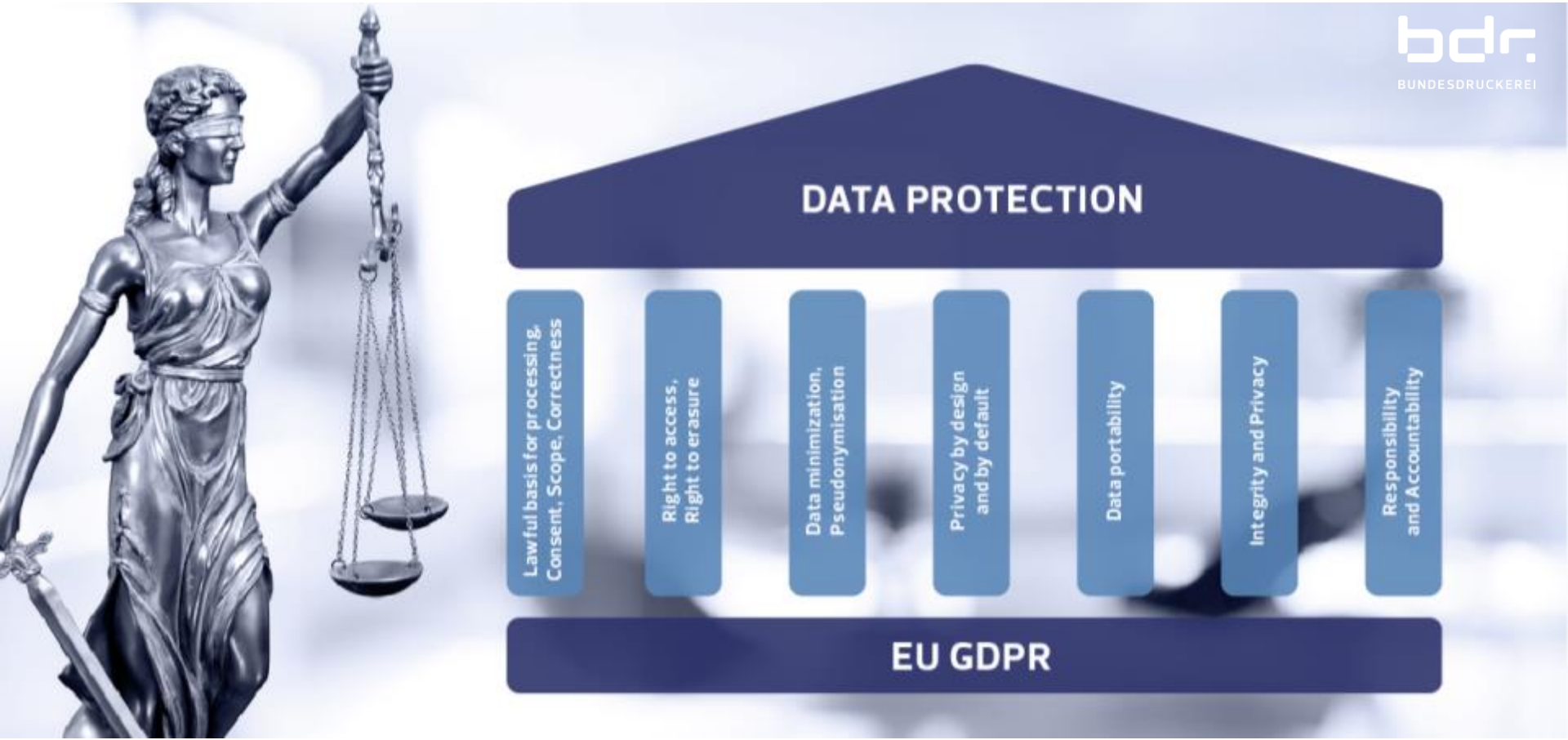
FIDO and GDPR

02.07.2018
Berlin, FIDO Seminar
Dr. Kim Nguyen, Bundesdruckerei GmbH & D-Trust GmbH

The protection of natural persons in relation to the processing of **personal data** is a **fundamental right**. Article 8 (1) of the Charter of Fundamental Rights of the EU and Article 16 (1) of the Treaty lay down that **everyone has the right to the protection of personal data** concerning him or her.

•The (…) principles and rules on the protection of individuals with regard to the processing of their personal data should, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably their right to the protection of personal data. It should **contribute to the accomplishment of an area of freedom, security and justice and of an economic union**, to economic and social progress, the strenghening and the convergence of the economies within the internal market, and the well-being of individuals.

GDPR


DATA PROTECTION
Lawful basis for processing, Consent, Scope, Correctness
Right to access, Right to erasure
Data minimization, Pseudonymisation
Privacy by design and by default
Data portability
Integrity and Privacy
Responsibility and Accountability
EU GDPR

The dark side of regulations

Notification

Immediately: typically within a couple of days (72h) to the supervisory board

Fines & Sanctions

GDPR: up to 4% of worldwide revenues

BUNDESDRUCKEREI

BUNDESDRUCKEREI

GDPR affects authentication in various aspects:

- **Data Security**
- **Consent and Individual Rights**
- **Biometrics**

BUNDESDRUCKEREI

Article 5: Processing of personal data

- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')

Article 25: Data protection by design and default

- Implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimization
- Implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed

BUNDESDRUCKEREI

Article 32: Requirements for data securiy

- Measures to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- Measures commensurate to the risk
- Measures to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

BUNDESDRUCKEREI

Article 7 requires that

- the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

Article 16-20 require that

- A right to rectification - allowing an individual to correct inaccurate personal data concerning him or her.
- A right to erasure – aka a "right to be forgotten" – allowing an individual to request that an entity delete all his or her personal data
- A right to data portability – allowing an individual to request a copy of his or her data, as well as transmitted to another entity

BUNDESDRUCKEREI

Article 4 defines Biometric Data as

"personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data."

