirements

5. **Systems:** Create overview and check in detail
   - C Process requirements
     Positive: if ISO-9000 readiness already exists, not much additional effort is required.
   - D App and infra requirements

Michael P. Hofmann / michael.hofmann@7isolutions.com / +41 78 796 4010

3 IMPLEMENTATION
Our offers

How can we support you?

GDPR Management Webinar

- Webinar
  - Summary
  - Priorities
  - Implementation
- Q&A

1-2 h

GDPR Quick Review SMB

- Focus on most important
  - Scope definition
  - Analysis
  - Issues list and priorities

2-6 h

GDPR Project & Implementation

- Scope definition
- Analysis
- Issues list and priorities
- Implementation within company
- Creation of required documentation

effort-based

GDPR Wiki Template & Workbook

- Tool for the implementation
- Contains:
  - Summeries with links
  - Reference solutions
  - Database for the implementation

see gdpr.7isolutions.com

Newsletter … so that you stay up to date in the coming months.

3 IMPLEMENTATION

Our offers - other

Professional, self-hosted, open-source e-business solutions

Projects	Project Mgmt.	Issue Mgmt.	Project Coord.	**Marketing**	Landing Page	Presentation Website	Corporate Website
	Version Control	Extranet & Downloads			Blog Website	News Website	Newsletter
Support	FAQs Wiki	Support Wiki	Support Manual	**Sales**	CRM	Issue Mgmt.	CRM Wiki
	Ticketing System	Q&A Forum	Discourse Forum				
Operations	Issue Mgmt.	Coordination Wiki		**Organization**	Team Wiki	Time Recording	EU-GDPR Wiki
	Custom Solutions				Knowledge Wiki	Password Mgmt.	
Collaboration	Issue Mgmt.	File-Server & Sync	E-Mail Server	**Infrastructure**	Server Mgmt.	System Monitor	Security Mgmt.
					Backup Mgmt.	Upgrade Mgmt.	

… with unlimited users and apps for a fixed price per server.

Next
Shareware

Michael P. Hofmann / michael.hofmann@7isolutions.com / +41 78 796 4010

4 LINKS
Reading list

Some good links

Article

- 2017-07-14 NZZ Schweizer Firmen sind gezwungen, Daten ihrer Kunden besser zu schützen
- 2017-12-13 WEKA Datenschutz: Handlungsbedarf für Schweizer Unternehmen in allen Bereichen
- 2017-12-15 The Economist New EU data rules will get tough on privacy
- 2018-01-12 NZZ Das Parlament lässt sich Zeit mit neuen Regeln beim Datenschutz
- 2018-02-03 NZZ am Sonntag Die EU schützt die Privatsphäre ihrer Bürger - davon profitieren auch Schweizer
- 2018-05-25 NZZ Was das neue EU-Datenschutzgesetz für die Schweiz bedeutet

EU

- EU-GDPR eur-lex.europa.eu (oder dsgvo-gesetz.de)

CH

- CH-DSG www.admin.ch/opc/de/classified-compilation/19920153/
- Data protection officer Switzerland www.edoeb.admin.ch
- Data protection officer Canton ZH dsb.zh.ch

Companies

- Microsoft www.microsoft.com/de-de/trustcenter/compliance/eu-model-clauses
- Amazon Web Services aws.amazon.com/de/data-protection
- Google G Suite support.google.com/a/team/answer/6366832?hl=de

5 Q&A

Questions?

michael.hofmann@7isolutions.com
+41 78 796 4010

See also ...

- gdpr.7isolutions.com
- www.7isolutions.com
- www.mphofmann.com