Homburger

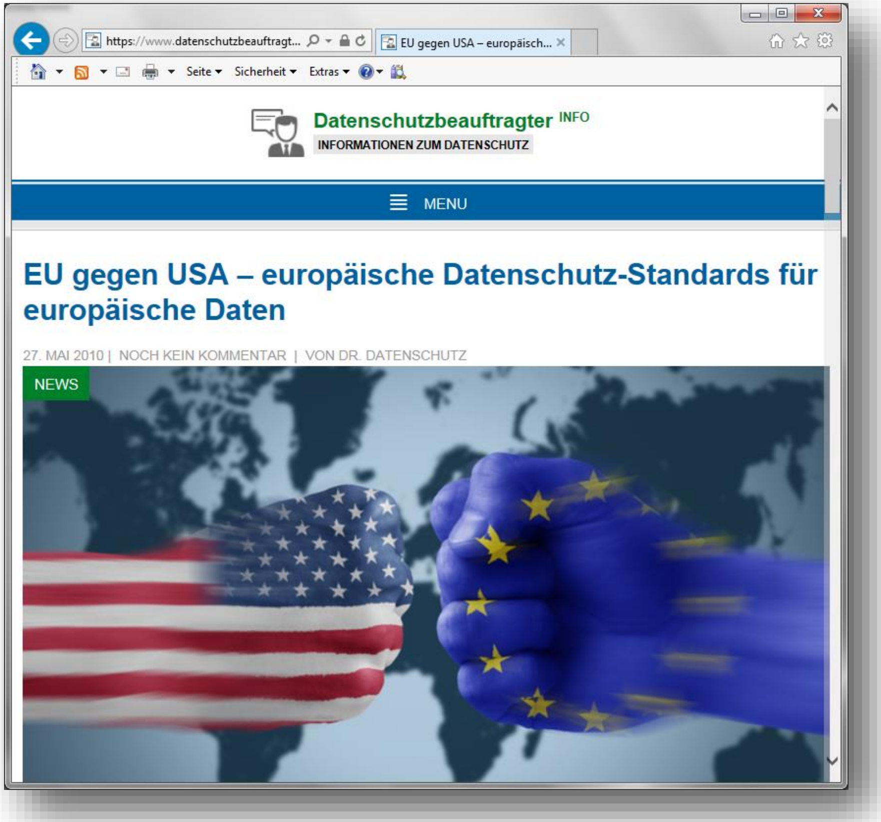
EU General Data Protection Regulation

The new global standard for data protection?

David Rosenthal

October 19, 2016

Version 1.01


https://www.datenschutzbeauftragt...
EU gegen USA – europäisch...
Seite
Sicherheit
Extras
MENU

