Security by Design and the GDPR – Pretty Much Best Friends?

Dr. h.c. Marit Hansen

State Data Protection Commissioner
of Schleswig-Holstein, Germany

Annual Privacy Forum 2026 – Salzburg, Austria – 9 September 2026

Plattform Privatheit

ULD

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Overview

1. Flying blind …
2. Upcoming: security by design
3. Relief for DPOs?
4. CRA: What do we get?
5. Disease ⇆ Cure
6. Conclusion & Outlook

Schleswig-Holstein

State of Germany

Flag

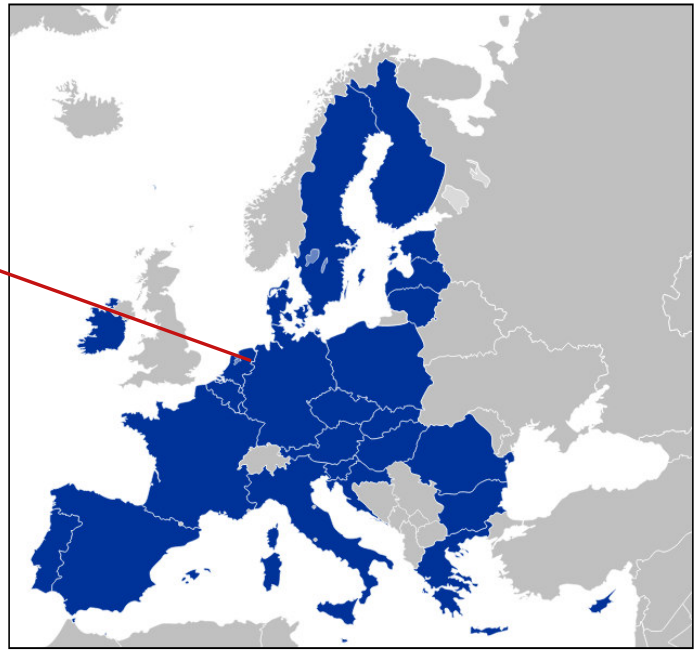
Coat of arms

Coordinates: 54°28′12″N 9°30′50″E

Country	Germany
Capital	Kiel
Government	
• Body	Landtag of Schleswig-Holstein
• Minister-President	Daniel Günther (CDU)
• Governing parties	CDU / Greens
• Bundesrat votes	4 (of 69)
Area	
• Total	15,763.18 km² (6,086.20 sq mi)

Setting of ULD

- State Data Protection Authority (DPA)
- Located in Kiel, Germany



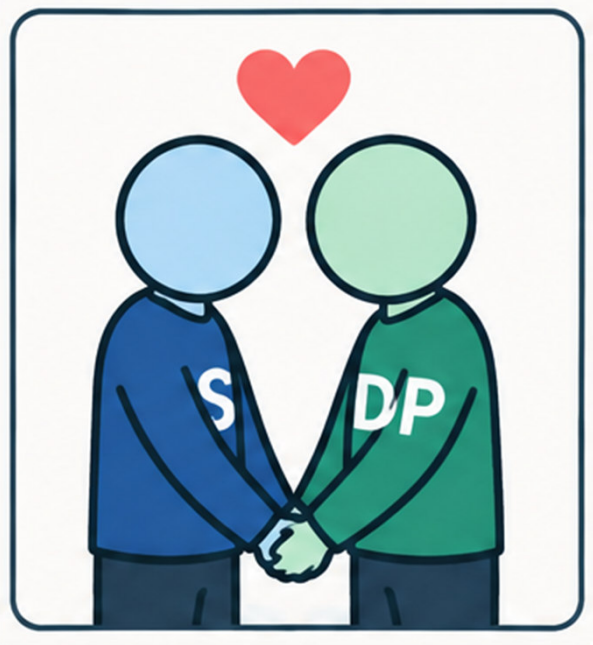
Source: Kolja21 via Wikimedia

Source: en.wikipedia.org/wiki/Schleswig-Holstein

My talk

Once upon a time, there were two lovers …

Security



Data Protection (GDPR)

Nah, let's stay professional

Overview

1. Flying blind …
2. Upcoming: security by design
3. Relief for DPOs?
4. CRA: What do we get?
5. Disease ⇆ Cure
6. Conclusion & Outlook

