

Practical problems in enforcing Data Protection by Design & by Default – the perspective of a Data Protection Authority

Marit Hansen

Data Protection Commissioner
Schleswig-Holstein, Germany

Chalmers Security & Privacy Lab, Göteborg
23 September 2022



Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Setting of ULD

- Data Protection Authority (DPA) for both the public and private sector
- Also responsible for freedom of information

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)
• Bundestag seats	28 (of 736)
Area	
• Total	15,804 km ² (6,102 sq mi)
Population (04.01.2022)^[1]	
• Total	2,920,850
• Density	180/km ² (480/sq mi)

Berlin



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

Enforcing Data Protection by

Source: www.maps-for-free.com

Overview



1. Data protection law and its objectives
2. Enforcement of the GDPR: task of the Data Protection Authorities
3. Art. 25 GDPR: Data Protection by Design & by Default
4. Status quo & difficulties
5. Further levers & wishlist
6. Conclusion



Source: Gerd Altmann via Pixabay

Imbalance
in power



data protection
necessary

Important:
Perspective of
the individual

More than
security of
personal data



Source: beludise via Pixabay

General Data Protection Regulation

- Idea: **One for All**
and
All for One

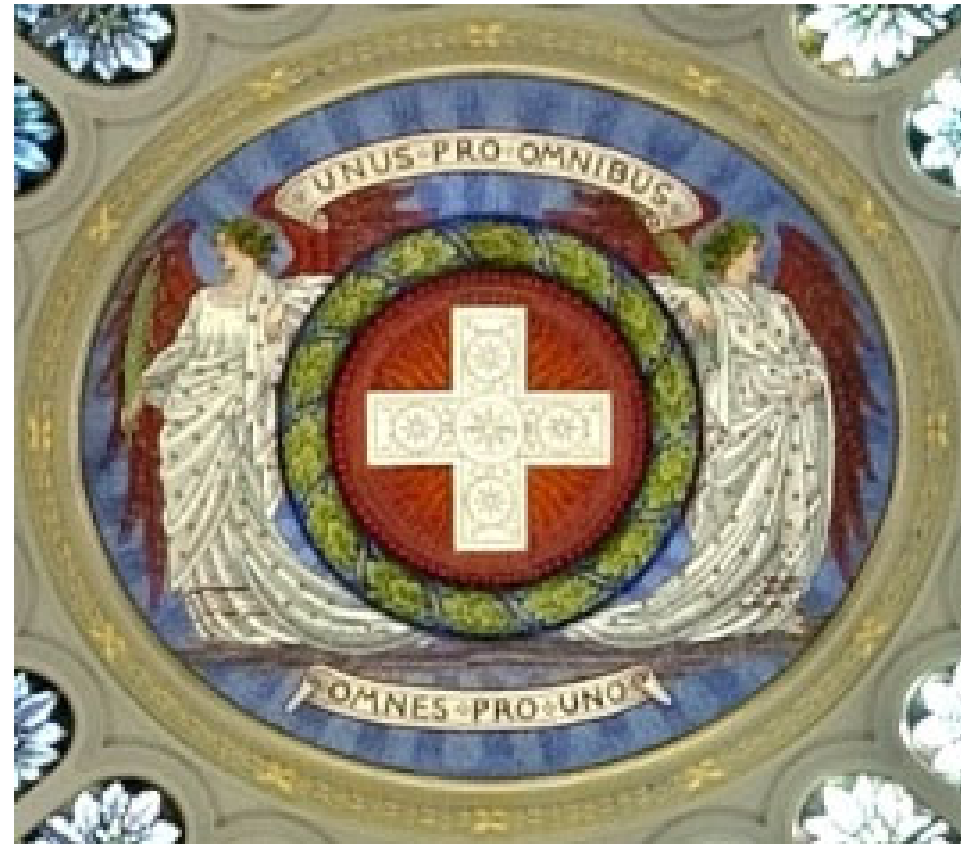
- Objectives:
real **harmonisation**,
"level playing field",
legal **certainty**,
European **enforcement**

Abstract wording

Significant sanctions

- Procedural** rights:

- [Art. 77, 78] ■ Data subject – DPA
- [Art. 79, 82] ■ Data subject – controller
- [Art. 80 GDPR] ■ Representative actions



https://upload.wikimedia.org/wikipedia/commons/8/85/Unus_pro_omnibus%2C_omnes_pro_uno.jpg

GDPR as "Game Changer" (?)