Datenschutzbeauftragter INFO

INFORMATIONEN ZUM DATENSCHUTZ

EU gegen USA – europäische Datenschutz-Standards für europäische Daten

27. MAI 2010 | NOCH KEIN KOMMENTAR | VON DR. DATENSCHUTZ

NEWS

facebook

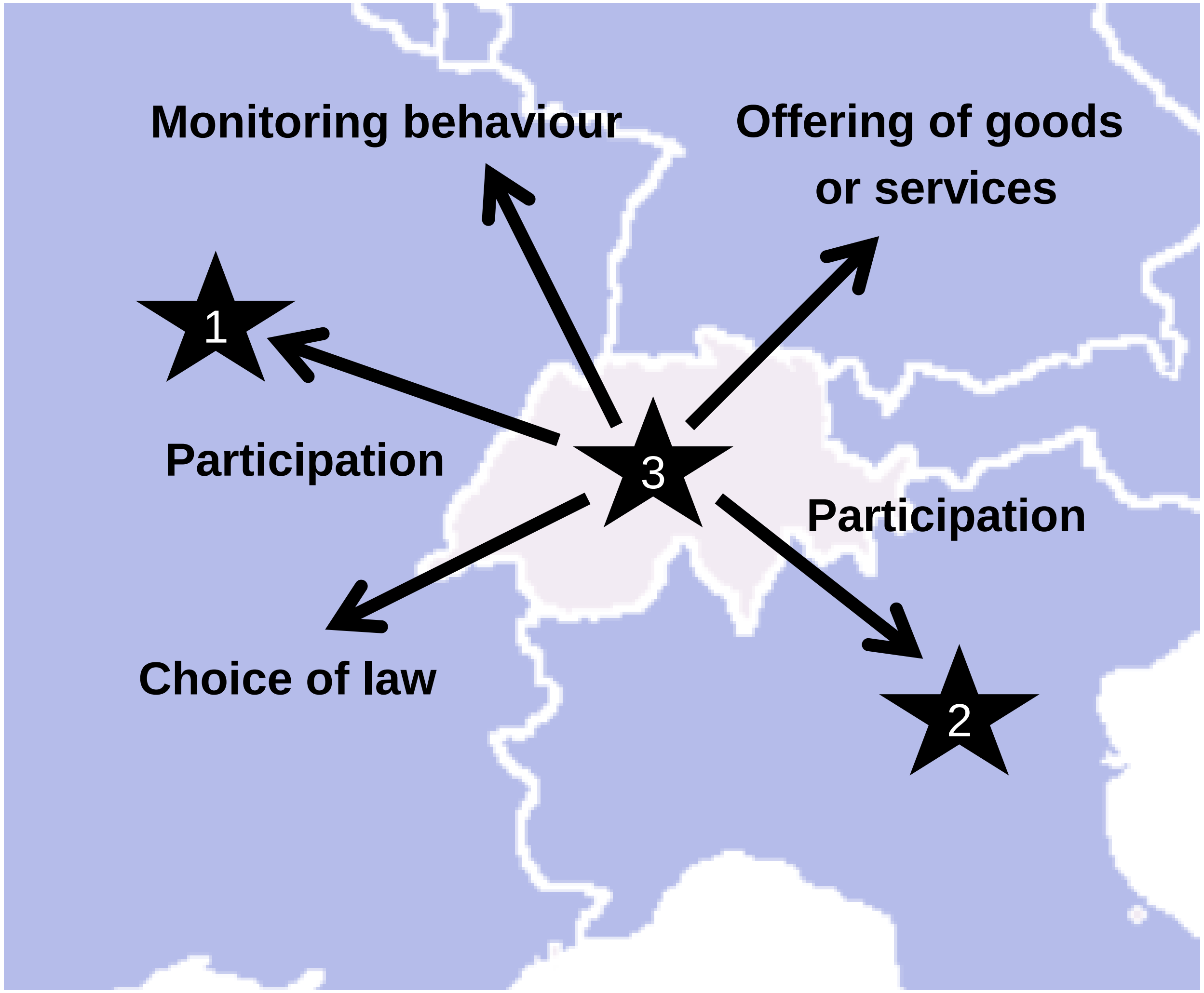
EU (and EEA) law

Targets U.S. companies

Targets online providers

Why should companies in Switzerland bother?

It applies to many of them …



★1 Controller

★2 Processor

★3 Controller or Processor

4%

(of the worldwide turnover or EUR 20m)

Talking about sanctions …

- Each (national) authority may issue **administrative sanctions**
  - They shall be "effective, proportionate and dissuasive"
  - Re governance|data of children: EUR 10 mio. or 2% of worldwide turnover, whichever is higher (revenue of the legal entity at issue, not the entire group)
  - Re substantive rules: EUR 20 mio. or 4% of worldwide turnover
- If administrative sanctions are not possible, **other penalities** are permitted
- Authorities have the powers to **intervene against data processing activities**
  - They can temporarily or permanently stop a certain data processing
  - They are obliged to deal with each complaint of a data subject
- Data subjects can enforce their rights and claims (e.g., damages) by court
  - Associations can act on behalf of data subjects or on their own
- **Note:** Switzerland will introduce sanctions in 2018 as well …

