Privacy Seals:
The European Privacy Seal EuroPriSe

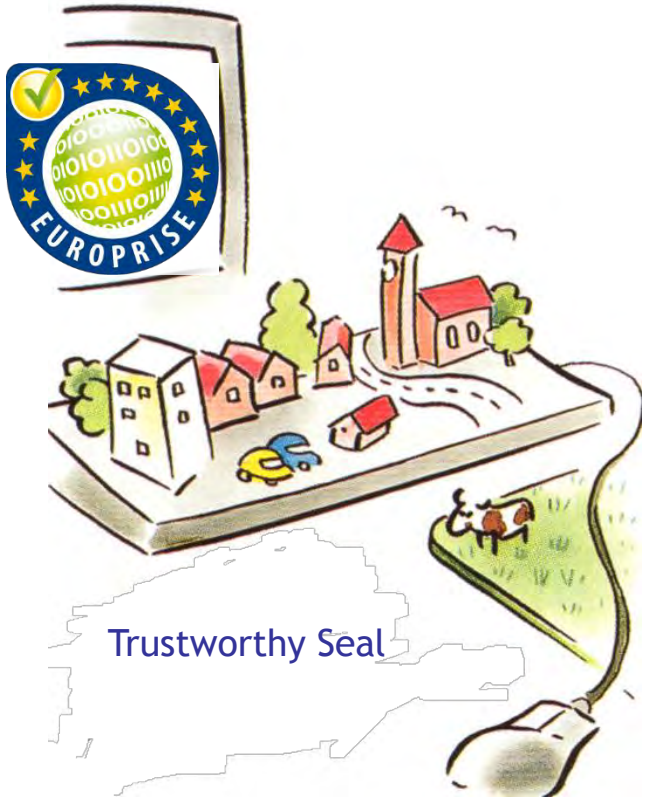
Sebastian Meissner, Head of EuroPriSe Certification Authority

DataEthics: Building Digital Trust – Hellerup, 19. May 2016

Why Privacy Seals?

- Lack of trust in today‘s information society (Cloud computing, IoT, Big Data, Profiling, Surveillance)
- Strong privacy seals as vital tools to rebuild consumer trust as well as to provide for trust in B2B relationships
- Advantage for data subjects: A seal enables consumers to easily identify privacy-friendly products and services
- Marketing advantage for certified companies: Seals are important tools to demonstrate compliance (and more)
- Advantage for business partners of certified companies: Assurance that data protection laws are complied with

Key Factors for Trust



Transparency

⇩

Verifiability

⇩

Credibility

=

Trust

EuroPriSe Project

- Project funding: 1,3 Mio by EU
- July 2007 – February 2009
- 18 pilot projects
- 6 certifications successfully completed
- Over 65 experts accredited
- Consortium: 9 partner from 8 EU countries

ULD

Agencia de Protección de Datos de la Comunidad de Madrid APDCM

CNIL

LONDON metropolitan university HRSJ Human Rights & Social Justice Research Institute

ITA INSTITUT FÜR TECHNIKFOLGEN-ABSCHÄTZUNG

TÜViT

ERNST & YOUNG

BORKING CONSULTANCY

VaF

EuroPriSe Deployment

- Deployment 1
  - Responsible entity: Office of Data Protection Commissioner of Schleswig-Holstein (ULD), DE
  - Location of Certification Authority (CA): Kiel, DE
  - Time frame: 03/2009 – 12/2013
- Deployment 2
  - Responsible entity: EuroPriSe GmbH
  - Location of Certification Authority: Bonn, DE
  - Time frame: since 01/2014
  - Approx. 100 admitted experts in 18 countries
  - Independent Advisory Board

EuroPriSe Certification Services

- IT products
  - Hardware (e.g., an external hard disc drive secured by strong encryption methods)
  - Software (e.g., a software module for obfuscation of video data or a fraud prevention software tool)
- IT-based services
  - Web-based services (e.g., a meta search engine or a service for collaboration of medical professionals)
  - Other services (e.g., a digitising service for photo negatives)
- Websites (since 2016)
  - Publicly accessible parts of a website (focus on interaction between website and website visitors)

