CISPA
Center for IT-Security, Privacy and Accountability

Datenschutz „by Default“

Zwischen Paternalismus und Pragmatismus

Art.25 DSGVO – Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

CISPA Center for IT-Security, Privacy and Accountability

2. Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

marnau@cispa.saarland

Art.25 DSGVO – Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

CISPA Center for IT-Security, Privacy and Accountability

2. Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch **Voreinstellung** ~~grundsätzlich~~ nur personenbezogene Daten, deren Verarbeitung **für den jeweiligen bestimmten Verarbeitungszweck erforderlich** ist, verarbeitet werden. Diese Verpflichtung gilt für die **Menge** der erhobenen personenbezogenen Daten, den **Umfang** ihrer Verarbeitung, ihre **Speicherfrist** und ihre **Zugänglichkeit**. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

marnau@cispa.saarland

Art.25 GDPR – Data protection by design and by default

2. The controller shall 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. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

CISPA
Center for IT-Security, Privacy and Accountability

Erwägungsgrund 78 DSGVO

(…) Um die Einhaltung dieser Verordnung nachweisen zu können, sollte der Verantwortliche interne Strategien festlegen und Maßnahmen ergreifen, die insbesondere den Grundsätzen des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) Genüge tun. Solche Maßnahmen könnten unter anderem darin bestehen, dass **die Verarbeitung personenbezogener Daten minimiert** wird, personenbezogene Daten **so schnell wie möglich pseudonymisiert** werden, Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten hergestellt wird, der betroffenen Person ermöglicht wird, die Verarbeitung personenbezogener Daten zu überwachen, und der Verantwortliche in die Lage versetzt wird, Sicherheitsfunktionen zu schaffen und zu verbessern. (...)

Aufgeschlüsselt

- Technisch-organisatorische Maßnahmen,
  - die sicherstellen,
    - dass Voreinstellungen sicherstellen,
      - dass Datenminimierung,
        - in Form von Limitierung nach Erforderlichkeit, von Menge, Umfang, Speicherfrist und Zugänglichkeit,
- ohne Eingreifen der Person umgesetzt wird.

marnau@cispa.saarland

CISPA
Center for IT-Security, Privacy and Accountability

Fragen

- Warum sind Voreinstellungen relevant?
- Wen verpflichtet Art. 25 Abs. 2?
- Geht Art 25 Abs 2 über die bloße Verpflichtung auf Datenminimierung und Zweckbindung hinaus?
- Beschränkt Art. 25 Abs. 2 den Funktionsumfang von Produkten?
- Verpflichtet Art. 25 Abs. 2 zur Implementierung von Defaults?
- Wie muss Art. 25 Abs. 2 umgesetzt werden?

marnau@cispa.saarland

CISPA
Center for IT-Security, Privacy and Accountability

Fragen

- **Warum sind Voreinstellungen relevant?**
- Wen verpflichtet Art. 25 Abs. 2?
- Geht Art 25 Abs 2 über die bloße Verpflichtung auf Datenminimierung und Zweckbindung hinaus?
- Beschränkt Art. 25 Abs. 2 den Funktionsumfang von Produkten?
- Verpflichtet Art. 25 Abs. 2 zur Implementierung von Defaults?
- Wie muss Art. 25 Abs. 2 umgesetzt werden?

marnau@cispa.saarland

Warum sind Voreinstellungen relevant?

CISPA Center for IT-Security, Privacy and Accountability

Defaults/Voreinstellungen bedeuten:

- Prekonfigurationen; Einstellungen, die zum Beginn der Nutzung greifen
- Spätere Veränderungen sind ggf. möglich
- Sollten nicht überraschend oder übervorteilend sein

Relevanz

- Großteil der Nutzer ändert Voreinstellungen nicht oder nur partiell

Decision Fatigue

CISPA
Center for IT-Security, Privacy and Accountability

Fragen

- Warum sind Voreinstellungen relevant?
- **Wen verpflichtet Art. 25 Abs. 2?**
- Geht Art 25 Abs 2 über die bloße Verpflichtung auf Datenminimierung und Zweckbindung hinaus?
- Beschränkt Art. 25 Abs. 2 den Funktionsumfang von Produkten?
- Verpflichtet Art. 25 Abs. 2 zur Implementierung von Defaults?
- Wie muss Art. 25 Abs. 2 umgesetzt werden?

marnau@cispa.saarland

Wer ist verpflichtet?