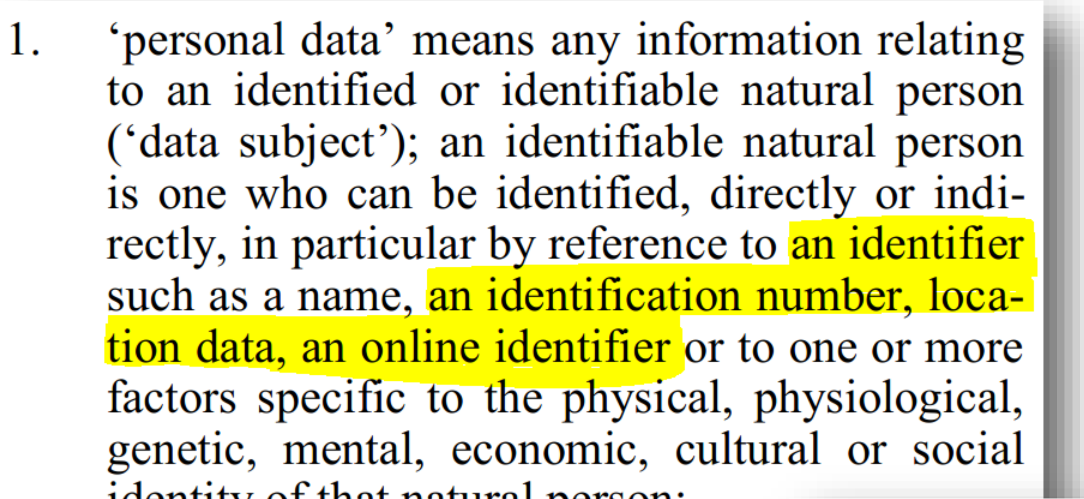
Art. 58, 77-84 GDPR

An overview …

Key changes

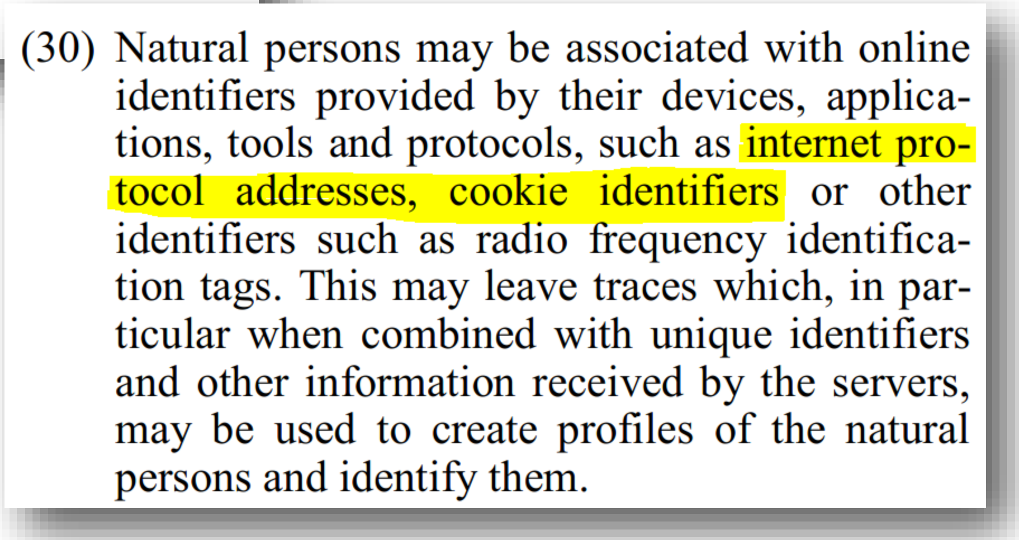
- **Basic concept** (what is permitted, what not) remains unchanged
  - Under EU law, any processing of personal data requires a justification (e.g., consent, compliance with law, legitimate interests)
- **Territorial applicability:** The GDPR also applies to many foreign companies
- **Personal data:** Definition widened (i.e. less room for anonymization)
- **Consent:** Conditions for valid consent have become stricter
- **Information obligations:** Much more information has to be provided
- **Data subject rights:** Data subjects get new access and intervention rights
- **Governance:** The work load in particular re the documentation increases
- **Data exports:** Most rules relevant in practice remain the same
- **Buzzwords:** Privacy by Design & Co. – often old wine in new bottles
- **Sanctions:** Severe sanctions, but really enforceable outside the EU?
- **Time to implement:** May 25, 2018

Personal data



1. 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

The EU increasingly follows an "absolute" approach with regard to the definition of personal data, even though such approach is questionable



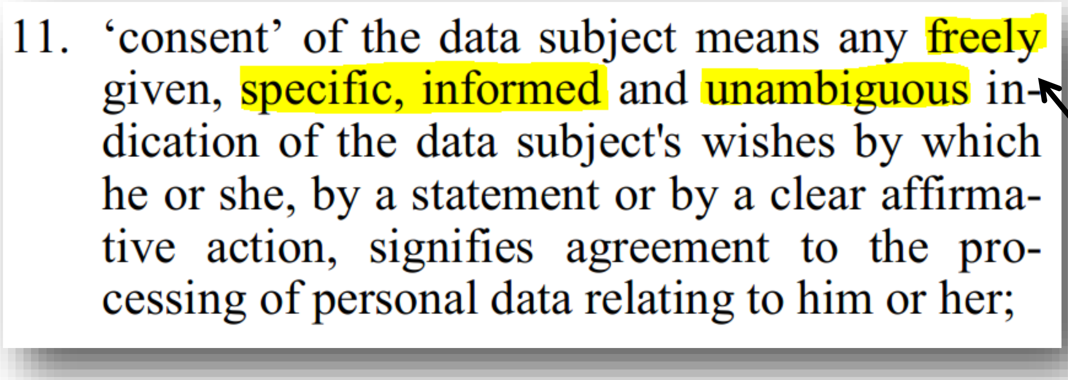
(30) Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

Under the Swiss DPA, the more or less same definition is interpreted pursuant to a "relative" approach, as confirmed in DFC 136 II 508 (Logistep)

Art. 27 GDPR, Consideration 26, 30

Consent

— **Relevance:** Apart from the performance of a contract, a legal obligation and "legitimate interests", consent is the most important grounds for data processing



11. ‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

Shall the consent provided for in a contract be optional with regard to all data processing activities that are not necessary for the performance of the contract (Art. 7(4))?

— Definition corresponds to definition of what is a valid consent under **Swiss law**

— Consent muss be presented **clearly distinguishable from other matters**

— Consent can **always be withdrawn** (with effect for the future; right to erasure)

— Consent that has already been validly obtained in the past continues to be valid

Art. 4(11), 6(1)(a), 7 GDPR

Information duties

- **Principle of transparency** is supplemented by an **obligation to inform** on a number of defined points
  - To the extent the data subject has not yet been informed
  - Also applies in case of indirect data collection (max. 1 month), except where it is impossible, result in a disproportionate effort or defeats the purpose (in which case alternatives such as information on a website shall be pursued)
  - Obligation to inform also applies in case of (later) secondary purposes
- **Consequence:** Extensive privacy notices become mandatory
  - Upon first contact or collection
  - On the website for all cases of indirect data collection not covered otherwise
  - Few exceptions, such as internal investigations
- **Pro memoria:** An obligation to inform may also exist in cases of data breaches

Art. 5, 7, 12-14, 21, 34 GDPR

Inform on what?

