General Data Protection Regulation

Rules, Common Mistakes & Challenges

KARLSTAD
UNIVERSITY
SWEDEN

Simone Fischer-Hübner

EU General Data Protection Regulation (GDPR) – Background

- Entered into affect on May 25th 2018 & replaced EU Directive 95/46/EC

Objectives:

- To **harmonize** data protection laws across Europe
- **Modernisation** of Data Protection Rules for the Digital Age
- **Strengthening** the existing **rights** and empowering individuals with more control
- Improved **level of compliance**

Scope:

Applies to the processing of **personal data** by controller/processor

- **established in the EU**
- **outside the EU that offer goods and services** to, or that **monitor, individuals in the EU**.

Definitions

- Art. 4 (I): **‘Personal data’** means any information relating **to an identified or identifiable natural person (‘data subject’);**

- **Types of personal data:**
  - **Explicitly disclosed data** *(e.g., name, delivery address)*

  - **Implicitly disclosed data** incl. meta data *(e.g., IP address, MAC address, cookies, location data, traffic data)*

  - **Derived data** *(e.g., user behavioral profiles)*

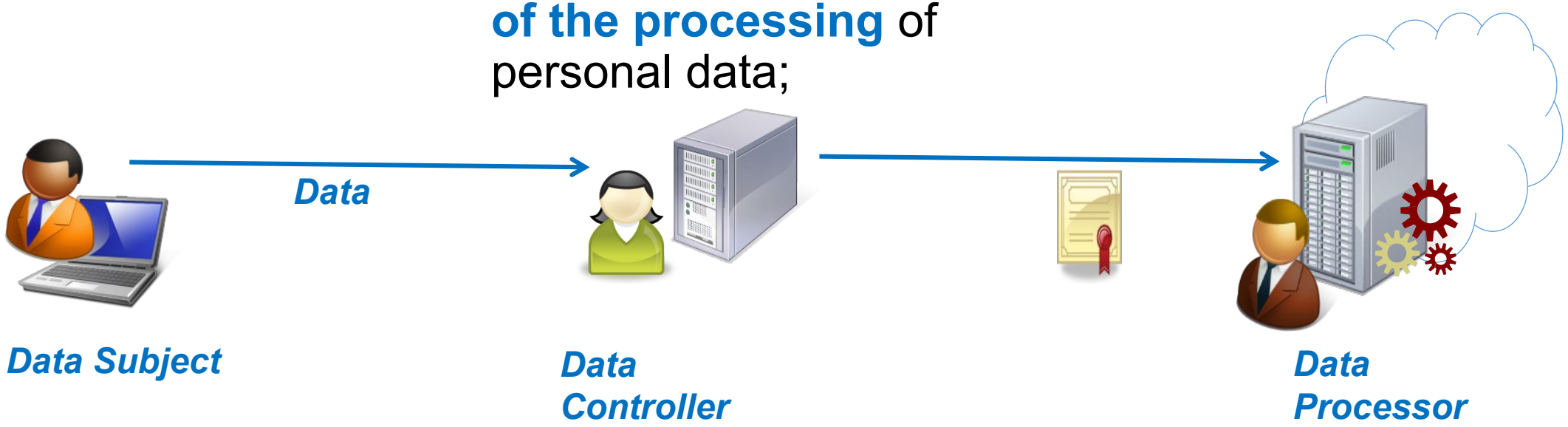
  - **Third party provided data** *(e.g., reputation scores)*

Definitions (II)

- **Art. 4 (1)**
  ”Data Subject”

- **Art. 4 (7) ”Controller”:** a natural or legal person, public authority, agency or other body which, alone or jointly with others, **determines the purposes and means of the processing** of personal data;

- **Art. 4 (8) ”Data Processor”:** a natural or legal person, public authority, agency or other body **which processes personal data on behalf of the controller**;



Principles relating to processing of personal data

(Art. 5):

- lawfulness, fairness and transparency
- purpose limitation
- data minimisation
- data accuracy
- storage limitation
- integrity and confidentiality
- accountability

Lawfulness of processing conditions

(Art. 6):