- Art. 25 Abs. 2:
  “Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen …“
- Verpflichtung trifft nur den Verantwortlichen
- Problem: Hersteller und Entwickler können nur mittelbar in die Pflicht genommen werden. Verantworliche müssen hier die Anforderungen weitergeben, z.B. in Form von Kriterien in Ausschreibungen

CISPA
Center for IT-Security, Privacy and Accountability

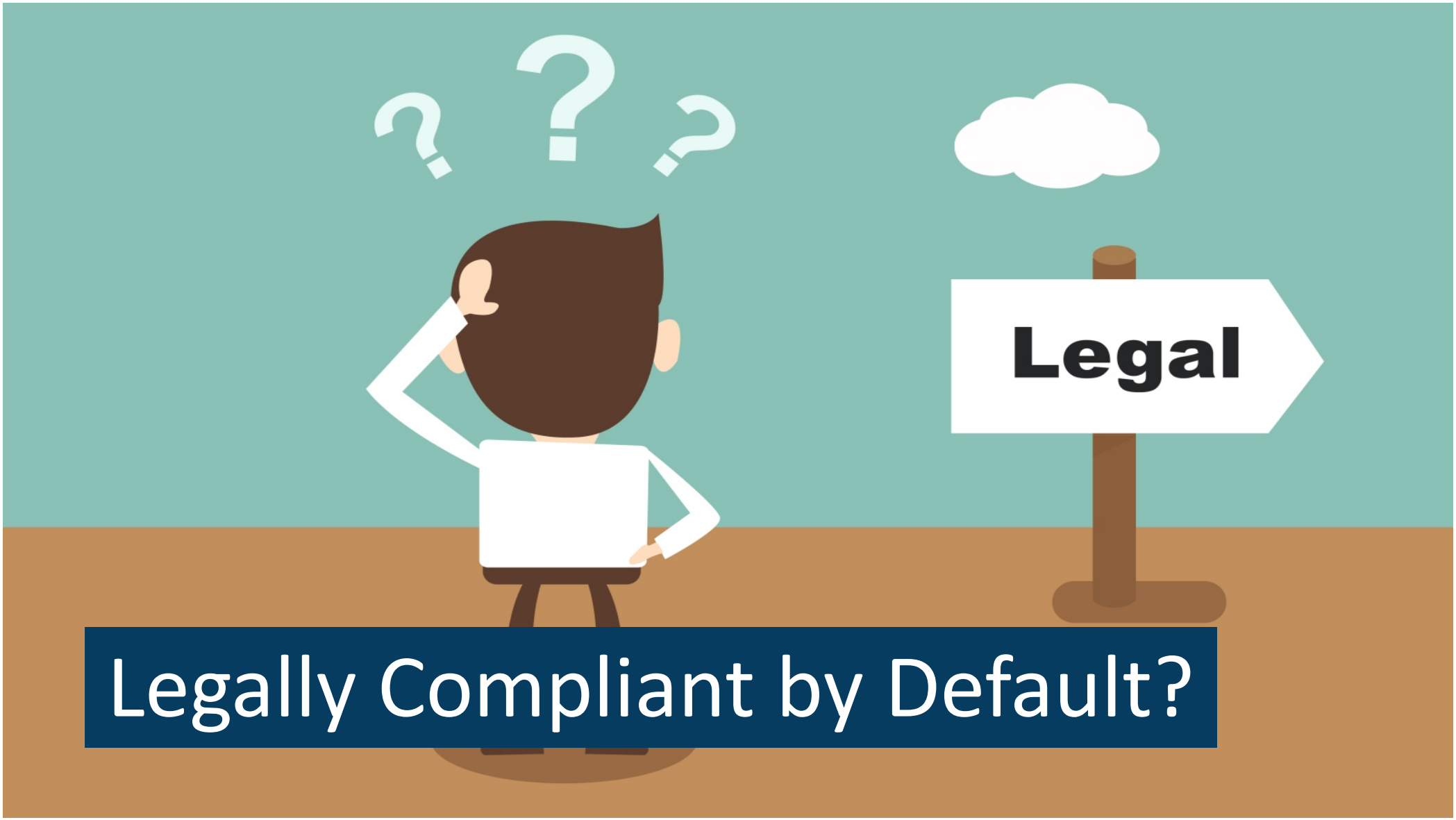
Fragen

- Warum sind Voreinstellungen relevant?
- Wen verpflichtet Art. 25 Abs. 2?
- **Geht Art 25 Abs 2 über die bloße Verpflichtung auf Datenminimierung und Zweckbindung hinaus?**
- Beschränkt Art. 25 Abs. 2 den Funktionsumfang von Produkten?
- Verpflichtet Art. 25 Abs. 2 zur Implementierung von Defaults?
- Wie muss Art. 25 Abs. 2 umgesetzt werden?

marnau@cispa.saarland

Kriterien

- für den jeweiligen bestimmten Verarbeitungszweck erforderlich
- Minimierung von
  - Menge
  - Umfang
  - Speicherfrist
  - Zugänglichkeit
- Social Media Clause: Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.


Legal
Legally Compliant by Default?

Kritik des EDPS (2012)*

CISPA Center for IT-Security, Privacy and Accountability

"Article 23(2) contains the principle of data protection by default, but it is **not given a clear substance**. The first sentence **does not add much to** the general principles of data processing in Article 5, and **the data minimisation principle** in Article 5(c) in particular, except from the confirmation that such principles should also be embedded in the design of relevant systems."

*https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf

Unterschied zu “legally compliant”

CISPA Center for IT-Security, Privacy and Accountability

- Anwendungen müssen ohnehin Datenminimierung, Zweckbindung und Data Protection by Design berücksichtigen