Data controllers …

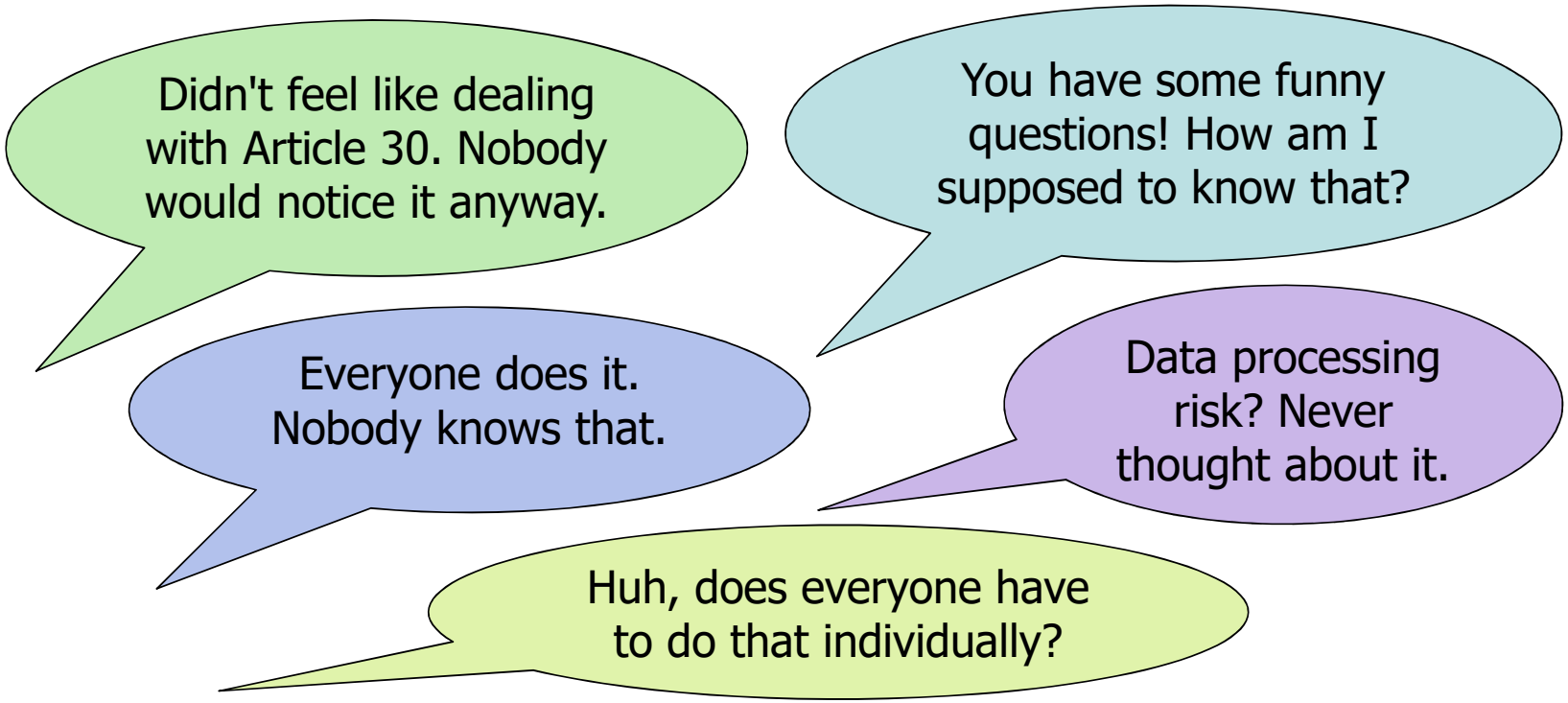
have no idea!

(more often than not)

Overview

1. Flying blind …

Sounds like the beginning of a joke: "A supervisory authority asks the data controller about the data processing …"



Overview

1. Flying blind …

Accountability

Article 5 (2) GDPR

(1) […Data protection principles …]

(2) The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Article 24 (1) GDPR

(1) Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

Overview

1. Flying blind …
2. Upcoming: security by design
3. Relief for DPOs?
4. CRA: What do we get?
5. Disease ⇆ Cure
6. Conclusion & Outlook

Let’s simplify things for this presentation:

We’ll focus on security

Overview

2. Upcoming: security by design

- Cyber Resilience Act (EU) 2024/2847 as product safety legislation
- Improvement of cybersecurity for "products with digital elements" (i.e., connectable to the Internet)
- Manufacturer obligations
  1. regarding cybersecurity by design
  2. regarding sustainable vulnerability management, including updates
- For the EU market: CRA compliance required, indicated by the CE marking

Icon: Ce Seal Icons by Freepik - Flaticon

Overview

2. Upcoming: security by design

Four categories: rising risk, increasing obligations

Standard

- Products with digital elements that are not important and not critical

Important (Class I)

- Operating systems
- Browsers, routers
- Identity and password managers
- Smart home products
- Wearables
- …

Important (Class II)

- Hypervisors
- Firewalls, intrusion detection systems
- Tamper-resistant microprocessors and microcontrollers

Critical

- Hardware devices with security boxes
- Smart meter gateways
- Devices for advanced security purposes
- Smartcards or similar devices, including secure elements

Icons: Document Icons by Awicon – Flaticon

Overview

2. Upcoming: security by design

Four categories: rising risk, increasing obligations

Standard
- Products with digital elements that are not important and not critical

Important (Class I)
- Operating systems
- Browsers, routers
- Identity and password managers
- Smart home products
- Wearables
- …

(Class II)
- … detection
- …microprocessors
- …ers

Critical
- Hardware devices with security boxes
- Smart meter gateways
- Devices for advanced security purposes
- Smartcards or similar devices, including secure elements

The greater the importance and criticality of products with digital elements, the more demanding the conformity assessment procedure that must be undergone before the product can be CE marked and placed on the market.

Icons: Document Icons by Awicon - Flaticon

Overview

2. Upcoming: security by design

Annex I of the CRA (Essential Cybersecurity Requirements), Part 1

(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.

Overview

Should Data Protection Officers applaud enthusiastically?