- **Consent** of the data subject

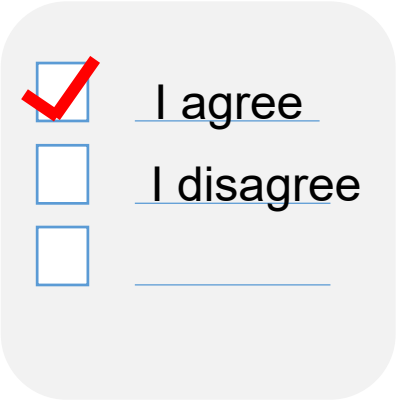
or processing is necessary:

- for the **performance of a contract** with the data subject
- for compliance with a **legal obligation**
- to protect the **vital interests of a data subject** or another person
- for the performance of a **task carried out in the public interest**
- for the purposes of **legitimate interests** pursued by the controller or a third party

Consent

(Art. 4 (11)): Consent has to be

- **Freely given**
  -> free choice, unbundled, no negative consequences if no consent is given
- **Specific**
  -> for a specific purpose, separate opt-in for each purpose
- **Informed** about:
  - controller's identity,
  - purposes,
  - type of data,
  - right to withdrraw consent,
  - any use for decisions based solely on auttomated processings,
  - risks of data transfers to third countries
- Unambigious indication of an agreement, by a statement or clear **affirmative action**
  - deliberate action, no pre-ticked opt-in boxes or opt-out constructions



Conditions for Consent (II)

(Art. 7):

- Controller needs to keep evidence that the data subject consented
- Data Subject has the right to withdraw consent at any time
- Withdrawal shall be as easy as to give consent

Overview to Data Subject Rights

Transparency Rights:

- Right to Information (ex ante)
- Right to Access (ex post)
- (Data Breach Notification)

• Intervenability Rights

- Right to rectification
- Right to erasure (”Right to be forgotten”)
- Right to restriction of processing
- Right to data portability
- Right to object to marketing & profiling
- (Right to withdraw consent)
- (Right to lodge complaint with supervisory authority)

Clear Rules for Business

- **One single set of rules** – which will make it simpler / cheaper for companies to do business in the EU.
- **One-stop-shop** – businesses will only have to deal with one single (lead) supervisory authority.
- **European rules on European soil** – companies based outside of Europe will have to apply the same rules when offering services in the EU.
- **Risk-based approach** – measures tailored to the respective risks.

Obligations - Controller

- Implement **appropriate technical & organisational data protection measures** (Art. 24, 25)

  - built into products and services from the earliest stage of development (**Data Protection by Design** – Art. 25 (1))
  - to ensure that only the data **necessary** should be processed, short storage period, limited accessibility (**Data Protection by Default** – Art. 25 (2))

Oligations – Controller (II)

- **Data breach notification** to
  - the supervisory authority (Art. 33) – without undue delay & within 72 hours if feasible (Art. 33)
  - the data subject – in case of high risk to their rights and freedom (Art. 34)

- **Data Protection Impact Assessement** (Art. 35) - for high risk data processing

Obligations – Processor & Controller

- Processing by processor governed by **contract** or **legal act** (Art. 28)

- **Security of Processing** (Art. 32)
  - Appropriate measures, such as pseudonymisation and/or encryption for protecting Confidentiality, Integrity and Availability

- Maintain **records of processing activities** (Art. 30)

- Designate a **data protection officer - DPO** (Art. 38)
  - Unless data processing is not their core business activity.

Data Transfers to Third Countries

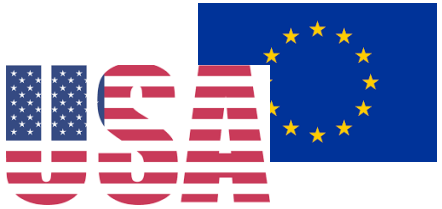
(Art. 45): Adequacy:

Personal data can only be transferred to third country, where the Commisson has decided an ”**adequate level of data protection**”.