- Voreinstellungen werden dann relevant, wenn abgestufte Invasivität und Funktionalität möglich sind

CISPA
Center for IT-Security, Privacy and Accountability

Fragen

- Warum sind Voreinstellungen relevant?
- Wen verpflichtet Art. 25 Abs. 2?
- Geht Art 25 Abs 2 über die bloße Verpflichtung auf Datenminimierung und Zweckbindung hinaus?
- **Beschränkt Art. 25 Abs. 2 den Funktionsumfang von Produkten?**
- Verpflichtet Art. 25 Abs. 2 zur Implementierung von Defaults?
- Wie muss Art. 25 Abs. 2 umgesetzt werden?

marnau@cispa.saarland

Kritik des EDPS (2012)*

CISPA Center for IT-Security, Privacy and Accountability

"The principle of data protection by default aims at protecting the data subject in situations in which there might be a lack of understanding or control on the processing of their data, especially in a technological context. **The idea behind the principle is that privacy intrusive features of a certain product or service are initially limited to what is necessary for the simple use of it.** The data subject should in principle be left the choice to allow use of his or her personal data in a broader way. The EDPS recommends including in Article 23(2) a reference to this position of the data subject and providing the necessary clarification in recital 61."

*https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf

Funktionsumfang

CISPA
Center for IT-Security, Privacy and Accountability

marnau@cispa.saarland

Funktionsumfang

Was qualifiziert Kernfunktion (“simple use”) eines Produkts?

“ ’data protection by default’ should encompass not only privacy by design as a default, but also least privacy-infringing (or maximally privacy-enhancing) default settings where this is reasonable.”