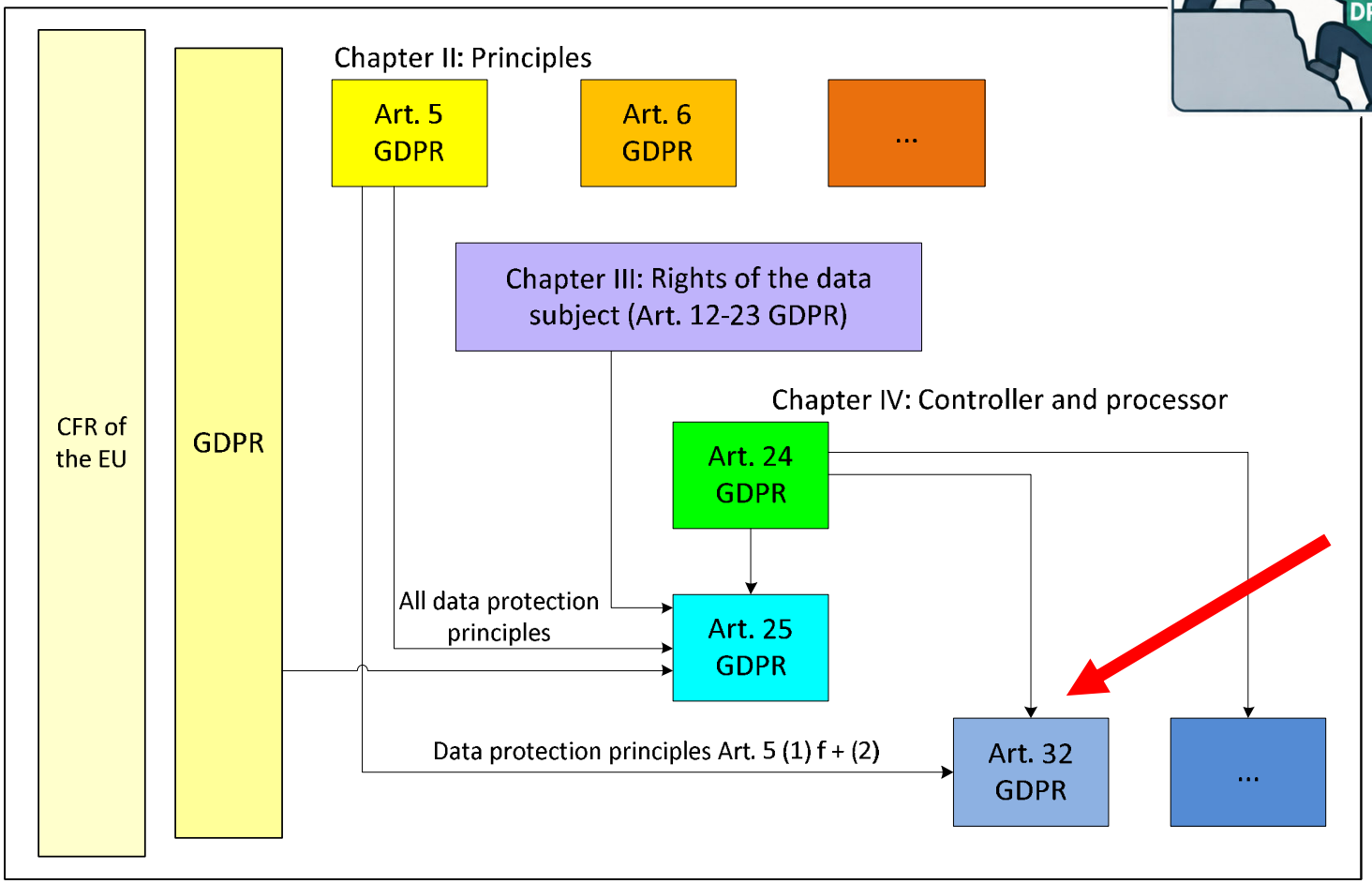
Overview

1. Flying blind …
2. Upcoming: security by design
3. Relief for DPOs?
4. CRA: What do we get?
5. Disease ⇆ Cure
6. Conclusion & Outlook

"Yay, together we'll manage the risk"

Overview

3. Relief for DPOs?



3. Relief for DPOs?

Overview

1. Flying blind …
2. Upcoming: security by design
3. Relief for DPOs?
4. CRA: What do we
5. Disease ⇆ Cure
6. Conclusion & Outlook

Article 5 GDPR

(2) The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Article 24 GDPR

(1) Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

Article 25 GDPR

(1) […] 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.

Article 28 GDPR

(3) […] That contract or other legal act shall stipulate, in particular, that the processor:
[…]
h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

Article 32 GDPR

(1) […] 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:
[…]
b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
[…]
d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Article 35 GDPR

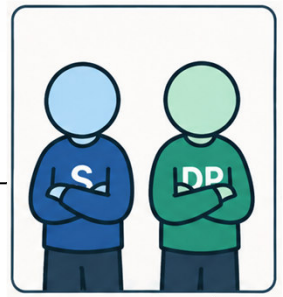
(7) The assessment shall contain at least:
[…]
d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