- **Special adequacy decisions: Privacy Shield**
  - Privacy shield replaced Safe Harbor after CJEU 2014 Decision on Schrems vs. Facebook
  - However: Concerns by EDPS & Art. 29 Working Party

Examples of exceptions:

- **Standard contractual clauses** (Art. 46)
- **Binding corporate rules** (BCRs – Art. 47)
- **Explicit consent** (Art. 49)



10 Mistakes in System Design from a Privacy Perspective (Hansen 2012)

1. Storage as a Default
2. Linkability as a Default
3. Real Name as Default
4. Function Creep as a Feature
5. Fuzzy or Incomplete Policy Information as Default
6. ”Location does not Matter”
7. No Lifecycle Assessment
8. Changing Assumptions or Surplus Functionality
9. No Interveneability foreseen
10. Consent not providing a Valid Legal Ground

Top 10 Mistakes in System Design from a Privacy Perspective and Privacy Protection Goals

Marit Hansen,

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein,
Holstenstr. 98, 24103 Kiel, Germany
marit.hansen@datenschutzzentrum.de

Abstract. Privacy requirements are often not well considered in system design. The objective of this paper is to help interested system designers in three ways: First, it is discussed how “privacy” should be understood when designing systems that take into account the protection of individuals’ rights and their private spheres. Here specifically the concept of linkage control as an essence of privacy is introduced. Second, the paper presents a list of ten issues in system design collected during the daily work of a Data Protection Authority. Some of the mistakes are based on today’s design of data processing systems; some belong to typical attitudes or mindsets of various disciplines dealing with system design (technology, law, economics and others). Third, it is explained how working with protection goals can improve system design: In addition to the well-known information security protection goals, namely confidentiality, integrity and availability, three complementing privacy protection goals – unlinkability, transparency and intervenability – are proposed.

Keywords: Privacy, Privacy Mistakes, System Design, Privacy Protection Goal, Unlinkability, Transparency, Intervenability.

1 Introduction

IT security consultants have been publishing information on typical security mistakes for a long time. From these mistakes, organizations and individuals can learn, and thereby they may avoid repeating the same mistakes all over again. Several of the mistakes might reside in human nature or in the professional socialization, for some mistakes poor design of data processing systems may be accounted. The same is true for “privacy mistakes”, or to narrow it down: mistakes in system design from a privacy perspective.

The findings of this paper are derived from the experiences of the author after having worked for more than 15 years in a Data Protection Authority. Being a computer scientist herself, the author has collaborated with people from various disciplines and thereby identified some typical attitudes or mindsets of system designers that may explain the vulnerability for various mistakes and other wrong-doings, be it intentional or not. The collection of Top 10 mistakes have been presented first at the IFIP Summer School 2011 on privacy and identity management, thereafter the list has been

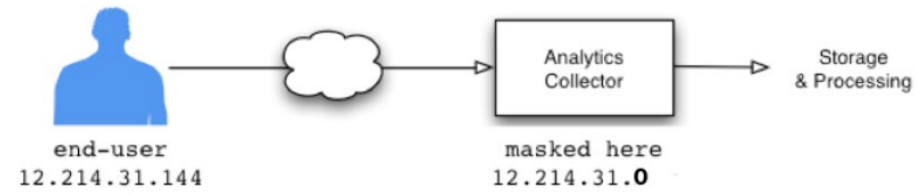
More typical mistakes….(I)

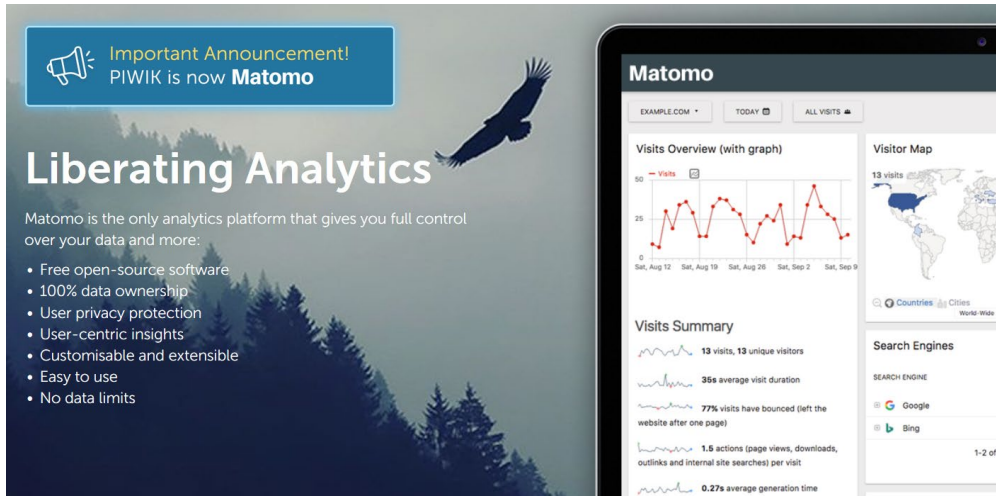
- Concept or personal data/special categories of data misunderstood
  - Deleting direct identifiers not enough
  - Encrypted personal data = personal data
  - Be aware of (sensitive) meta data / derived data
  - Avoid freetext fields