M. Hansen, IFIP 2013 https://link.springer.com/content/pdf/10.1007/978-3-642-37282-7_2.pdf

CISPA
Center for IT-Security, Privacy and Accountability

Fragen

- Warum sind Voreinstellungen relevant?
- Wen verpflichtet Art. 25 Abs. 2?
- Geht Art 25 Abs 2 über die bloße Verpflichtung auf Datenminimierung und Zweckbindung hinaus?
- Beschränkt Art. 25 Abs. 2 den Funktionsumfang von Produkten?
- **Verpflichtet Art. 25 Abs. 2 zur Implementierung von Defaults?**
- Wie muss Art. 25 Abs. 2 umgesetzt werden?

marnau@cispa.saarland

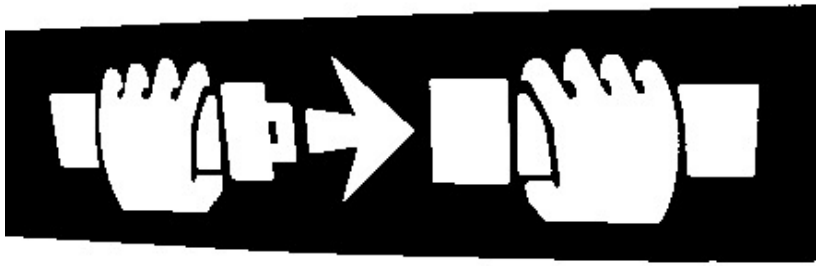
CISPA
Center for IT-Security, Privacy and Accountability

Fragen

- Warum sind Voreinstellungen relevant?
- Wen verpflichtet Art. 25 Abs. 2?
- Geht Art 25 Abs 2 über die bloße Verpflichtung auf Datenminimierung und Zweckbindung hinaus?
- Beschränkt Art. 25 Abs. 2 den Funktionsumfang von Produkten?
- Verpflichtet Art. 25 Abs. 2 zur Implementierung von Defaults?
- **Wie muss Art. 25 Abs. 2 umgesetzt werden?**

marnau@cispa.saarland

Paternalismus



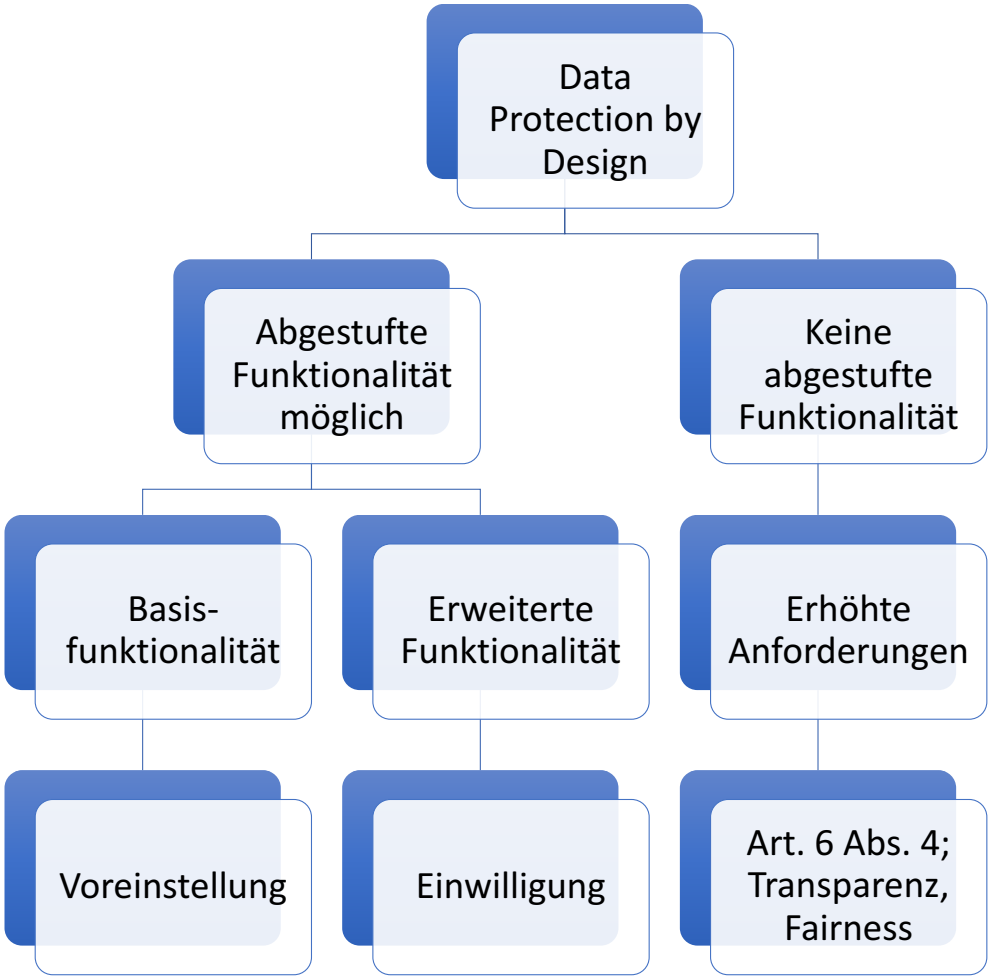
- Voreinstellungen können erwartete Funktionalität behindern
- Betroffene können sich bevormundet fühlen
- Informationelle Selbstbestimmung kann auch durch zuviel Schutz beschränkt werden
- Usability beim Freischalten von Zusatzfunktionen ist nicht einfach und bedarf der Aktion des Betroffenen