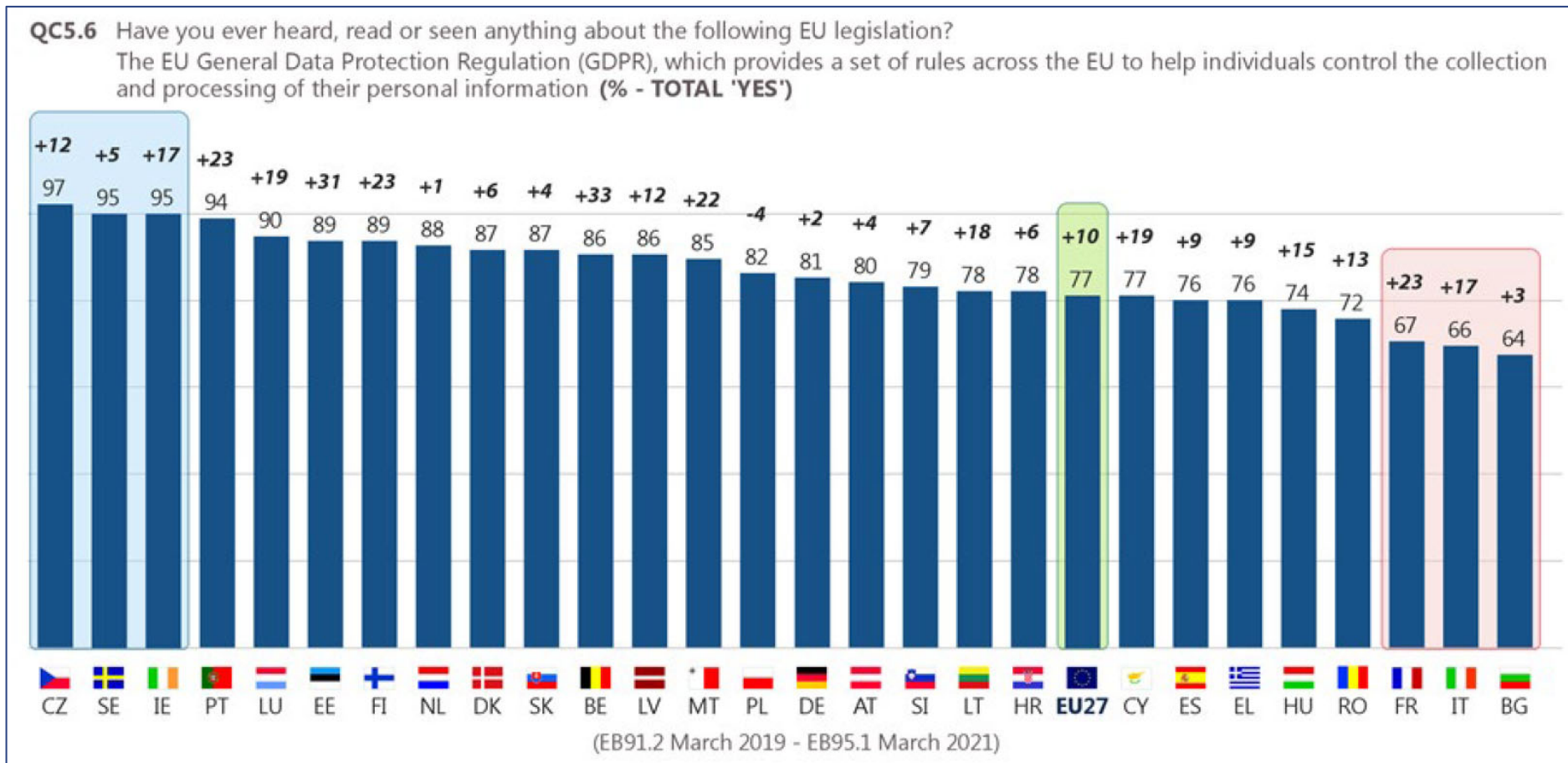


Source: Astryd_MAD via Pixabay

Powerful **toolbox**
if applied
appropriately

- **Market location principle** (Art. 3 GDPR) 
- **Responsibility** (Art. 24 GDPR)
- **Data protection by design** (Art. 25(1) GDPR) 
- **Data protection by default** (Art. 25(2) GDPR)
- **Security** (Art. 32 GDPR)
- **Data protection impact assessment** (Art. 35 GDPR – "Rights and freedoms of natural persons")
- **Certification** (Art. 42+43 GDPR)
- **Fines & sanctions by Data Protection Commissioners** (Art. 83+84 GDPR) 
- **Courts** 

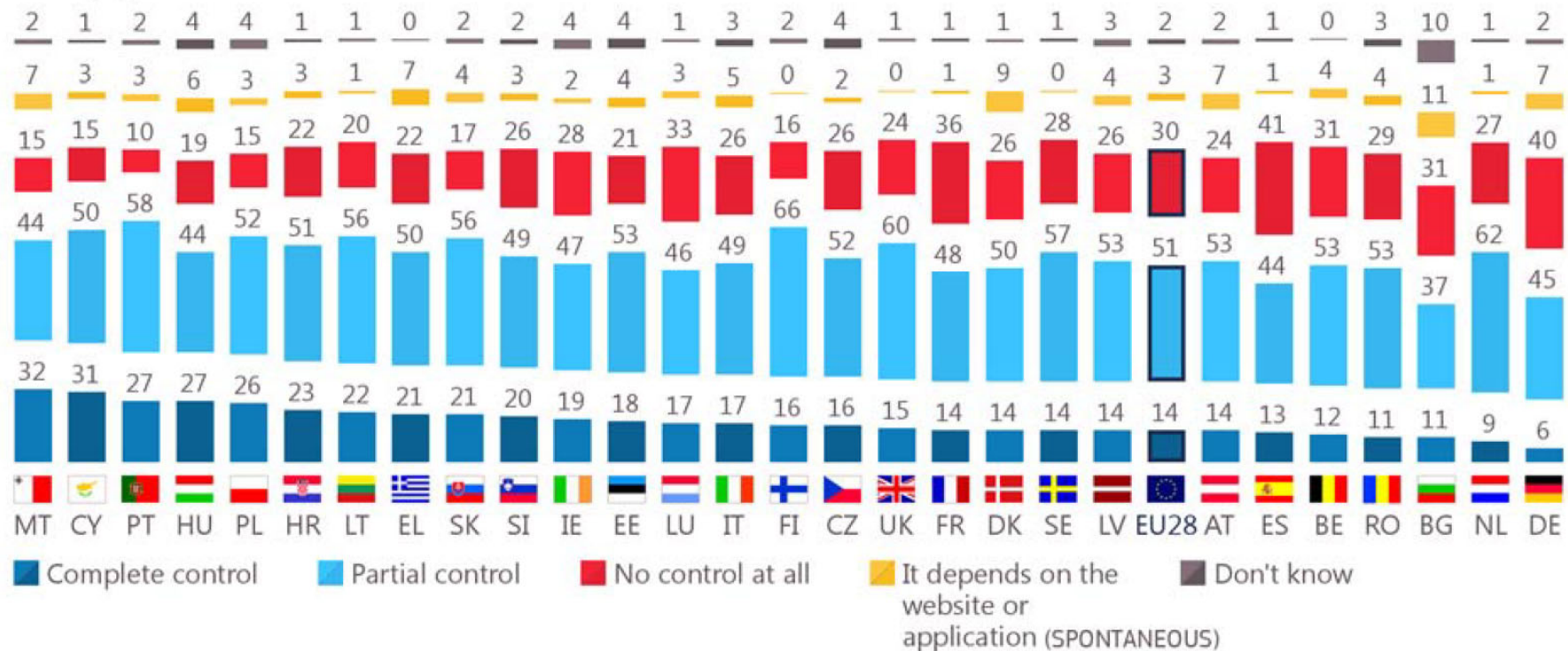
Eurobarometer: "heard about the GDPR" (2021 compared with 2019)



<https://webgate.ec.europa.eu/ebsm/api/public/deliverable/download?doc=true&deliverableId=76246>, S. 29

Eurobarometer 2019: online full control?

QB9 How much control do you feel you have over the information you provide online, e.g. the ability to correct, change or delete this information?
(%)