- Name, contact details of the controller and data protection officer
- Purposes of use, data categories, categories of recipients (if any)
- Legitimate interests, if relied upon
- Whether exports are intended, whether to a whitelisted country, and if not, where the data subject can obtain a copy of the safeguards used
- Data sources (if data is collected indirectly)
- Period for which data will be stored (or criteria used to determine it)
- Information on the right of the data subject for access, rectification, erasure, restriction, objection and data portability
- Right to withdraw a consent (and eventually the consequences)
- Right to lodge a complaint with the supervisory authority
- Whether the data requested is necessary for the performance of a contract and the consequences of not disclosing the data requested
- Automated decision-making (including profiling), the logic and consequences

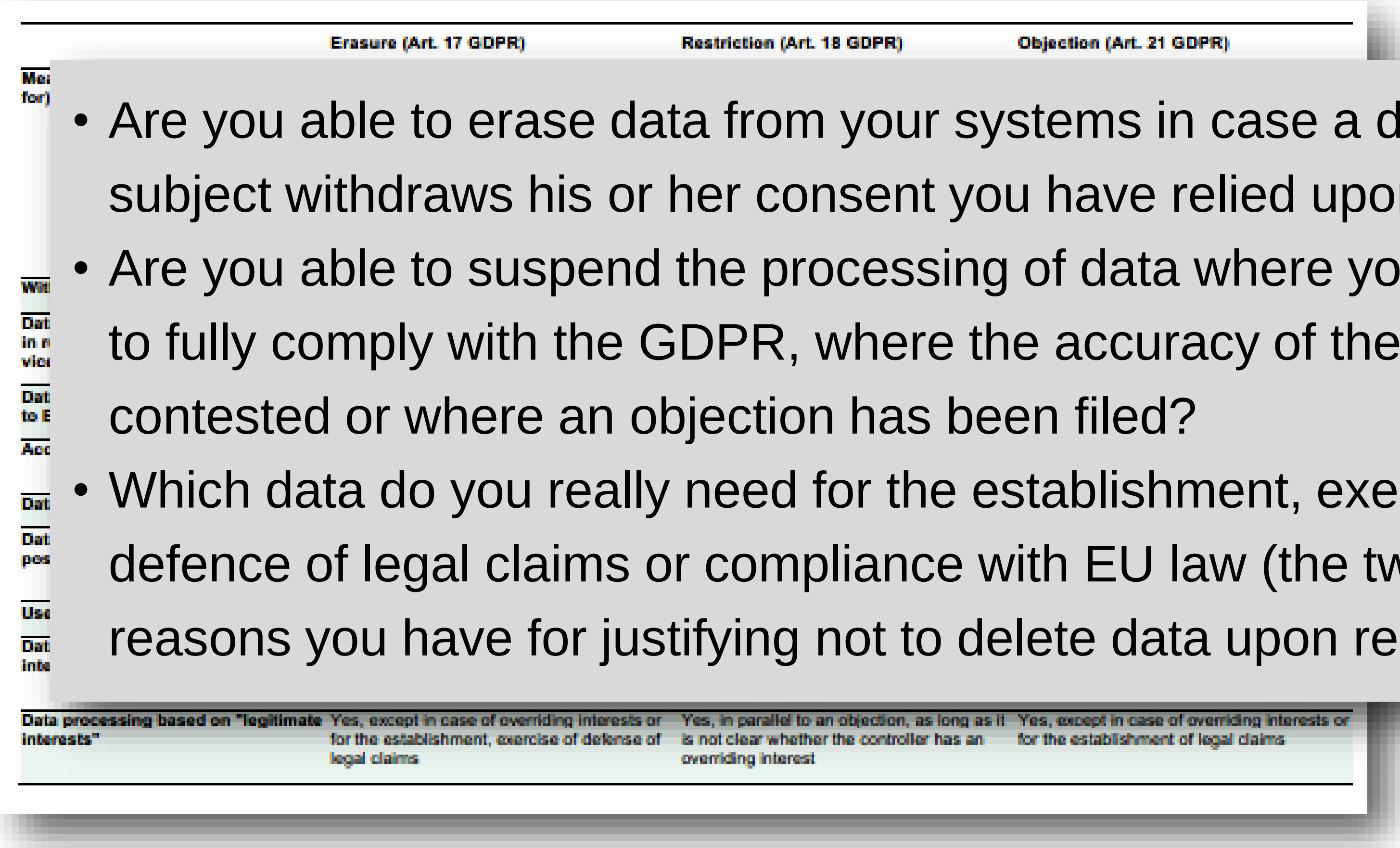
Art. 13, 14 GDPR

Data subject rights

- Data subject rights are significantly **extended** and become more **complicated**
  - It remains unclear to which extent data subjects will make use of them
  - They require **changes** to data processing procedures and systems
- All requests must be complied with at **no charge** and **within one month**
  - Extension of deadline is possible by two months
  - In case of "manifestly unfounded or excessive" requests it is possible to charge a reasonable fee or refuse to act upon the request
  - Previous data recipients may have to be informed of the request
- Right of **access** and **data portability** (= return of own data)
- Right to **rectification**
- Right to **erasure** ("right to be forgotten"), **restriction** (= partial usage ban) and **objection** (= complete usage ban)
- Right to **"human intervention"** in case of automated decision-making