CISPA
Center for IT-Security, Privacy and Accountability

Pragmatismus

- Basisfunktionen identifizieren
- Nutzererwartungen an das Produkt berücksichtigen; Produkt muss benutzbar bleiben
- Offline-Funktionalität höher gewichten
- In Usability investieren
- Unterschiedliche Vorkonfigurationen/Profile beim Start zur Auswahl anbieten
- Bundle-Konfigurationen erlauben (mehrere Zusatzservices gemeinsam freischaltbar)

marnau@cispa.saarland



marnau@cispa.saarland

Verhältnis zu Rechtsgrundlagen der Verarbeitung

Gilt die Pflicht zu datenschutzfreundlichen Voreinstellungen auch für alle Rechtsgrundlagen gleichermaßen?

- Legitimes Interesse
- Erlaubnis oder Pflicht zur Verarbeitung aus anderen Gesetzen
- Zweckändernde Weiterverarbeitung

Verhältnis zu Rechtsgrundlagen der Verarbeitung

CISPA Center for IT-Security, Privacy and Accountability

These:

- Data Protection by Default schränkt die Rechtsgrundlagen der Verarbeitung aus Art. 6 auf die Basisfunktionalität eines Produkts ein (z.B. bei legitimen Interesse)
- Funktionen über die Basisfunktion hinaus können nur mit Einwilligung aktiviert werden
- Unklar: Zweckändernde Weiterverarbeitung. Widersinnig hier gestufte Funktionalität zu Verlangen. Data Protection by Design + Interessenabwägung wohl ausreichend

Fazit

- Mächtiges Werkzeug
- Potentiell leichtere Kontrolle als Data Protection by Design
- Kernherausforderung: Identifikation von Basisfunktionalität
- Leitlinien und Modellprojekte der Aufsichtbehörden zu Fallgruppen für Funktionalitätsabstufung wünschenswert
- Verhältnis zu Rechtsgrundlagen der Verarbeitung noch nicht vollständig geklärt

marnau@cispa.saarland


CISPA
Center for IT-Security, Privacy
and Accountability
GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung
UNIVERSITÄT
DES
SAARLANDES
SAARLAND