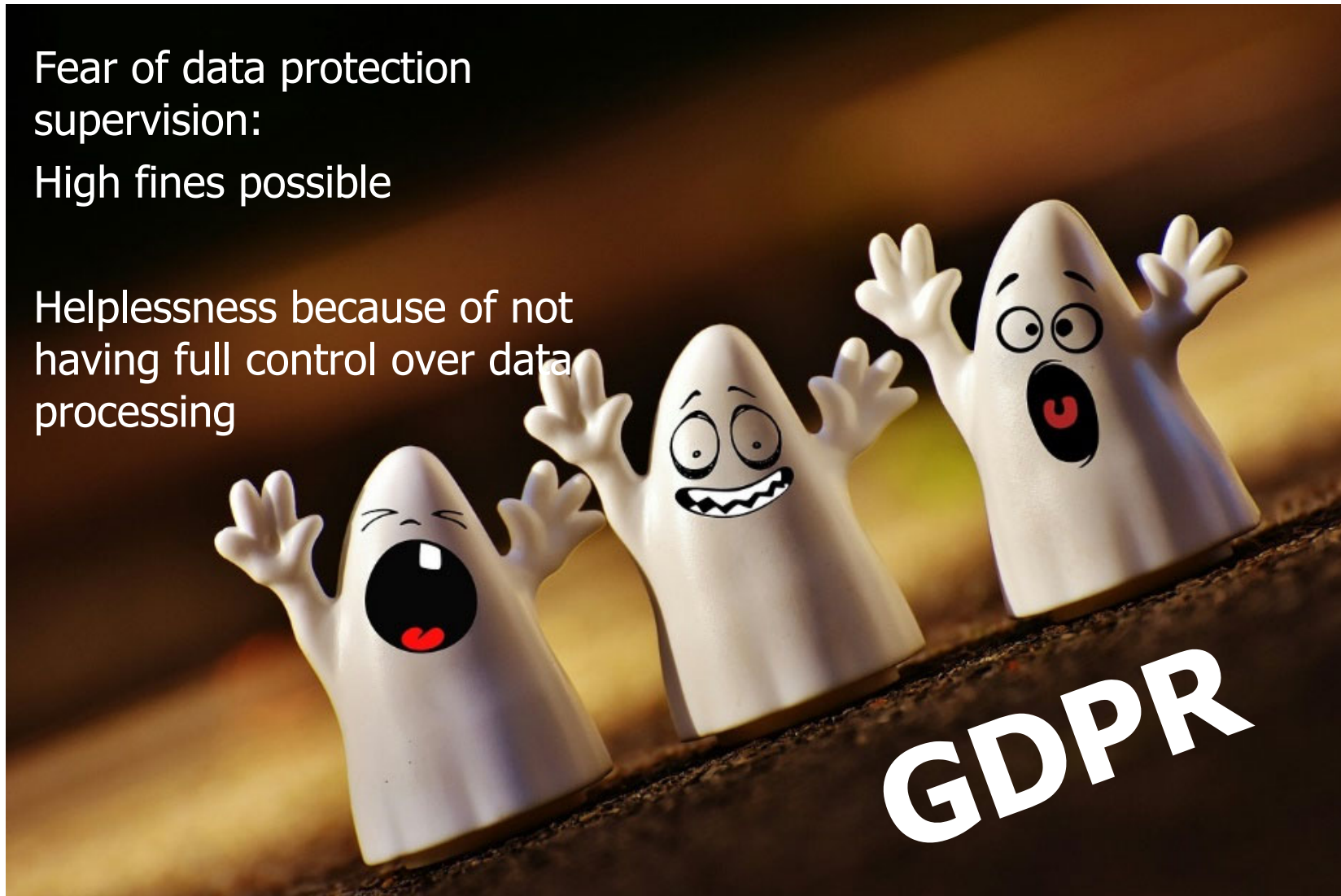
Base: respondents who have provided personal information online (N=18,975)

<https://webgate.ec.europa.eu/ebsm/api/public/deliverable/download?doc=true&deliverableId=69701>, S. 35

Nightmare GDPR?

Fear of data protection supervision:
High fines possible

Helplessness because of not having full control over data processing



Overview



1. Data protection law and its objectives
2. **Enforcement of the GDPR: task of the Data Protection Authorities**
3. Art. 25 GDPR: Data Protection by Design & by Default
4. Status quo & difficulties
5. Further levers & wishlist
6. Conclusion



Source: Gerd Altmann via Pixabay

Tasks – Art. 57 GDPR

Article 57

Tasks

1. Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

(a) monitor and enforce the application of this Regulation;

(b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;

(c) advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;

(d) promote the awareness of controllers and processors of their obligations under this Regulation;

(e) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;

(f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 30, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

(g) cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;

(h) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;

(i) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;

(j) adopt standard contractual clauses referred to in Article 28(3) and in point (d) of Article 46(2);

(k) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4);

(l) give advice on the processing operations referred to in Article 36(2);

(m) encourage the drawing up of codes of conduct pursuant to Article 40(1) and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5);

(n) encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5);

(o) where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7);

(p) draft and publish the requirements for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

(q) conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

(r) authorise contractual clauses and provisions referred to in Article 46(3);

(s) approve binding corporate rules pursuant to Article 47;

(t) contribute to the activities of the Board;

(u) keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and

(v) fulfil any other tasks related to the protection of personal data.

2. Each supervisory authority shall facilitate the submission of complaints referred to in point (f) of paragraph 1 by measures such as a complaint submission form which can also be completed electronically, without excluding other means of communication.

3. The performance of the tasks of each supervisory authority shall be free of charge for the data subject and, where applicable, for the data protection officer.

4. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

... monitor and enforce the application of this Regulation ...

- 1) Investigative powers
- 2) Corrective powers
- 3) Authorisation and advisory powers

Powers – Art. 58 GDPR

Article 58

Powers

1. Each supervisory authority shall have all of the following investigative powers:

- (a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;
- (b) to carry out investigations in the form of data protection audits;
- (c) to carry out a review on certifications issued pursuant to Article 42(7);
- (d) to notify the controller or the processor of an alleged infringement of this Regulation;
- (e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;
- (f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

2. Each supervisory authority shall have all of the following corrective powers:

- (a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;
- (b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;
- (c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

(e) to order the controller to communicate a personal data breach to the data subject;

(f) to impose a temporary or definitive limitation including a ban on processing;

(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;

(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;

(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

(j) to order the suspension of data flows to a recipient in a third country or to an international organisation.

3. Each supervisory authority shall have all of the following authorisation and advisory powers:

(a) to advise the controller in accordance with the prior consultation procedure referred to in Article 36;

(b) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;

(c) to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation;

(d) to issue an opinion and approve draft codes of conduct pursuant to Article 40(5);

(e) to accredit certification bodies pursuant to Article 43;

(f) to issue certifications and approve criteria of certification in accordance with Article 42(5);

(g) to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2);

(h) to authorise contractual clauses referred to in point (a) of Article 46(3);

(i) to authorise administrative arrangements referred to in point (b) of Article 46(3);