- GDPR-in-compliant use of services (Google Suite, Dropbox, Survey Monkey…)
  - Be aware of data transfer outside of EEA
  - Data processing agreement needed

More typical mistakes .... (II)

- Use of Google Analytics without AnonymizeIP
  - Use AnonymizeIP extension
  - Alternative tools running locally (e.g. Piwik/Matomo)





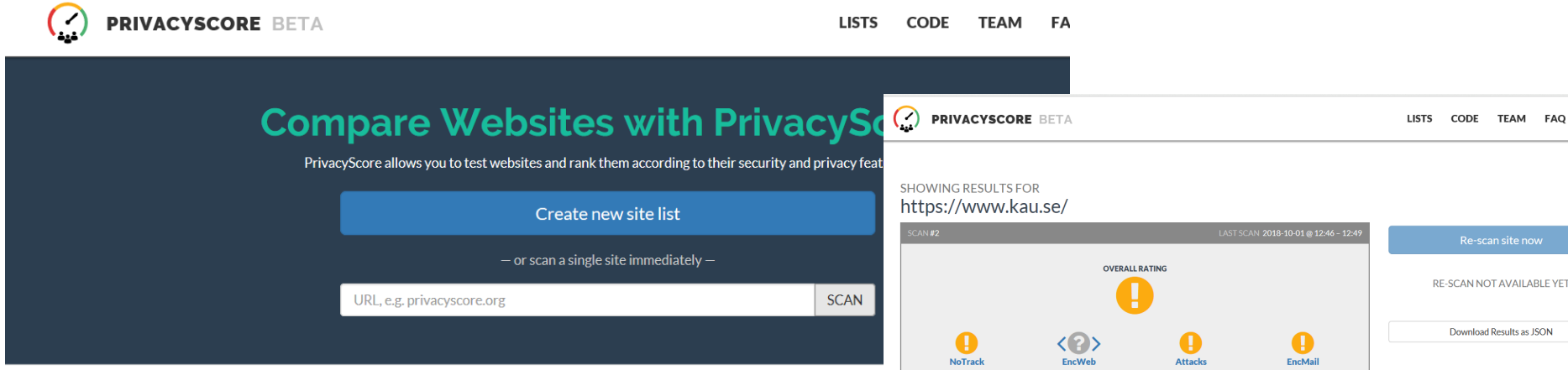
- Website privacy leaks
  - Set referrer-Policy to “no-referrer”
  - Minimise third party cookies/services/trackers
  - ....

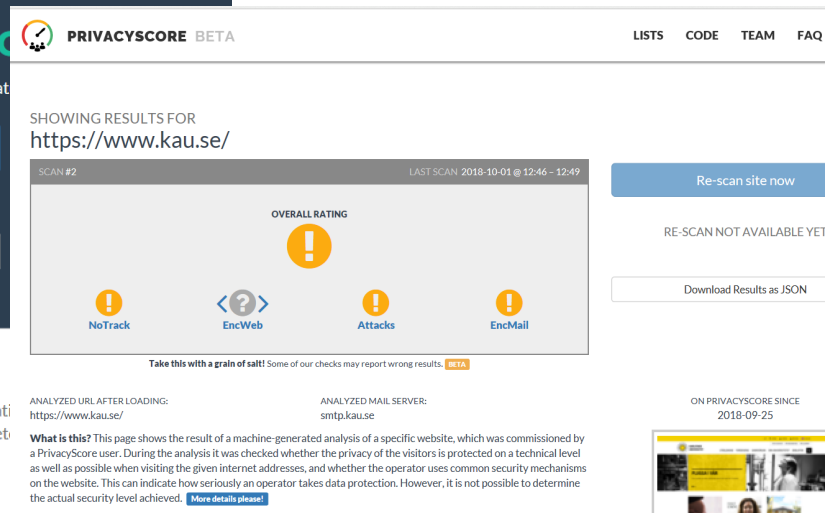
- Privacy of audience not considered
  - Alternative Channels for YouTube