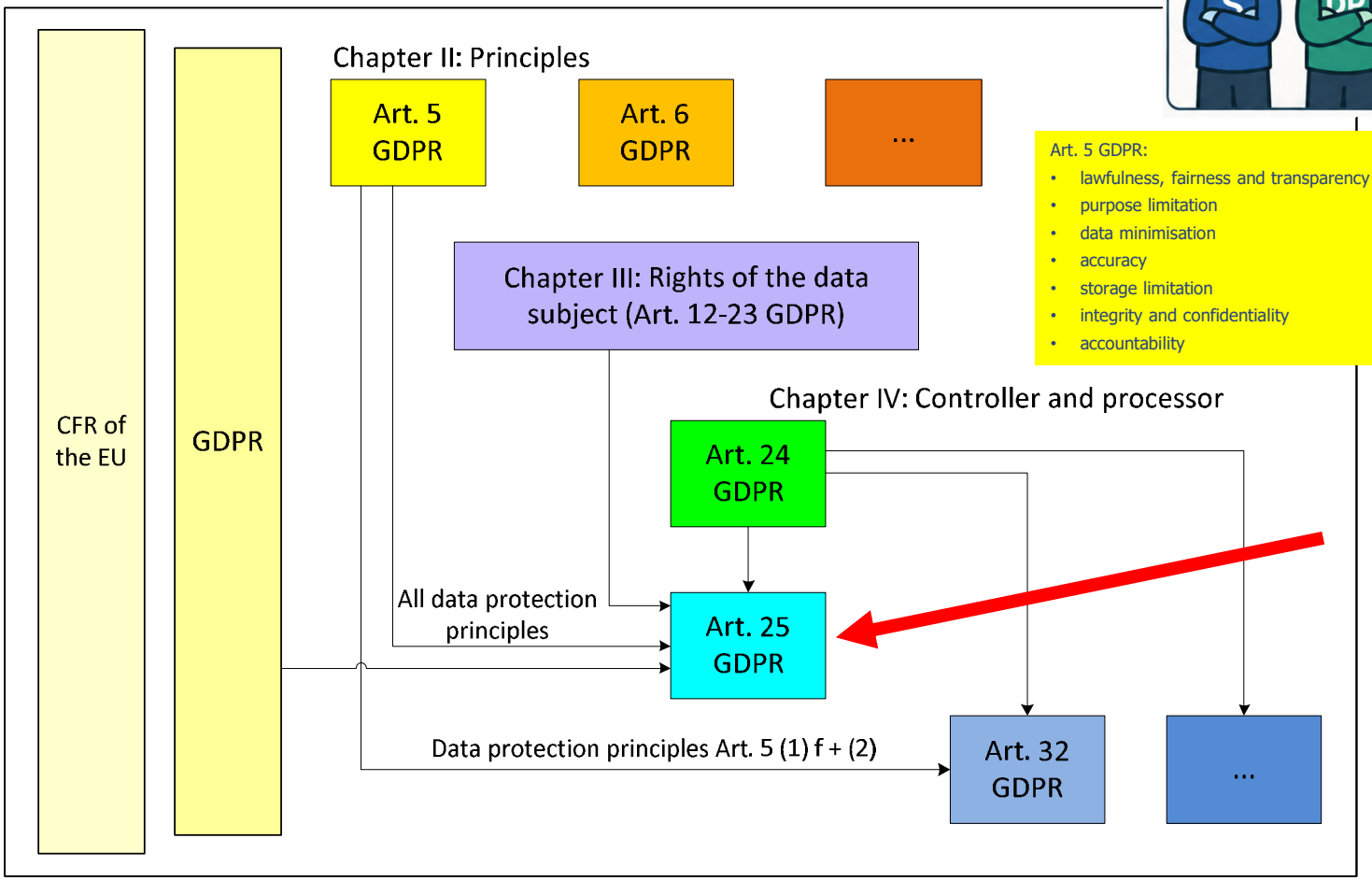
Effective: effective regarding the intended effect; taking potential side effects into account
Examinable: possibility of meaningful examination of the guaranteed properties and effects
Lasting: at any time; also in the future; resilient

Hansen/Probst: Souveräne Sicherheit, Zero Trust und das Datenschutzrecht, DuD 10/2023, 623-628

Overview

3. Relief for DPOs?





Overview

3. Relief for DPOs?

Images: ChatGPT

Overview

1. Flying blind …
2. Upcoming: security by design
3. Relief for DPOs?
4. CRA: What do we get?
5. Disease ⇆ Cure
6. Conclusion & Outlook

Okay, but security is no longer an empty promise?

Great!

Let's take a look at the fine print (the annexes of the CRA).

Overview

4. CRA: What do we get?

CE marking

Annex I, Part I para. 2 letters e-h CRA

(2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:
[…]
e) … confidentiality …
f) … integrity …
g) …
h) … availability …
[…]

Icon: Ce Seal Icons by Freepik - Flaticon

Overview

1. Flying blind …
2. Upcoming: security by design
3. Relief for DPOs?

4. CRA: What do we get?

CE marking

Art. 5(1)(c) GDPR

(1) Personal data shall be:
[…]
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

Annex I, Part I para. 2 letter g CRA

(2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:
[…]
g) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimisation);

Icon: Ce Seal Icons by Freepik - Flaticon

Overview

4. CRA: What do we get?

CE marking

Info to the user

Technical documentation

SBOM (Software Bill of Materials)

- Basis: manufacturer's technical documentation
- … across the entire supply chain
- Valuable for security
- Valuable for the accountability of the controller

Icons: Manual Icons by srip sowie Ce Seal Icons, Document Icons, Product Icons und Source Code Icons by Freepik - Flaticon

Overview

4. CRA: What do we get?

CE marking

Info to the user

Technical documentation

SBOM (Software Bill of Materials)

Article 31 CRA
Technical Documentation

Annex VII
Content of the Technical Documentation incl. SBOM (where applicable)

Annex II
Information and Instructions to the User

Icons: Manual Icons by srip sowie Ce Seal Icons, Document Icons, Product Icons und Source Code Icons by Freepik - Flaticon

4. CRA: What do we get? Technical documentation (valuable or boring?)

Cyber Resilience Act – consolidated version:
https://eur-lex.europa.eu/eli/reg/2024/2847/2024-11-20

Annex II: Information and Instructions to the User

At minimum, the product with digital elements shall be accompanied by:

1. the name, registered trade name or registered trademark of the manufacturer, and the postal address, the email address or other digital contact as well as, where available, the website at which the manufacturer can be contacted;

2. the single point of contact where information about vulnerabilities of the product with digital elements can be reported and received, and where the manufacturer's policy on coordinated vulnerability disclosure can be found;

3. name and type and any additional information enabling the unique identification of the product with digital elements;

4. […]

Overview

4. CRA: What do we get? Technical documentation (valuable or boring?)

Annex II: Information and Instructions to the User

At minimum, the product with digital elements shall be accompanied by:
[…]