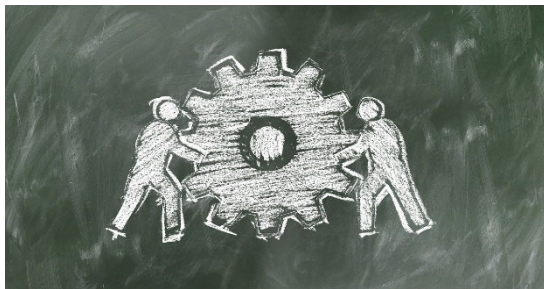
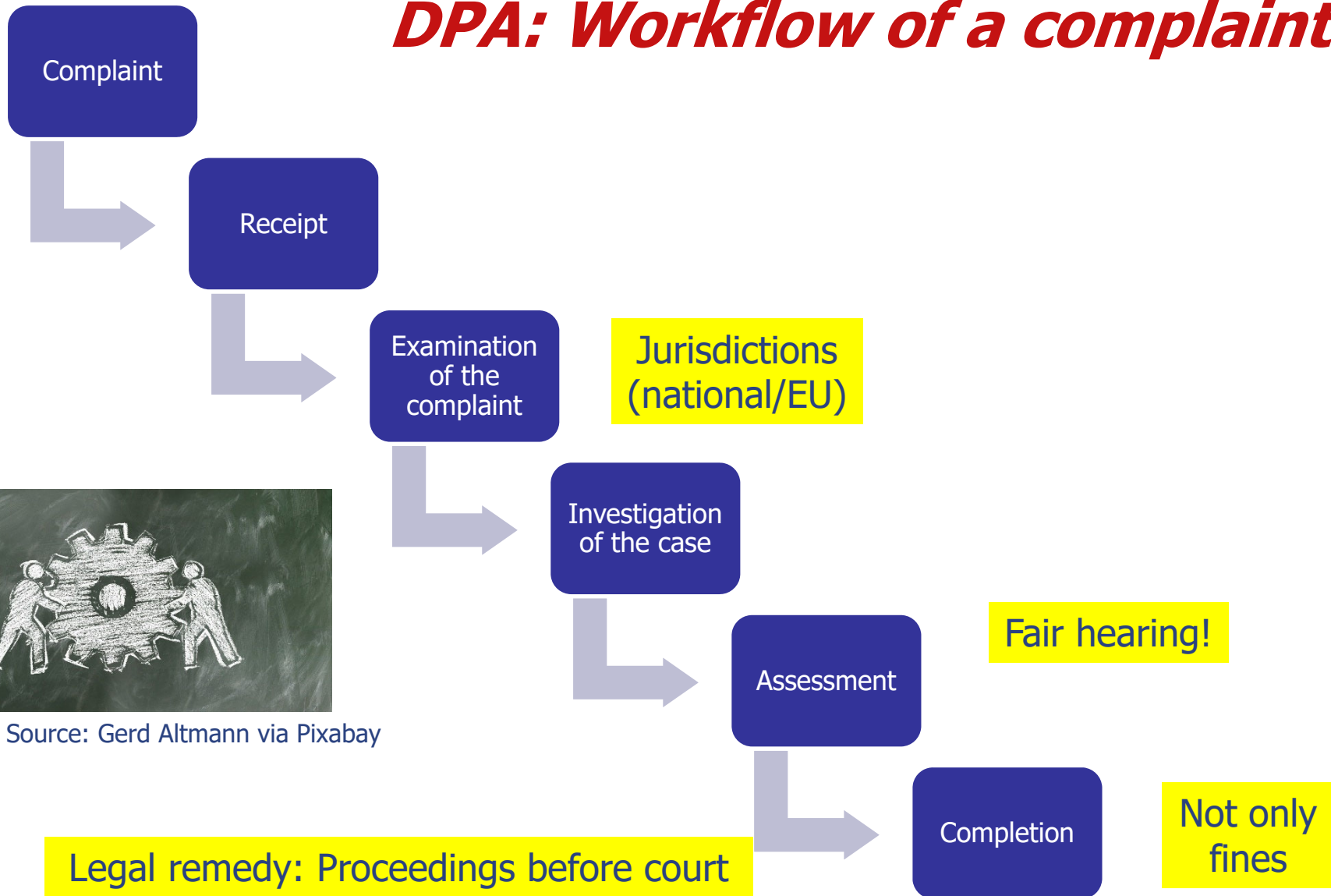
(j) to approve binding corporate rules pursuant to Article 47.

4. The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter.

5. Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation.

6. Each Member State may provide by law that its supervisory authority shall have additional powers to those referred to in paragraphs 1, 2 and 3. The exercise of those powers shall not impair the effective operation of Chapter VII.

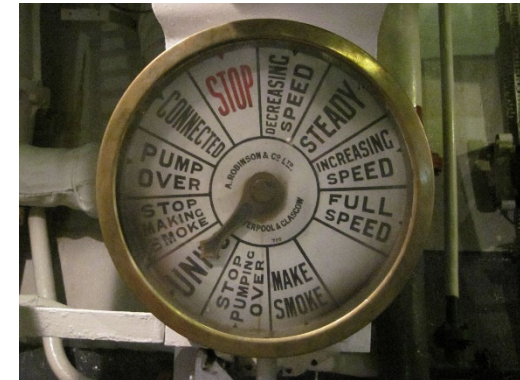
DPA: Workflow of a complaint



Source: Gerd Altmann via Pixabay

Art. 58 (2) GDPR: Corrective powers

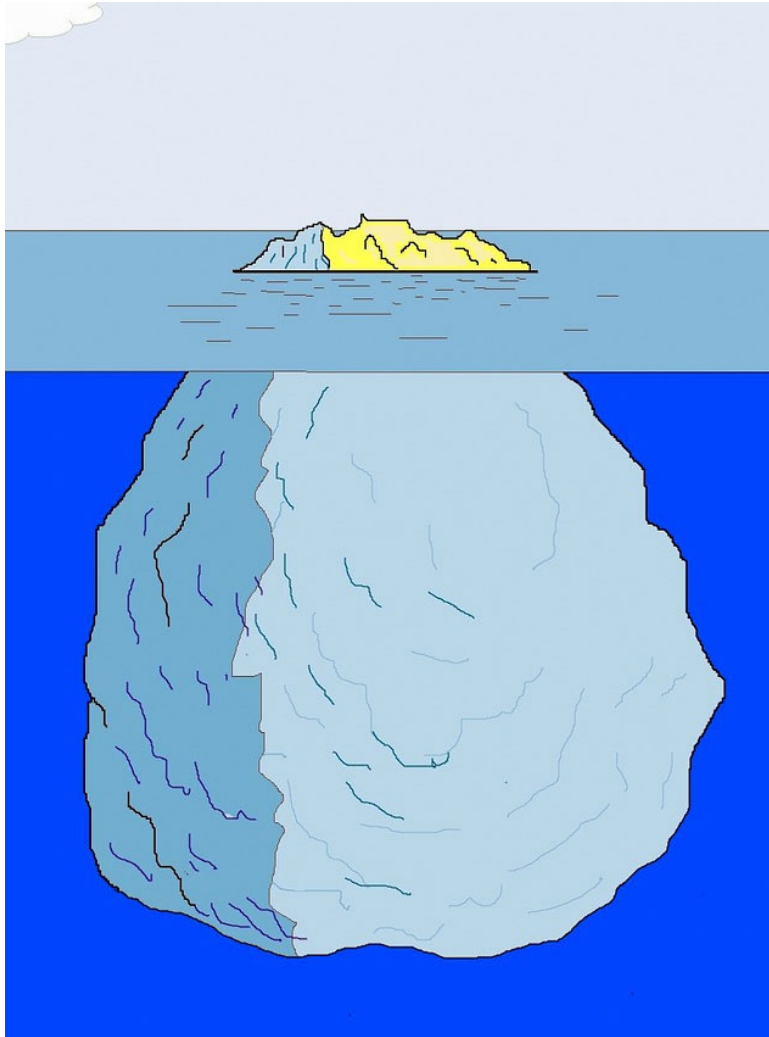
- Issue **warnings** (ex ante)
- Issue **reprimands** (ex post)
- **Order** the controller/processor to comply with the data subject's requests
- **Order** the controller/processor to bring processing operations into compliance with the GDPR
- Impose a temporary or definitive **limitation** including a ban on processing
- **Order** the rectification or erasure of personal data
- Impose an administrative **fine**
- **Order** the suspension of data flows to a recipient



Source: Sriom via Pixabay

**Common:
Legal remedy
against
the decision**

Investigations by DPAs



- Relevance of regular investigations:
 - Complaints only address the **visible part**
 - How to deal with **structural effects?**
- Problem of **non-auditability**: termination of investigation?
- Investigations **always after the fact** (unless prior consultation)
- Moving targets: **changing** systems
- **Sisyphian task: effort**



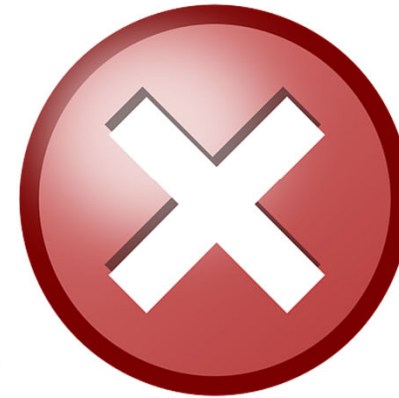
Source: Josep Monter Martinez
via Pixabay

Resources? Effort? Target of evaluation?