Art. 12, 15-22 GDPR

Erasure, restriction and objection



	Erasure (Art. 17 GDPR)	Restriction (Art. 18 GDPR)	Objection (Art. 21 GDPR)
Mea for)			
Wit			
Dat in r vic			
Dat to E			
Acc			
Dat			
Dat pos			
Use			
Dat inte			
Data processing based on "legitimate interests"	Yes, except in case of overriding interests or for the establishment, exercise of defense of legal claims	Yes, in parallel to an objection, as long as it is not clear whether the controller has an overriding interest	Yes, except in case of overriding interests or for the establishment of legal claims

- Are you able to erase data from your systems in case a data subject withdraws his or her consent you have relied upon?
- Are you able to suspend the processing of data where you failed to fully comply with the GDPR, where the accuracy of the data is contested or where an objection has been filed?
- Which data do you really need for the establishment, exercise or defence of legal claims or compliance with EU law (the two main reasons you have for justifying not to delete data upon request)?

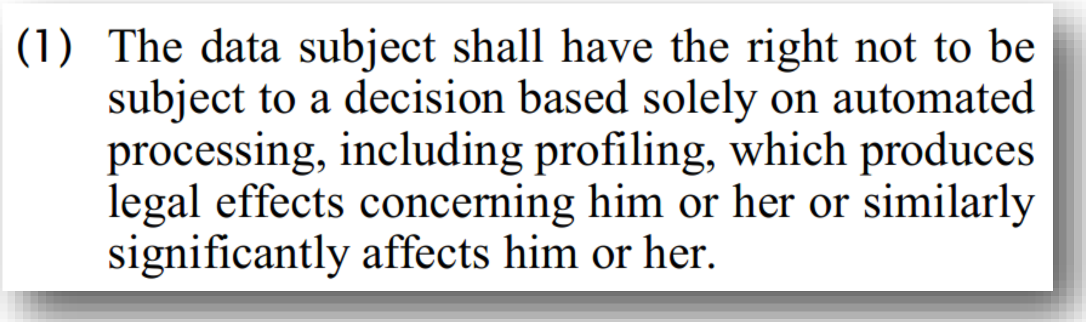
Available at http://www.homburger.ch/dataprotection

Data portability

- **Five preconditions (cumulative)**
  - Personal data of the data subject
  - Provided (by the data subject) to a controller (not just processor)
  - Processing is based on consent or a contract
  - Processing is carried out by automated means
  - Rights and freedoms of other persons are not adversely affected
- **What can the data subject ask for?**
  - Return of the data in a "structured, commonly used and machine-readable format" in order to pass it along to another controller
  - Where technically feasible to have it transmitted directly to the other controller
- **Atypical use cases are still unclear** (the provision aims at Facebook & Co.)
  - Doctors (patient data)? Banks (orders)? Auction platforms (offerings)? Telcos (CDRs)? Online-shops (past orders)? Employers (job application data)?

Automated decisions, profiling

— **Prohibition** or a **right to object?**



(1) The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

The provision aims at automated credit- or e-recruitment decisions without human intervention, but applies to many other cases, e.g., personalized prices, activation of software, security monitoring

— **Option 1:** Profiling or automated decisions are used only where they do not produce legal or similar effects to the data subject (e.g., personalized ads)

— **Option 2:** Profiling or automated decisions are used only for entering into or performing a contract, without sensitive data, and the data subject has the right to present his or her view to a human and have the decision reconsidered

— **Option 3:** The explicit consent is obtained beforehand, and steps are taken to deal with its withdrawal; human intervention must still be possible

Governance

- Concept of **"accountability"**: Controller has to be able to "prove" its compliance
- **Contracts with processors:** Detailed requirements as to what the contract has to cover, but not many changes in substance (exception: veto on subprocessors)
- Maintaining **records of processing activities** becomes mandatory, also for processors; the minimum required content corresponds plus/minus to what is required pursuant to Art. 11a DPA, plus information on exports, retention periods, and technical and organizational measures undertaken
- Obligation to undertake a formal **privacy impact assessment** in case of likely "high risk" projects, and to **prior consultation** of the supervisory authority if the project is indeed of a high (privacy) risk high absent mitigation measures
- If the business of a company is based on the monitoring of individuals or on the processing of sensitive data, then a **data protection officer** must be appointed