4. the intended purpose of the product with digital elements, including the security environment provided by the manufacturer, as well as the product's essential functionalities and information about the security properties;

5. any known or foreseeable circumstance, related to the use of the product with digital elements in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to significant cybersecurity risks;

6. where applicable, the internet address at which the EU declaration of conformity can be accessed;

7. the type of technical security support offered by the manufacturer and the end-date of the support period during which users can expect vulnerabilities to be handled and to receive security updates;

Overview

4. CRA: What do we get? Technical documentation (valuable or boring?)

Annex II: Information and Instructions to the User

At minimum, the product with digital elements shall be accompanied by:

[…]

8. detailed instructions or an internet address referring to such detailed instructions and information on:

(a) the necessary measures during initial commissioning and throughout the lifetime of the product with digital elements to ensure its secure use;

(b) how changes to the product with digital elements can affect the security of data;

(c) how security-relevant updates can be installed;

(d) the secure decommissioning of the product with digital elements, including information on how user data can be securely removed;

(e) how the default setting enabling the automatic installation of security updates, as required by Part I, point (2)(c), of Annex I, can be turned off;

(f) where the product with digital elements is intended for integration into other products with digital elements, the information necessary for the integrator to comply with the essential cybersecurity requirements set out in Annex I and the documentation requirements set out in Annex VII.

9. If the manufacturer decides to make available the software bill of materials to the user, information on where the software bill of materials can be accessed.

Overview

4. CRA: What do we get? Technical documentation (valuable or boring?)

Annex VII: Content of the Technical Documentation

2. a description of the design, development and production of the product with digital elements and vulnerability handling processes, including:

(a) necessary information on the design and development of the product with digital elements, including, where applicable, drawings and schemes and a description of the system architecture explaining how software components build on or feed into each other and integrate into the overall processing;

(b) necessary information and specifications of the vulnerability handling processes put in place by the manufacturer, including the software bill of materials, the coordinated vulnerability disclosure policy, evidence of the provision of a contact address for the reporting of the vulnerabilities and a description of the technical solutions chosen for the secure distribution of updates;

(c) necessary information and specifications of the production and monitoring processes of the product with digital elements and the validation of those processes;

3. an assessment of the cybersecurity risks against which the product with digital elements is designed, developed, produced, delivered and maintained pursuant to Article 13, including how the essential cybersecurity requirements set out in Part I of Annex I are applicable;

[…]

Overview

4. CRA: What do we get? Overall picture

Recital 32 of the Cyber Resilience Act

"[…] Data protection by design and by default, and cybersecurity in general, are key elements of Regulation (EU) 2016/679. By protecting consumers and organisations from cybersecurity risks, the essential cybersecurity requirements laid down in this Regulation are also to contribute to enhancing the protection of personal data and privacy of individuals. […]"

Overview

1. Flying blind …
2. Upcoming: security by design
3. Relief for DPOs?
4. CRA: What do we get?
5. Disease ⇆ Cure
6. Conclusion & Outlook

Sounds good. But:

Do security measures always contribute to enhancing data protection?

Overview

5. Is the Cure worse than the Disease?

- What if a security measure itself creates a risk?
- When processing personal data: the GDPR++ applies
- E.g. for logging, surveillance of employees, use of biometrics, malware scanning …

Image: Sabrina Belle via Pixabay

5. Disease ⇆ Cure

- Security as a legal obligation under the GDPR: What is required, what is permitted?
- What is permitted:
  - No processing of personal data without a legal basis
  - This also applies to technical and organisational measures (TOMs) that process personal data
- Typical legal bases:
  - Compliance with a legal obligation: Art. 6(1)(c) GDPR (in conjunction with ... e.g., Art. 32 GDPR or NIS-2 law)
  - Balancing of interests: Art. 6(1)(f) GDPR
  - Necessity, proportionality, ...

Overview

5. Disease ⇆ Cure
(Absence of) a security measure creates risks

Risks to consider if …

… there is no logging	… logging takes place
Unlawful changes of purpose	Disproportionate logging
Lack of examinability	Disclosure of confidential data
Difficulty in controlling the processing	Monitoring of conduct and performance of employees
Uncertainty regarding the correctness of processing	Manipulation of logfiles
Uncertainty regarding the availability of processing (in retrospect)	
Lack of confidentiality	
Non-compliant data processing	
Dynamic changes in IT	
Inability to resolve security incidents	

"TOM-TOMs"

Suitable TOMs for the TOM "Logging", e.g. access control, protection against manipulation, processes for analysis/investigation, appropriate deletion periods …

Source: New building block „Protokollieren" of the Standard Data Protection Model: https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V3.1_Protokollieren_V2.0.pdf

Example: Malware scan

Federal Office for Information Security

OPS.1.1.4 Protection Against Malware

Cloud services designed to improve the detection performance of virus protection programs SHOULD be used. If the cloud functions of such products are used, it MUST be ensured that there are no conflicts regarding data or confidentiality protection. In addition to real-time and on-demand scans, it MUST also be possible to scan compromised and encrypted data for malware with the solution chosen.

OPS.1.1.4.A5 Operation and Configuration of Virus Protection Programs (B)

Virus protection programs MUST be configured appropriately for their operational environment. The focus SHOULD be on detection performance unless data protection or performance reasons influence this in individual cases. If the security-relevant functions of a virus protection program are not used, this SHOULD be explained and documented. In the case of protection programs that are specially optimised for desktop virtualisation, it SHOULD be transparently documented whether certain detection procedures have been omitted in

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi_it_gs_comp_2022.html

Overview

Example: Malware scan

ars TECHNICA

PRYING EYES —

Microsoft is scanning the inside of password-protected zip files for malware

If you think a password prevents scanning in the cloud, think again.