DPA's assessments can be powerful and influence the market

DPA: "The processing is: ..."



... compliant:

On the basis of

- a) an own investigation [scope]
- b) a certification [Art. 42 GDPR]
- c) a (final) court decision

... not compliant:

On the basis of

- a) an own investigation
[with potential input of security / privacy researchers]
- b) a (final) court decision

https://www.datenschutzkonferenz-online.de/media/oh/20201111_checkliste_oh_videokonferenzsysteme.pdf

Video conferencing: ← joint criteria as checklist

Checkliste Datenschutz in Videokonferenzsystemen		
Stand 11.11.2020		
Bezogen auf die Orientierungshilfe Videokonferenzsysteme, Stand 23.10.2020		
Kapitel in der Orientierungshilfe	Anforderung erfüllt? <small>[ja/kein/nicht zutreffend]</small>	Referenz
3 Rechtliche Anforderungen		
Rollen und Verantwortlichkeiten der Beteiligten sind klar verteilt und eindeutig festgelegt (Art. 4 Nr. 7 DS-GVO i.V.m. Art. 28 Abs. 3 und/oder Art. 26 DS-GVO).		
3.1 Selbst betriebener Dienst		
Der Betreiber des Videokonferenzsystems ist sich seiner Verantwortlichkeit im Sinne der DS-GVO bewusst, da er oder sie im Rahmen des Einsatzes dieses Systems über die Zwecke und Mittel der Verarbeitung bestimmt.		
Es bestehen jeweils die erforderlichen Rechtsgrundlagen für die unterschiedlichen Verarbeitungen personenbezogener Daten durch den selbst betriebenen Dienst.		
Der Verantwortliche setzt für Betrieb und Wartung ausreichende technische und personelle Kapazitäten ein.		
Der Verantwortliche ergreift geeignete technische und organisatorische Maßnahmen zum Schutz der Daten.		
3.2 Betrieb durch einen externen IT-Dienstleister		
Der Verantwortliche (im Folgenden auch: der Veranstalter) hat einen wirksamen Vertrag zur Auftragsverarbeitung nach Art. 28 DS-GVO mit dem IT-Dienstleister abgeschlossen.		
Der Auftragsverarbeiter (im Folgenden auch: der Anbieter) bietet hinreichende Garantien zu den erforderlichen technischen und organisatorischen Maßnahmen (Art. 28 Abs. 1 DS-GVO).		
Die eingesetzte oder Teilnehmenden angebotene Software wurde auf Datenabflüsse überprüft. Dies schließt Diagnose- und Telemetriedaten oder sonstige Datenabflüsse z.B. an Hersteller ein.		
Entsprechende Datenabflüsse wurden unterbunden, soweit nicht eine Rechtsgrundlage hierfür besteht.		
3.3 Online-Dienst		
Im Falle einer Verarbeitung zu eigenen Zwecken durch den Anbieter verfügt der Veranstalter für jede Offenlegung personenbezogener Daten an den Anbieter über eine Rechtsgrundlage.		
Der Anbieter verfügt für jede Verarbeitung personenbezogener Daten in eigener Verantwortlichkeit über eine Rechtsgrundlage.		
Die Notwendigkeit einer Vereinbarung zur gemeinsamen Verantwortlichkeit		

	<input type="checkbox"/>	6	meetzi	https://meetzi.de	meetzi – Auftragsverarbeitings (AV)-Vertrag nach Art. 28 DS-GVO, Version 3 (14.12.2020) [Deutsch]
	(v)	<input type="checkbox"/>	Microsoft Teams (unter Geltung der Online Service Terms, etwa als Teil von Microsoft 365 oder in der kostenfreien Version bei Anmeldung in einer Arbeits- oder Organisationsumgebung)	https://www.microsoft.com/de-de/microsoft-365/microsoft-teams/group-chat-software	Anhang zu den Datenschutzbestimmungen für Microsoft-Onlinedienste Januar 2020 [Deutsch] – Dateiversionen (laut Metadaten) vom 3.1.2020 und 9.6.2020 (Version ist im Dokument selbst nicht ersichtlich); Microsoft-Onlinedienste Nachtrag zum Datenschutz, Letzte Aktualisierung: 21. Juli 2020 [Deutsch]; Additional Safeguards Addendum to Standard Contractual Clauses (Reference Copy gemäß Ankündigung November 2020) [Englisch]; Microsoft Online Services Data Protection Addendum, Last updated December 9, 2020 [Englisch]
	7	<input type="checkbox"/>	Microsoft Teams (kostenlose Version ohne Anwendbarkeit der Online Service Terms, also nicht bei Anmeldung in einer Arbeits- oder Organisationsumgebung)	https://www.microsoft.com/de-de/microsoft-365/microsoft-teams/group-chat-software	Microsoft-Servicevertrag gültig ab 1. Oktober 2020, Datenschutzerklärung von Microsoft Letzte Aktualisierung: Januar 2021 [Deutsch]
	<input checked="" type="checkbox"/>		NETWAYS Web Services Jitsi	https://nws.netways.de/de/apps/jitsi/	AVV v1.7 [Deutsch]
	<input checked="" type="checkbox"/>		OSC BigBlueButton	https://www.open-source-company.de/bigbluebutton-hosting/	Vertrag zur Verarbeitung von personenbezogenen Daten im Auftrag, Version 1.6 (Stand 16.12.2020) [Deutsch]
	<input checked="" type="checkbox"/>		sichere-videokonferenz.de	https://sichere-videokonferenz.de	Vertrag über die Auftragsverarbeitung personenbezogener Daten nach EU Datenschutz-Grundverordnung Stand 06/2020 [Deutsch]

https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2021-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf

Example: camera-equipped cars in Germany 2008 / 2020

SPiEGEL International

Privacy Concerns

German Towns Saying 'Nein' to Google 'Street View'

Google's corporate slogan might be "don't be evil," but some communities in northwestern Germany see something nefarious in the company's photographing all their streets and houses. If they get their way, they will remain black holes in the universe.


29.09.2008, 17:11 Uhr

Google's mission "to organize the world's information" has just met a formidable foe in the form of the town of Molfsee near Kiel in the northwestern German state of Schleswig-Holstein.

The picturesque, but not picture-friendly town hopes to block the Internet giant from filming its streets and the houses of its fewer than 5,000 inhabitants for its "Street View" program -- a service that provides 360-degree, street level images via the Google Maps search engine.


"We are not going to let this happen," Reinhold Harwart, the leader of the CDU on the town council, told the *Lübecker Nachrichten* daily Sunday. "You can see everything in those photos! That is opening house and home to criminals!"

<https://www.spiegel.de/international/germany/privacy-concerns-german-towns-saying-nein-to-google-street-view-a-581177.html>



About us | Awarders | Press | Support | Contact

Autos überwachen



öffentlichen Raum!