Compliance +

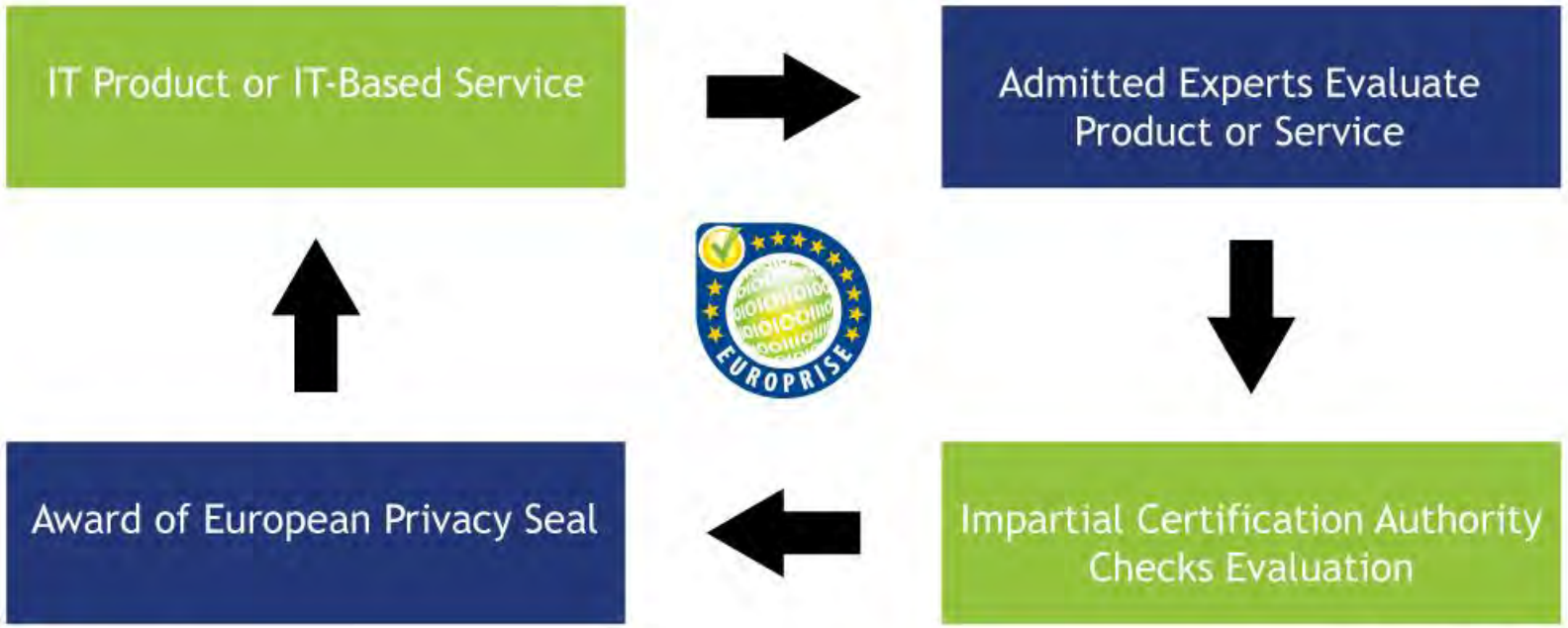
- EuroPriSe certifies compliance with EU data protection law (= globally highest standard in data protection)
- Reasoning based on Court of Justice of the European Union and Article 29 Working Party (particularly strict interpretation of the law)
- At least one requirement is rated „excellent“
- Recommendations by Certification Authority how to go beyond mere compliance with the law

Transparency: Public Criteria

EuroPriSe Criteria for IT products and IT-based services are publicly available at

www.european-privacy-seal.eu/EPS-en/Criteria

Transparency: Procedure



Validity: 2 years

Monitoring for IT-based services

Transparency → Verifiability: Publication of Results (I)

European Privacy Seal for Brainlab AG

Brainlab AG provides the cloud-based service Quentry, which facilitates the collaboration of medical professionals. Quentry enables medical professionals to share medical images, to display medical images in a web-based viewer and to add comments such as medical opinions. Customers of Brainlab are provided with meaninful information on how to make use of the service in compliance with EU data protection law. Particularly, they are advised that the legitimate use of the service requires the collection of patients' consent and release from medical confidentiality and that they must verify the identity of other customers prior to sharing medical information with them. Quentry comes with a functionality which allows the de-identification of meta data about patients prior to data being uploaded to the service. Customers who adhere to Brainlab's privacy advice can be sure that processing of sensitive health data by means of Quentry is in line with the high requirements of EU data protection law.

https://www.quentry.com

Press Release

Disclaimer:

This register is kept with the utmost care. However, EuroPriSe does NOT guarantee the accuracy of information found on the Site. Your reliance on information found on the Site is at your own risk.

Product/Version

quentry®

Quentry® service as provided to EU customers

Function as provided in March 2016

Qualification: IT-based service

View the Quentry Certificate

Transparency → Verifiability: Publication of Results (II)

In addition:
Short Public Report to be drafted by EuroPriSe Experts

BEST

Brainlab AG implemented a sophisticated multi-layered encryption solution which provides a high level of confidentiality regarding sensitive patient data that is processed within Quentry. Brainlab went to great lengths to implement a solution that approximates the level of a true end-to-end encryption to the greatest extent possible. Note: End-to-end encryption is impossible in the Quentry context since the service involves processing of patient data in the cloud.

In detail, confidentiality of personal data within Quentry is secured by means of an interplay of the following encryption methods:

- All communication between the user (client) and the Quentry-server is secured over TLS.
- User data and patient data are encrypted during transmission to the Quentry-server by TLS communication.
- User login process (External Authentication Service) is encrypted and secured by TLS-Webserver-Authentication and TLS-Web-Client-Authentication.
- During processing, patient data is encrypted in the CPU/RAM of the Quentry-server through a multi-layered encryption process.
- Only after the patient data is encrypted, the data is stored in a secured environment.