DAN GOODIN - 5/16/2023, 2:15 AM

https://arstechnica.com/information-technology/2023/05/microsoft-is-scanning-the-inside-of-password-protected-zip-files-for-malware/

Sumarigo-MSFT
46,286 • Microsoft Employee

Aug 28, 2024, 5:18 PM

[…]

Microsoft Defender for Storage performs a full malware scan on uploaded content in near real-time using Microsoft Defender Antivirus capabilities. It is designed to help fulfill security and compliance requirements for handling untrusted content. However, there is a file size limit of 2 GB for each scan. Additionally, Microsoft has methods for scanning the contents of password-protected zip files, such as extracting possible passwords from the bodies of an email or the name of the file itself

https://learn.microsoft.com/en-us/answers/questions/2007466/are-costs-incurred-when-attempting-to-scan-passwor

Overview

Example: Malware scan

ars TECHNICA

PRYING EYES —

Microsoft is scanning the inside of password-protected zip files for malware

If you think a password prevents scanning in the cloud, think again.

DAN GOODIN - 5/16/2023, 2:15 AM

https://arstechnica.com/information-technology/2023/05/microsoft-is-scanning-the-inside-of-password-protected-zip-files-for-malware/

Sumarigo-MSFT
46,286 • Microsoft Employee
Aug 28, 2024, 5:18 PM

To mitigate the impact on monthly limits, you might consider the following approaches:

1. **File Size Management**: Ensure that the size of the password-protected zip files does not exceed the 2 GB limit to avoid unnecessary consumption of the scanning quota.
2. **Password Management**: Use common passwords that Microsoft Defender can easily extract and scan, reducing the likelihood of these files being counted as unscannable.
3. **Quota Monitoring**: Regularly monitor the scanning quota usage and adjust the storage and scanning policies accordingly.

…uploaded content in near
…esigned to help fulfill
…ontent. However, there is a
…methods for scanning the
…sible passwords from the

https://learn.microsoft.com/en-us/answers/questions/2007466/are-costs-incurred-when-attempting-to-scan-passwor

Overview

Example: Access control with biometrics

MARCH 30, 2022

New Evidence that Biometric Data Systems Imperil Afghans

Taliban Now Control Systems with Sensitive Personal Information Published in

The Taliban control systems holding sensitive biometric data that Western donor governments left behind in Afghanistan in August 2021, putting thousands of Afghans at risk, Human Rights Watch said today.

A United States military official takes the fingerprints of a man in Afghanistan.

© 2010 AP Photo/Julie Jacobson

These digital identity and payroll systems contain Afghans' personal and biometric data, including iris scans, fingerprints, photographs, occupation, home addresses, and names of relatives. The Taliban could use them to target perceived opponents, and Human Rights Watch research suggests that they may have already used the data in some cases.

https://www.hrw.org/node/381593/printable/print

BR24 How Biometric Devices Are Putting Afghans in Danger

27.12.2022 06:12

How Biometric Devices Are Putting Afghans in Danger

By Rebecca Ciesielski, Maximilian Zierer

Reporting by Bayerischer Rundfunk has found that the lives of people in Afghanistan are in danger because Western militaries failed to protect biometric data from the Taliban. Their fates could be sealed due to biometric scanners that NATO troops left behind in the country.

https://interaktiv.br.de/biometrie-afghanistan/en/

Overview

1. Flying blind …
2. Upcoming: security by design
3. Relief for DPOs?
4. CRA: What do we get?
5. Disease ⇆ Cure
6. Conclusion & Outlook

Example: Access control with biometrics

EURACTIV

LEAKS: EU Parliament mulls using MEPs' fingerprints to register attendance, 03.10.2023

The European Data Protection Supervisor (EDPS), which is responsible for ensuring that European institutions respect the right to privacy and data protection when they process personal data, has made a series of recommendations to ensure that the Parliament's new biometric data system conforms with the data protection laws drafted and agreed by MEPs.

According to the document seen by Euractiv, the Parliament believes that it is feasible to implement all the recommendations except one, regarding the 'one-to-many' system of data storage.

Specifically, EDPS recommended that the Parliament use a 'one-to-many' system that allows biometric templates to be changed and cancelled in order to reduce the risks of unauthorised access to biometric data. The EDPS also pointed to the value of using a 'one-to-one system' in which no biometric data would be stored on the local database of fingerprint readers.

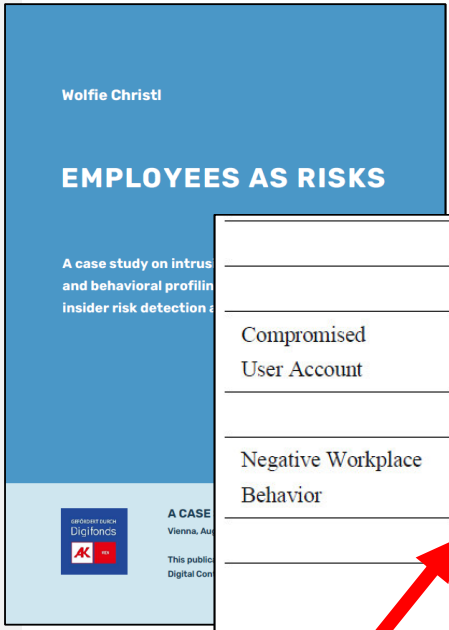
The Parliament consulted its service provider on this point but the company indicated that the use of renewable and cancellable templates would affect the biometric performance and was not supported by their system, Euractiv understands.

https://edps.europa.eu/data-protection/our-work/publications/opinions/2023-05-11-edps-opinion-mep-biometric-attendance-register_en
https://www.euractiv.com/section/data-protection/news/leaks-eu-parliament-mulls-using-meps-fingerprints-to-register-attendance/

Overview

1. Flying blind …
2. Upcoming: security by design
3. Relief for DPOs?
4. CRA: What do we get?
5. Disease ⇆ Cure
6. Conclusion & Outlook

Example: DLP, IDS, SIEM, UEBA, Zero Trust ⇆ Employee surveillance?