Laudator: Dr. Thilo Weichert

The BigBrotherAward 2020 in the "Mobility" Category goes to

Tesla Inc., represented by Tesla Germany GmbH in Munich,

not for the logging of a Brandenburg forestry to build their new plant, and not for the accidents caused by inattentive drivers who overtrusted Tesla's assistance systems.

Tesla receives this award for marketing cars that extensively and perpetually surveil their passengers and car surroundings. The data obtained is constantly analysed and can be used for any purpose.

<https://bigbrotherawards.de/en/2020/mobility-tesla>

Are there complaints?

Is it a structural problem?

Do we need a structural solution?

Who to address?

What about other member states?

GDPR: highest fines

Statistics: Highest individual fines (Top 10)

The following statistics shows the highest individual fines imposed to date per data controller (only top 10 fines).

	Controller	Sector	Country	Fine [€]	Type of Violation	Date
1	Amazon Europe Core S.à.r.l.	Industry and Commerce	LUXEMBOURG	746,000,000	Non-compliance with general data processing principles	16 Jul 2021
2	WhatsApp Ireland Ltd.	Media, Telecoms and Broadcasting	IRELAND	225,000,000	Insufficient fulfilment of information obligations	02 Sep 2021
3	Google LLC	Media, Telecoms and Broadcasting	FRANCE	90,000,000	Insufficient legal basis for data processing	31 Dec 2021
4	Facebook Ireland Ltd.	Media, Telecoms and Broadcasting	FRANCE	60,000,000	Insufficient legal basis for data processing	31 Dec 2021
5	Google Ireland Ltd.	Media, Telecoms and Broadcasting	FRANCE	60,000,000	Insufficient legal basis for data processing	31 Dec 2021
6	Google LLC	Media, Telecoms and Broadcasting	FRANCE	50,000,000	Insufficient legal basis for data processing	21 Jan 2019
7	H&M Hennes & Mauritz Online Shop A.B. & Co. KG	Employment	GERMANY	35,258,708	Insufficient legal basis for data processing	01 Oct 2020
8	TIM (telecommunications operator)	Media, Telecoms and Broadcasting	ITALY	27,800,000	Insufficient legal basis for data processing	15 Jan 2020
9	Enel Energia S.p.A	Transportation and Energy	ITALY	26,500,000	Insufficient legal basis for data processing	16 Dec 2021
10	British Airways	Transportation and Energy	UNITED KINGDOM	22,046,000	Insufficient technical and organisational measures to ensure information security	16 Oct 2020

<https://www.enforcementtracker.com/?insights>

Overview



1. Data protection law and its objectives
2. Enforcement of the GDPR: task of the Data Protection Authorities
3. **Art. 25 GDPR: Data Protection by Design & by Default**
4. Status quo & difficulties
5. Further levers & wishlist
6. Conclusion



Source: Gerd Altmann via Pixabay

Data Protection by Design & by Default

- Art. 25 GDPR
- Targeted at controllers
- Producers of IT systems
“should be encouraged”
(Rec. 78)
- Objective: **to design systems + services**
from early on, for the full lifecycle ...
 - a) ... in a **data-minimising** way
 - b) ... with the most **data protection-friendly pre-settings**

Art. 25 Data Protection by Design and by Default

1. Taking into account the **state of the art**, the **cost** of implementation and the **nature, scope, context and purposes** of processing as well as the **risks** of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, 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**, [...] which are designed to implement data-protection principles [...], in an effective manner [...]

Data Protection by Design & by Default

- Art. 25 GDPR
- Targeted at controllers
- Producers of IT systems
"should be encouraged"
(Rec. 78)

Art. 25 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. [...]

- Objective: to design systems + services from early on, for the full lifecycle ...
 - a) ... in a data-minimising way
 - b) ... with the most data protection-friendly pre-settings

Data Protection Principles – Art. 5 GDPR

Art. 5 GDPR – Principles relating to processing of personal data

Design requirements

(1)

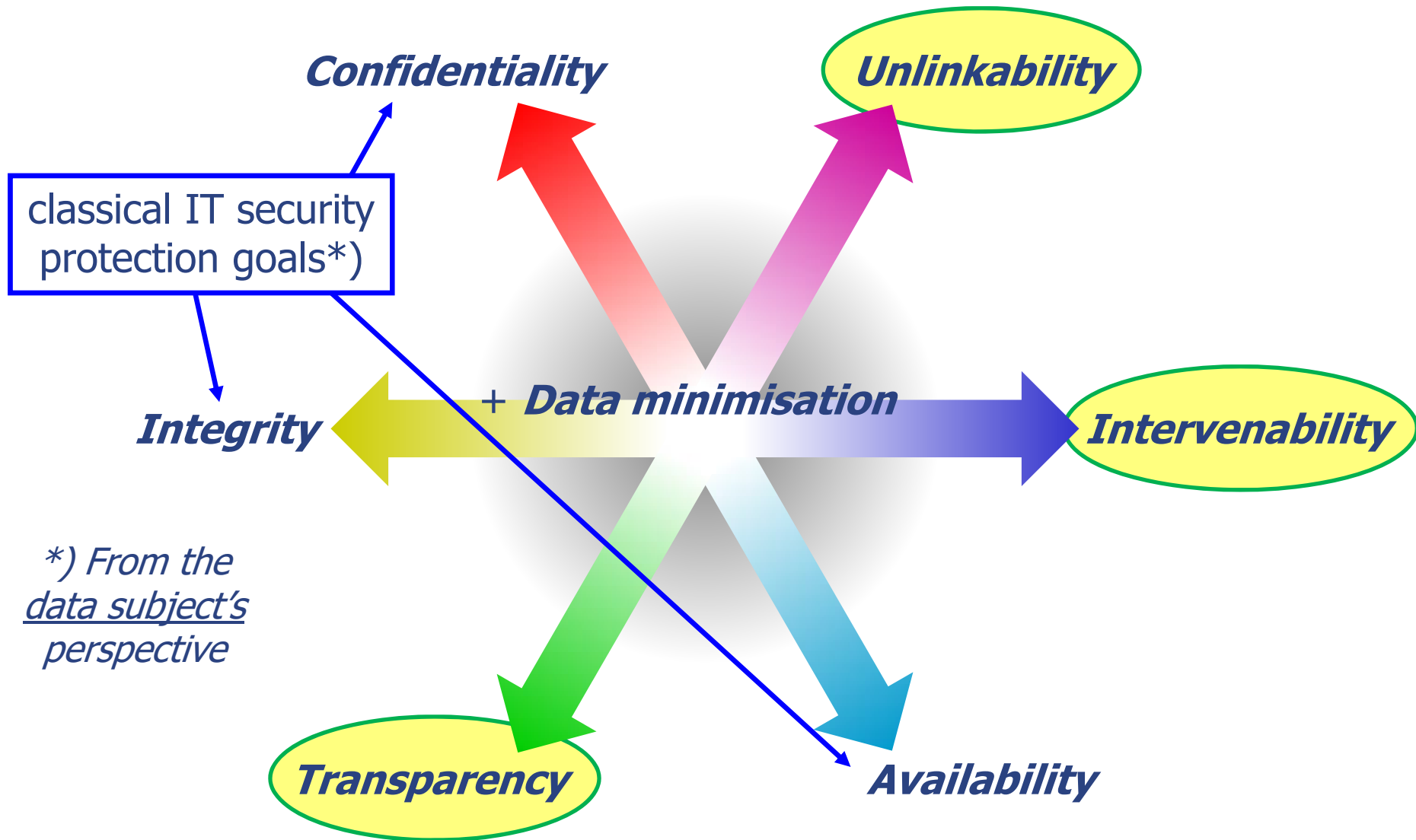
- a) Lawfulness, fairness and **transparency**
- b) **Purpose limitation**
- c) **Data minimisation**
- d) **Accuracy**
- e) **Storage limitation**
- f) Integrity and confidentiality (~ **security**)