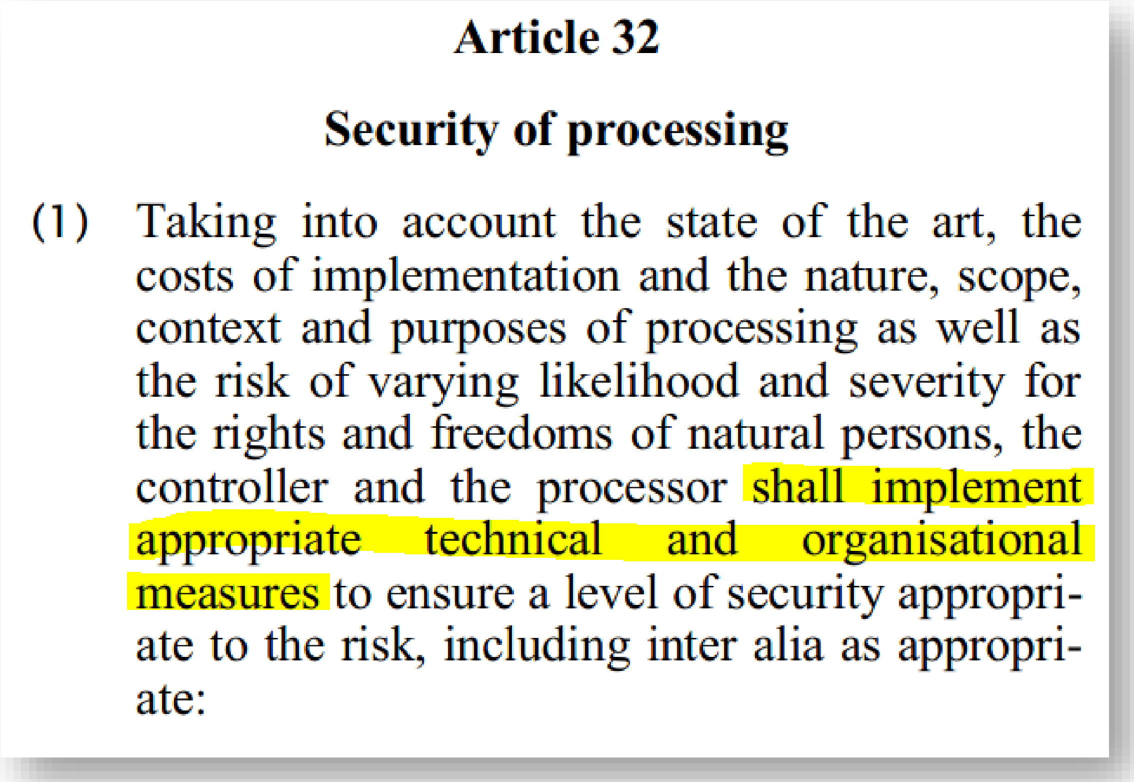
Art. 5, 28, 30, 35-39 GDPR

Exporting data

- **The good news:** Exports that are permitted today in principle remain permitted also under the GDPR
  - Concept of **adequacy decisions** by the European Commission remains
    - Existing decisions keep their validity; Switzerland has the right to be found adequate provided it complies with the revised CoE Convention 108
  - Concept of **contractual safeguards** and **binding corporate rules** (BCRs) continues to work for unsafe third countries (despite the safe harbor decision)
    - BCRs are still subject to approval by the supervisory authority
    - EU model clauses continue to be valid (but are likely to be revised)
- Exports to unsafe third countries may also be undertaken on the basis of approved **code of conducts** and approved **certification mechanisms**
- The provisions are only of limited relevance for exports from non-EU countries
  - The new GDPR concepts are already supported by the existing DPA

And what about security?

Security as a legal obligation



Article 32

Security of processing

(1) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

Art. 5 GDPR:

"… protection against unauthorised or unlawful processing and against accidental loss, destruction or damage …"