	Suspicious Research	People researching ways to commit suspicious actions
	Physical Access	Abnormal physical access to sensitive areas
Compromised User Account	Phishing	Risk of employees falling victim to phishing, for example through malicious attachments or links in emails [description by the author of this study]
	Malware	Risk that employees have unintentionally installed malware [description by the author of this study]
Negative Workplace Behavior	Obscene Content	Obscene content activity, either through web searches or web browsing
	Negative Sentiment	Negative sentiment and signs of improper discussions within communications
	Flight Risk Communications	Communications conducive with an employee leaving, such as emailing a resume or searching for a new job
	Financial Distress Communications	Communications activity indicative of financial turmoil and employees looking for a way to get re-solve the issue
	Oversight Evasion	Signs of oversight evasion attempts within communications
	Decreased Productivity	Employees spending a large amount of time doing non work related tasks
	Corporate Disengagement	Employees who are not interacting with core company assets
	Recipient Cardinality	Users talking to less employees, compared to their previous baselined activity

https://crackedlabs.org/dl/CrackedLabs_Christl_SecurityRiskProfiling.pdf, p. 16

DLP: Data Loss Prevention
IDS: Intrusion Detection System
IPS: Intrusion Prevention System
IRM: Insider Risk Management
SIEM: Security Information Event Management
UEBA: User and Entity Behaviour Analytics
Zero Trust: "Never trust, always check"

Overview

1. Flying blind …
2. Upcoming: security by design
3. Relief for DPOs?
4. CRA: What do we get
5. Disease ⇆ Cure
6. Conclusion & Outlook

Example: DLP, IDS, SIEM, UEBA, Zero Trust ⇆ Employee surveillance?

Organizations must protect themselves from cyberattacks, data loss and criminal misconduct. This is not optional, and, in several ways, mandated by law. Nevertheless, **intrusive security and risk surveillance raises serious concerns** about misuse by employers, disproportionate monitoring and profiling across purposes, flawed risk assessments and arbitrary suspicions. As discussed in the final section of this study, **employers can potentially misuse** these technologies to spy on employees, target organized labor, suppress internal dissent, apply excessive behavioral policing or impose arbitrary disciplinary action. These systems **put employees under general suspicion** and can undermine privacy, human dignity, autonomy, freedom of expression and trust in the workplace. [...]

https://crackedlabs.org/dl/CrackedLabs_Christl_SecurityRiskProfiling.pdf, p. 5

DLP: Data Loss Prevention
IDS: Intrusion Detection System
IPS: Intrusion Prevention System
IRM: Insider Risk Management
SIEM: Security Information Event Management
UEBA: User and Entity Behaviour Analytics
Zero Trust: "Never trust, always check"

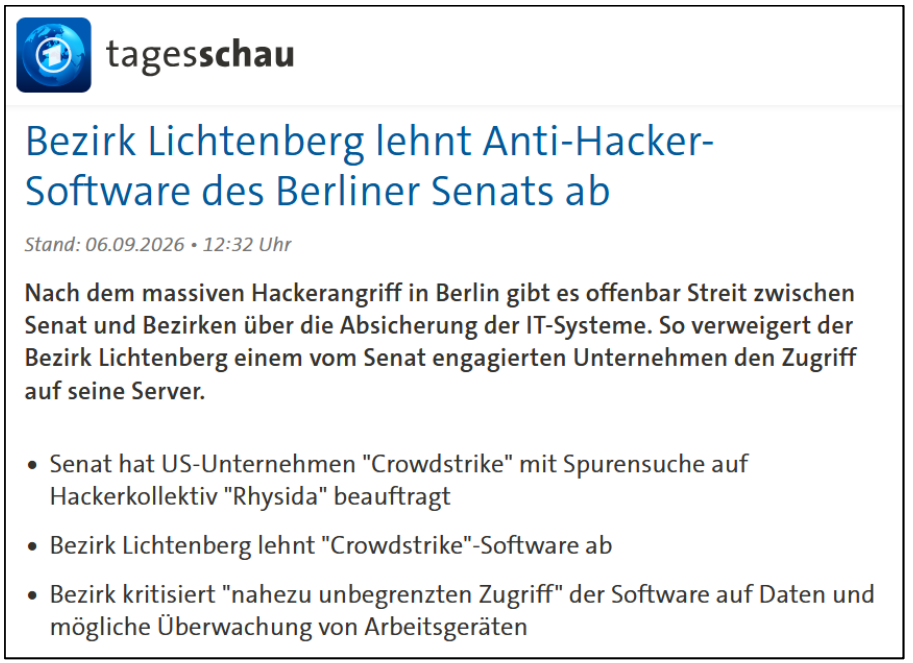
Overview

Example: no adequate level of data protection – software and services

Case "Berlin Hack", August-September 2026:

Ex-post data breach measure: Usage of security software with data protection risk:

- Berlin senate commissions US company CrowdStrike to investigate hacker attack
- Lichtenberg district rejects CrowdStrike because of the software's "virtually unlimited access" to data and potential monitoring of work devices



tagesschau

Bezirk Lichtenberg lehnt Anti-Hacker-Software des Berliner Senats ab

Stand: 06.09.2026 • 12:32 Uhr

Nach dem massiven Hackerangriff in Berlin gibt es offenbar Streit zwischen Senat und Bezirken über die Absicherung der IT-Systeme. So verweigert der Bezirk Lichtenberg einem vom Senat engagierten Unternehmen den Zugriff auf seine Server.