Technical and organisational measures



(2) **Accountability**

Standard Data Protection Model



Data minimisation + Unlinkability

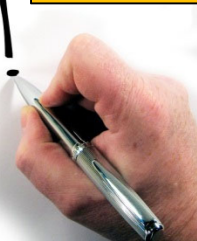
Limit data collection, separation of domains, purpose binding, encryption, anonymisation, pseudonymisation



Source: ivanacoi via Pixabay

Please, help me!

E.g. help desk, deactivation, rectification, objection, legal redress, no automated decisions/reversal of decisions, liability ...



Source: geralt via Pixabay

Intervenability

How to?
Scrutinise the processing, check "starting point" defaults

Transparency

Goal: comprehensibility & auditability

Source: geralt via Pixabay

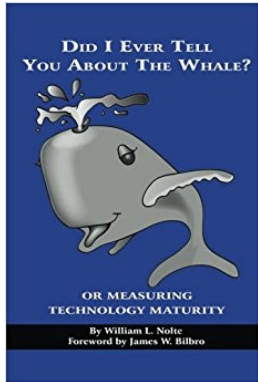
Main goals:

- **Fairness**
- Mitigating the **risk** for the rights and freedoms of natural persons

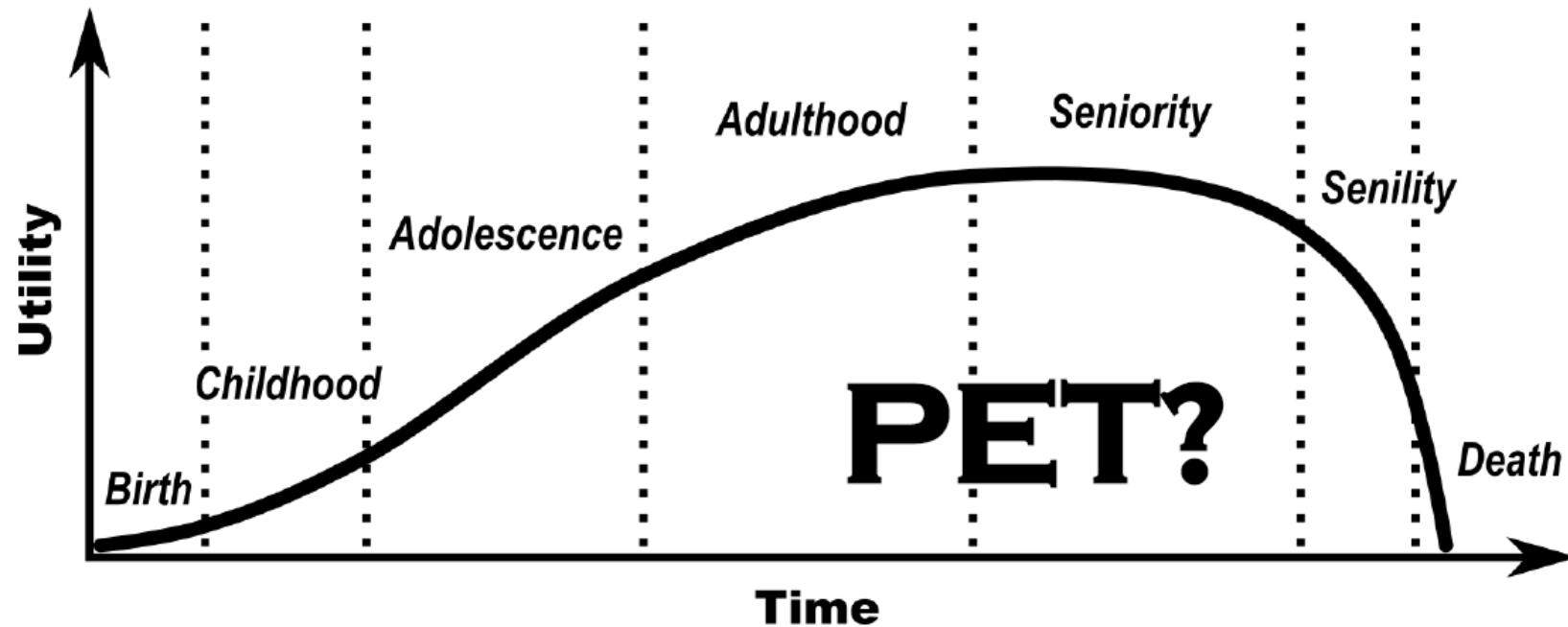
How important is the state of the art?

- Only one of the criteria, but usually sought: standard **market solutions**
- The **"D"** in R & D
- Not to underestimate: **open source code**
- Considering PETs: see "Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies", ENISA 2015
 - <https://www.enisa.europa.eu/publications/pets> (2015)
 - <https://www.enisa.europa.eu/publications/enisa2019s-pets-maturity-assessment-repository> (2019)