Source: https://support.google.com/analytics/answer/2763052?hl=en, *https://matomo.org/*

Tools for checking Privacy Status of websites

- PrivacyScore



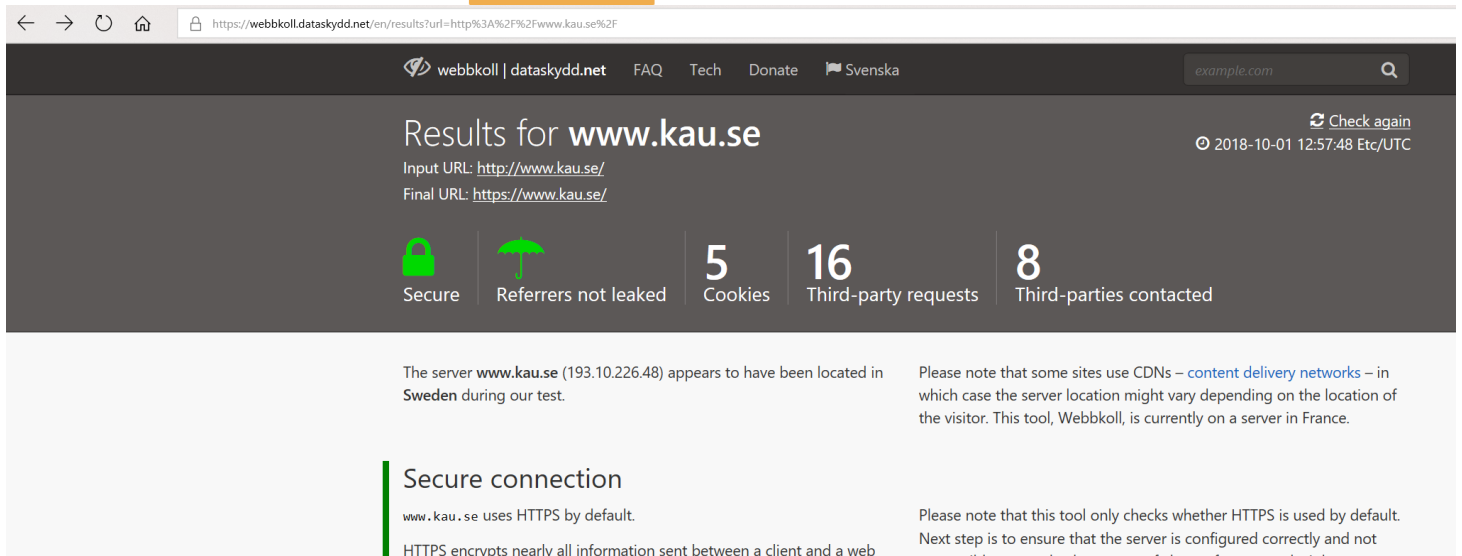


PrivacyScore is in public beta since 8 June 2017.
We post updates on Twitter.
Some parts of the site are also available in German. Please contact us if you want to contribute by translati
Note that it is not possible to edit lists at the moment. Feel free to create a new list and inform us so that we can delet

Lists in the Spotlight

We present selected lists of websites that have been added to PrivacyScore.
Long lists load quite slowly. Please be patient.
IMPROVEMENTS UNDERWAY

- Dataskydd.net



More typical mistakes .... (III)

- Sensitive data need special protection
  - Rules of thumb: 2 factor authentication, encryption (SSL/TLS), etc.

- Public data still require data protection!

Open Challenges

- Open data, data management plans
- Usable privacy notices
- Distinction: sensitive vs non-sensitive data
- Transparency & Fairness of AI Algorithms
- Right to Explanations
- Purpose binding for derived data & ”sticky policies”

- …

Questions?