Similar provisions are found in articles 24, 25 and 28 GDPR

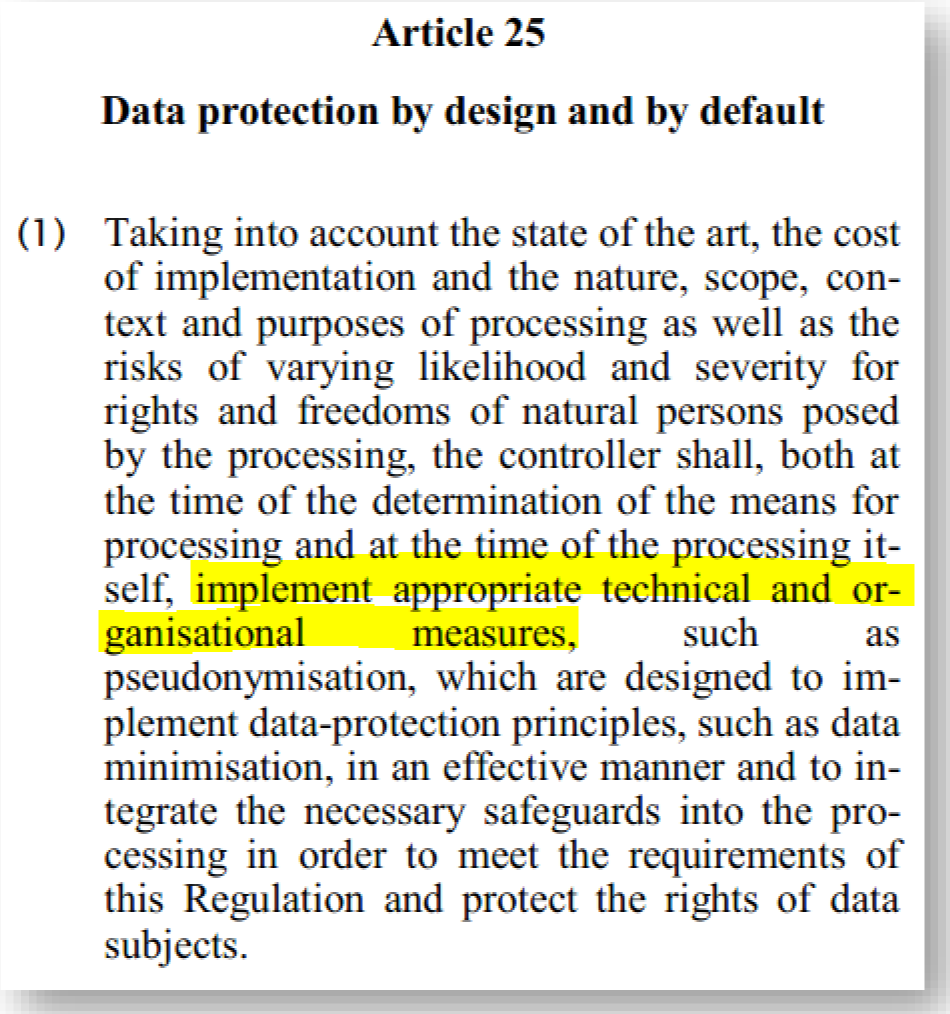
Art. 5, 32, 24, 25, 28 GDPR

Security as a legal obligation

- Technical and organizational measures **to ensure compliance** with principles and rules of data protection and avoid loss or damage of personal data
  - Technical measures: ACL, encryption, pseudonymisation, firewalls, logs, etc.
  - Organizational measures: Policies, instructions, training, audits, etc.
  - Obligation not only to implement security, but also safety (e.g., backups)
- Measures need (only) to be **adequate**, but are to be **documented**, **reviewed regularly**, adapted if necessary and their effectiveness is to be **verified**
  - Obligation of both controllers and processors (i.e. service providers)
- In principle corresponds to obligations under **current Swiss law**, but …
  - The bar has been set higher
  - Sanctions for non-compliance (even if no other unlawful processing occurs)
  - Obligation to prove compliance (security certifications may not be sufficient)

Art. 5, 32, 24, 25, 28 GDPR

Privacy by Design



Article 25

Data protection by design and by default

(1) Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

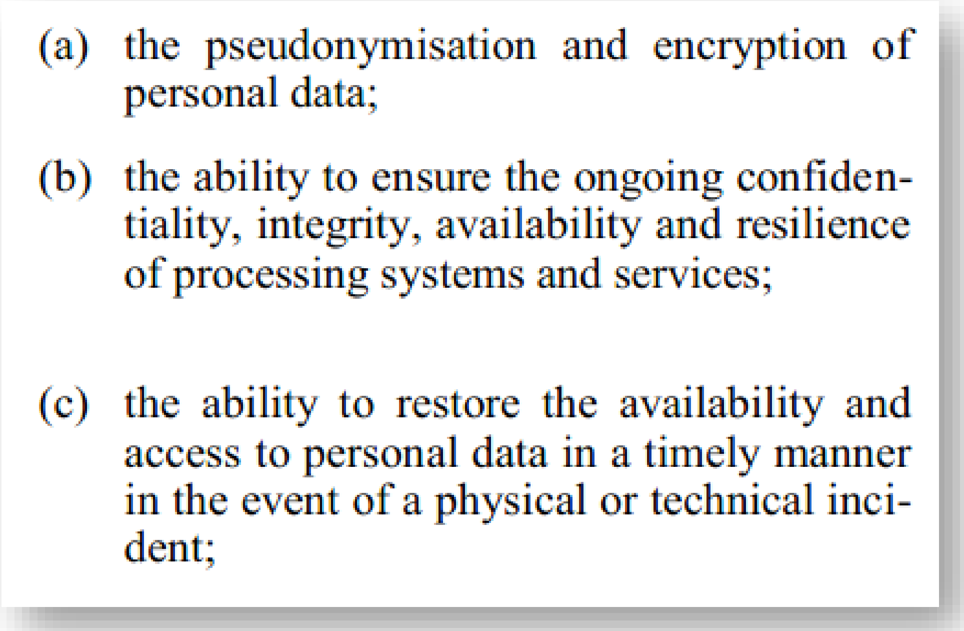
Basically the **same requirement** expressed in other words

"Privacy by Default" as another concept set forth in article 25

Both have become **"privacy buzzwords"**, but their practical meaning remains unclear …

Art. 25 GDPR

No specific measures set forth



(a) the pseudonymisation and encryption of personal data;

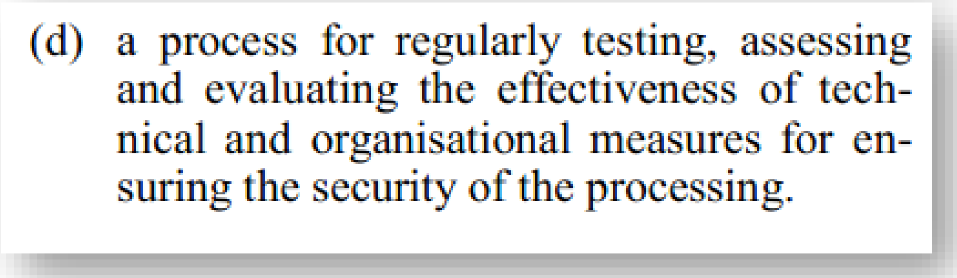
(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