ATTENTION

Regarding the processing of patient data, it must be highlighted that users of Quentry qualify as controllers whereas Brainlab acts as processor on behalf of the customers. Brainlab provides customers with meaningful information on how to make use of the service in compliance with EU data protection law. Particularly, customers are advised that the legitimate use of the service requires the collection of patients' consent and release from medical confidentiality. The customer must verify the identity of other customers prior to sharing medical information with them. More detailed information on this topic is available under"Details" as well as in the **Short Public Report**.

Brainlab uses Salesforce as a cloud service provider for the authentication of users (customers). For the time being, Brainlab relies on standard contractual clauses (SCC) for the transfer of minimum authentication data to the U.S. In this context, it must be stressed that Brainlab will adhere to future guidance of the Article 29 Working Party regarding the impact of the so-called "Schrems judgment" of the European Court of Justice on the eligibility of SCC to legitimize international data transfers and make changes to the authentication solution (if necessary).

SUMMARY

Credibility: Auditors and CA

- EuroPriSe Legal and Technical Experts
  - Qualified Privacy Professionals
  - Proved capability of conducting an evaluation by means of a training evaluation
  - Independent from applicant
- EuroPriSe Certification Authority
  - High expertise in data protection
  - Independent from applicant
  - Impartial

Quality-assured procedure (“Four-Eye-Principle”)

Credibility: EuroPriSe Advisory Board

- Advisory Board Members
  - Experienced privacy professionals
  - Representatives and (former) heads of DPAs

Photograph taken during constituent meeting of AB

From left to right: Meissner (CA), Le Grand, Weichert, Borking, Kotschy, Farmer, Drost (CA), Schaar, Priebe

Credibility: Recognition by DPAs

- Mutual Recognition
  - EuroPriSe offers combined certification projects together with the German Data Protection Authority ULD

- Approval as Certification Authority
  - EuroPriSe acts as Certification Authority for the regional privacy seal of the German federal state of Mecklenburg-Vorpommern
  - This seal is based on the regional Data Protection Act and is granted in consultation with the Data Protection Commissioner

Privacy Mark Emblem

European Privacy Seal

EP-P-BS3XJV / Valid till 2016-04

Seal Validity Period

Unique Certification Number

P = Product
S = Service
W = Website

Success Stories

StartPage and Ixquick Once Again Earn Coveted EuroPriSe Certification

Privacy Seals and the General Data Protection Regulation

Encouragement to establish privacy seals

- GDPR introduces a legal framework for data protection certifications and seals on EU level for the very first time
- Core provisions: Art. 42 f.
- "The Member States, the supervisory authorities, the Board and the Commission shall encourage, **in particular at Union level**, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation" (Art. 42(1), sentence 1)
- The certification shall be **voluntary** (Art. 42(3))

Privacy Seals and the General Data Protection Regulation

Scope

- "for the purpose of demonstrating compliance with this Regulation of **processing operations by controllers and processors**" (Art. 42(1), sentence 1)

- Controllers and Processors
  - Controllers and processors that are subject to the Regulation
  - Controllers and processors that are not subject to the Regulation within the framework of personal data transfers to third countries or international organizations (Art. 42(2), Art. 46(2)(f))

    → Approved certification = appropriate safeguards for personal data transfers to third countries!

Privacy Seals and the General Data Protection Regulation

Criteria / Types of seal issuing bodies

- Certifications shall be issued "on the basis of criteria approved by the competent supervisory authority or by the European Data Protection Board" (Art. 42(5), sentence 1)
- "Where the criteria are approved by the Board, this may result in a common certification, **the European Data Protection Seal"** (Art. 42(5), sentence 2)
- "A certification shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority" (Art. 42(5), sentence 1)

Privacy Seals and the General Data Protection Regulation

Certification bodies

- Requirements for accreditation (Art. 43(2)):
  - Demonstration of **independence and expertise** in relation to the subject-matter of the certification;
  - Undertaking to **respect the criteria** (approved by the competent supervisory authority or the board)
  - Establishment of **procedures for the issuing, periodic review and withdrawal** of certifications, seals and marks;
  - Establishment of **procedures and structures to handle complaints** about certification related issues and disclosure of the procedures/structures to data subjects & the public;
  - Demonstration that their tasks and duties **do not result in a conflict of interests.**

Privacy Seals and the General Data Protection Regulation

Legal benefits

- "Certifications may be used as an element by which to **demonstrate compliance** with the obligations of the controller or processor" (Art. 24(3), 25(3), 28(5) + 32(3))
- appropriate safeguards for a **transfer of personal data to a 3rd country** outside the EU/EEA "may be provided for by approved certification mechanisms together with binding and enforceable commitments of the controller or processor in the third country" (Art. 46(2)(f))
- "When deciding whether to impose an **administrative fine** and deciding on the amount of the fine due regard shall be given to" approved certification mechanisms (Art. 83(2)(j))

Thank you very much for your interest in EuroPriSe!

Contact:

Sebastian Meissner

Head of Certification Authority

EuroPriSe GmbH

Joseph-Schumpeter-Allee 25

53227 Bonn / Germany

Email: ca@european-privacy-seal.eu

Website: https://www.european-privacy-seal.eu