- Senat hat US-Unternehmen "Crowdstrike" mit Spurensuche auf Hackerkollektiv "Rhysida" beauftragt
- Bezirk Lichtenberg lehnt "Crowdstrike"-Software ab
- Bezirk kritisiert "nahezu unbegrenzten Zugriff" der Software auf Daten und mögliche Überwachung von Arbeitsgeräten

https://www.tagesschau.de/inland/regional/berlin/rbb-bezirk-lichtenberg-lehnt-anti-hacker-software-des-berliner-senats-ab-102.html

Overview

6. Conclusion & Outlook

- Situation of today:
  Data controllers have no idea! (more often than not)
- This means: Accountability is effectively rendered meaningless.
- Upcoming: security by design. In products. (Blind spot of the GDPR.)
- Cybersecurity legislation and product liability may be a game changer!
- Valuable for data protection (Art. 32 GDPR),
  valuable as source of information on data processing
- DPOs should not only applaud ☺, but demand information on security

Overview

6. Conclusion & Outlook

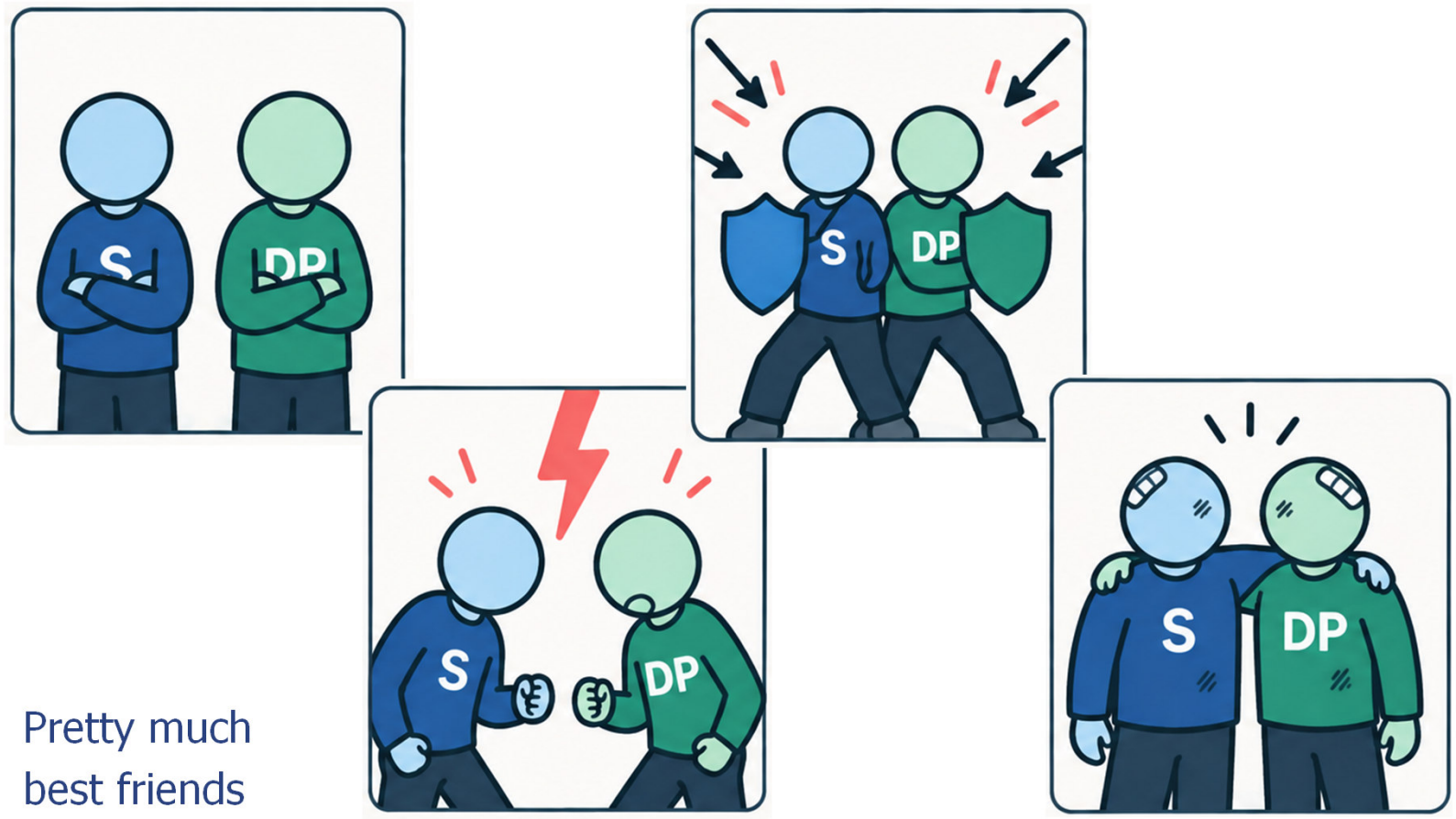
- However: be aware of potential tensions between security and data protection
- All data protection principles have to be taken into account
- "Security first and foremost" could become a problematic trend

- Legal basis, proportionality, think also about "TOM-TOMs"
- Joint effort needed to integrate the different perspectives. ISMS + DPO + works councils++ should work together. Communication is key.

Image: ChatGPT

Overview

6. Conclusion & Outlook



Pretty much best friends