Article 9 states that

- "*Processing of…biometric data…shall be prohibited.*" – but then lays out a number of conditions where this prohibition might be lifted.

BUNDESDRUCKEREI

Summarized:

1. Organizations need to **implement MFA** as part of their approach in order to be compliant with the requirements of data protection under GDPR

2. Organizations need to **authenticate individuals** who are providing consent to their sensitive data being captured or are asking for their data to be erased, corrected, or transmitted to another party.

3. For organizations using **biometrics** as part of their authentication solution, they must ensure that the biometrics application does not run afoul of GDPR.

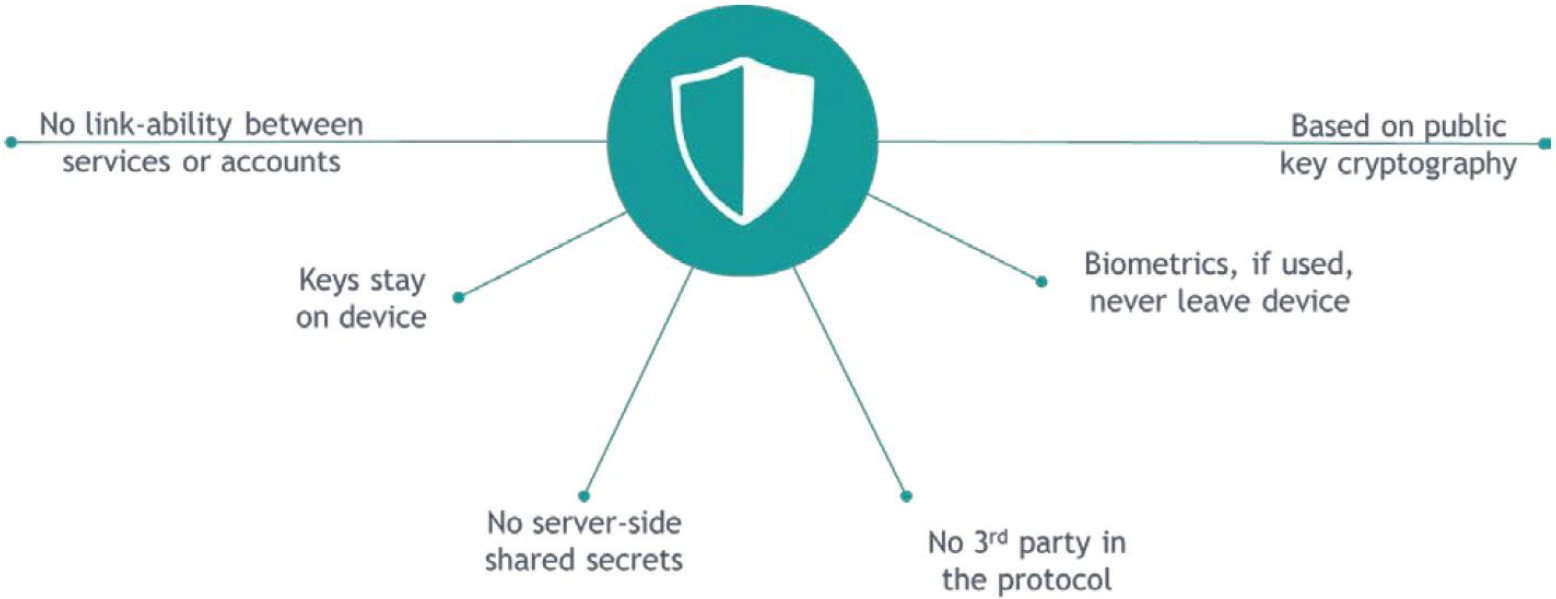

Privacy by Design
GDPR

1. In a typical smartphone FIDO solution, the **biometric (the first factor) is on the user** and the **private cryptographic key (the second factor) is stored on the device**. The biometric is presented to the device and **matched locally**.

2. The independence of these FIDO authentication factors can be enhanced by the use of **modern hardware-backed technologies** present on an ever increasing percentage of consumer devices (mobile and desktop) such as **Secure Elements**, Trusted Execution Environments (**TEE**) or Trusted Platform Modules (**TPM**).

3. This model is further enhanced by the **Attestation Key** that allows the characteristics of a FIDO Authenticator to be bound to a particular device. The attestation key allows any online service provider to **know what specific security elements are on the device and make a judgement as to whether to trust it**;

FIDO & Privacy by design



THE DIFFERENT DIMENSIONS OF FIDO

Security

Usability

Privacy

Interoperability

Summary

- There is no „silver bullet“ which solves all GDPR topics.
- MFA is a vital component in a GDPR compliant solution.

- The design of FIDO is built on „Privacy by design“
- FIDO supports independence of authentication factors

- FIDO is adopted globally
- FIDO offers unique cross-platform support

Thank you!

Questions?