Minimize exposure

Security

Safety | business continuity



(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Validation, management system

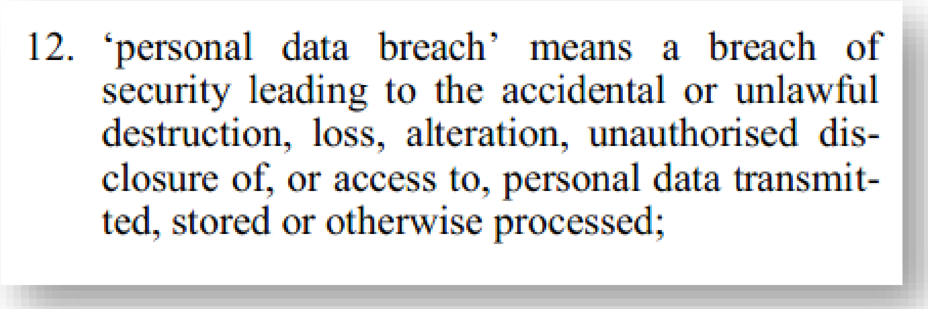
Pseudonymization

- **Replacing identifiers** with randomized codes and keeping the correlation secret
- GDPR does not prescribe this method, but **promotes** it
  - Art. 6 para. 4 let. e GDPR to make new purposes "compatible" with old ones
  - Art. 32, 40 and 89 GDPR as one technical mean to increase data protection
  - Art. 25 GDPR as one mean to implement "Privacy by Design"
  - Art. 11 GDPR partially exempts pseudonymized data from data subject rights
- **However:** Pseudonymized data remains personal data (GDPR still applies)
  - Contrary to the situation under Swiss law
- Nevertheless, be prepared to use it **much more often** in the future (cf. art. 32)
- **Anonymization** is the absence of any identifier, whether in clear-text or code

Art. 4, 6, 11, 25, 32, 40, 89 GDPR

Data Breach Notifications

- **What is a data breach?**
  - Not just every breach of data protection or privacy



12. 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

- *First*, a provision meant to ensure **data security** must have been **breached** or **not complied** with
  - Lack of data security and the controller's intentional breach of the principles of data protection is no data breach
  - Breach of an organizational measure (e.g., a policy) is sufficient
- *Second*, **data control or integrity** must have been negatively **affected**
  - Excessive use of data or misuse for an unlawful purpose is no breach, but the unauthorized access by employees without permission to access data is

Art. 4 GDPR

Data Breach Notifications

- **Each breach** needs to be recorded and **documented** (art. 33 para. 5 GDPR)
- Each breach with a **risk for the data subject** needs to be **notified** to the national **data protection authority** (art. 33 para. 1-4 GDPR)
  - Risk of a physical, monetary or immaterial damage to the data subject
    - e.g. discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality, loss of control over data, other economic or social disadvantages
    - E-mail to wrong recipient? Paper documents sent to the wrong recipient, but returned? A hacker-break-in? Loss of a notebook with encrypted data?
  - What has happened? Which data? Who is affected (and how many)? What are the likely consequences? Measures taken or planned? Contact?
  - Notification to occur within 72 hours following discovery of the breach (explanation and rolling notice if deadline can't be met)

Data Breach Notifications

- Breach with a (ongoing) **likely "high risk"** for the data subject also needs to be **notified to the data subject** itself (art. 34 GDPR)
  - National authority can require a company to notify data subjects
  - Notification only needs to describe the nature of breach (but no details), the likely consequences, the measures taken and contact information
  - Notification has to happen "without undue" delay, i.e. a delay is possible where necessary to avoid further data breaches, damage, etc.
  - If notification results in a "disproportionate" effort: A public communication or similar measure to inform the data subjects in equally effective manner
- **Processors** only need to notify a data breach to the controller (art. 33 para. 2)
- **No "safe harbor" clause** – a notification can be used against the controller
- Non-compliance can be **fined** with up to 2% of the worldwide turnover
- Operations need to establish the **proper processes** and **responsibilities**

Art. 33, 34 GDPR

Final thoughts

Take action

- The GDPR **can't be ignored** in Switzerland
  - Multinationals already consider the GDPR to be a "global" standard
  - Swiss law will follow-up by 2018 with similar concepts, including sanctions
- The area where most improvement is necessary is **governance**
  - Data protection is today handled *ad hoc* at many companies
  - Many of them have no overview of their own processing of data
  - GDPR compliance requires defined processes within an organization
  - Current board-room attention (sanctions!) bears an enormous chance
- Yet, a **risk-based approach** is essential
  - Full GDPR compliance will not be possible; also, many questions remain
  - Risk-based decisions become necessary, but they require an understanding of how data is processed within the organization and where the gaps are
  - No time left for starting the necessary compliance projects

Thank you for your attention!

David Rosenthal
david.rosenthal@homburger.ch
T +41 43 222 16 69

Homburger AG
Prime Tower
Hardstrasse 201 | CH-8005 Zürich
Postfach 314 | CH-8037 Zürich

www.homburger.ch

Additional presentations on the GDPR, a version of the GDPR with its English and German text side-by-side and more useful materials are available at http://www.homburger.ch/dataprotection