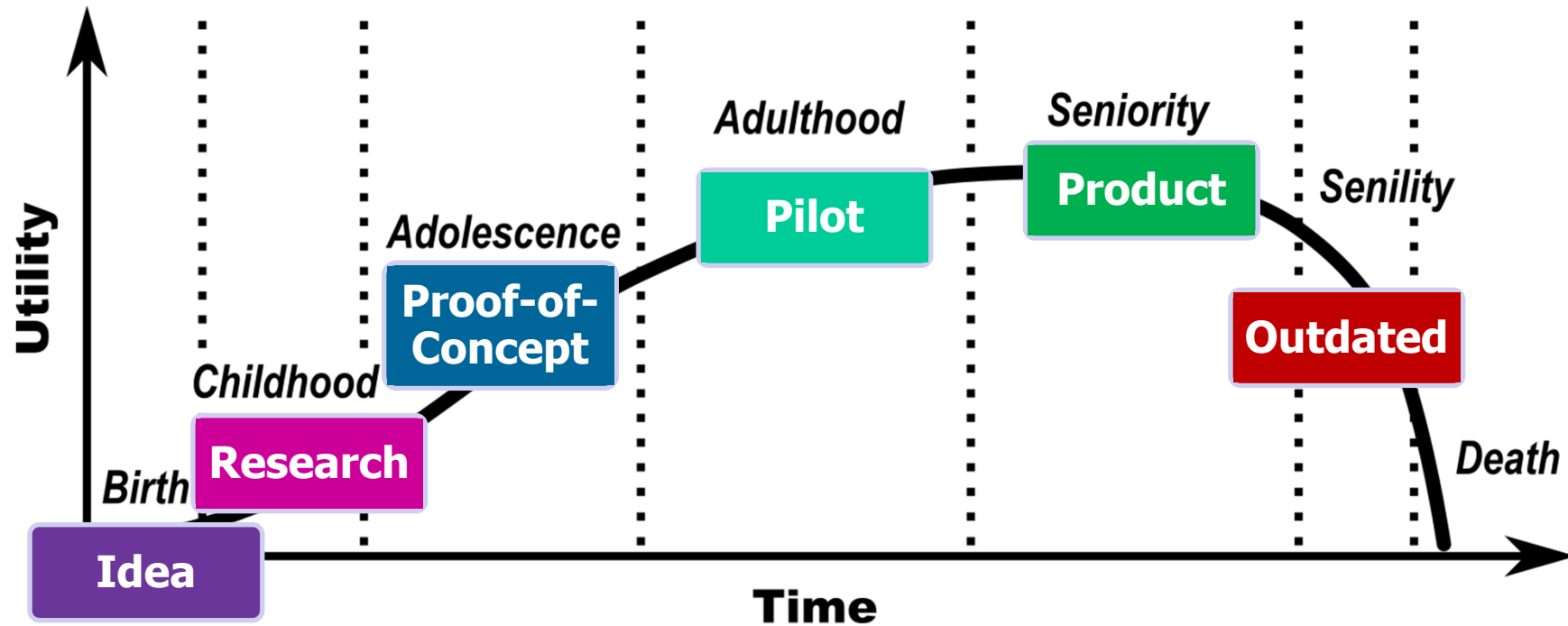


Technology Maturity

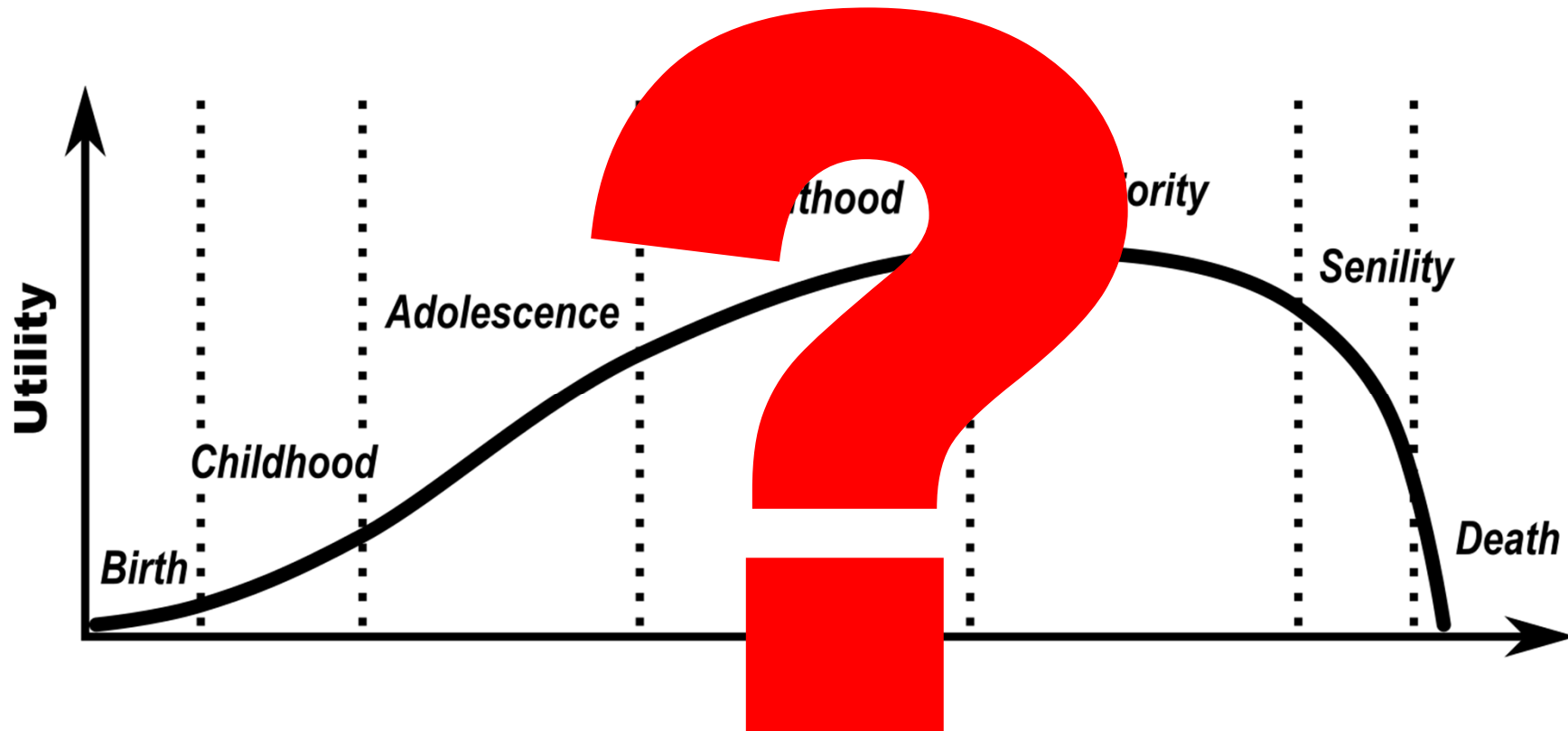


Examples: MD5, Windows XP, ...

PET Maturity: Readiness Scale



PET Maturity: Quality Scale



PET Maturity: Quality Scale



PET Maturity: Quality Scale

Protection:	--	-	0	+	++
Trust Assumptions:	--	-	0	+	++
Side Effects:	--	-	0	+	++
Reliability:	--	-	0	+	++
Performance Efficiency:	--	-	0	+	++
Operability:	--	-	0	+	++
Maintainability:	--	-	0	+	++
Transferability:	--	-	0	+	++
Scope:	--	-	0	+	++
Total Quality:	--	-	0	+	++



PET Maturity Scale: What does Art. 25 GDPR ask for?

--	-	0	+	++
Idea ⁻⁻	Idea ⁻	Idea ⁰	Idea ⁺	Idea ⁺⁺
Research ⁻⁻	Research ⁻	Research ⁰	Research ⁺	Research ⁺⁺
PoC ⁻⁻	PoC ⁻	PoC ⁰	PoC ⁺	PoC ⁺⁺
Pilot ⁻⁻	Pilot ⁻	Pilot ⁰	Pilot ⁺	Pilot ⁺⁺
Product ⁻⁻	Product ⁻	Product ⁰	Product ⁺	Product ⁺⁺
Outdated ⁻⁻	Outdated ⁻	Outdated ⁰	Outdated ⁺	Outdated ⁺⁺

Scope: the entire processing system (not one PET component only)



How does "excellence" count?



Usually compliance only means "good enough" considering the risk

Possible to advance the state of the art

Overview



1. Data protection law and its objectives
2. Enforcement of the GDPR: task of the Data Protection Authorities
3. Art. 25 GDPR: Data Protection by Design & by Default
4. **Status quo & difficulties**
5. Further levers & wishlist
6. Conclusion

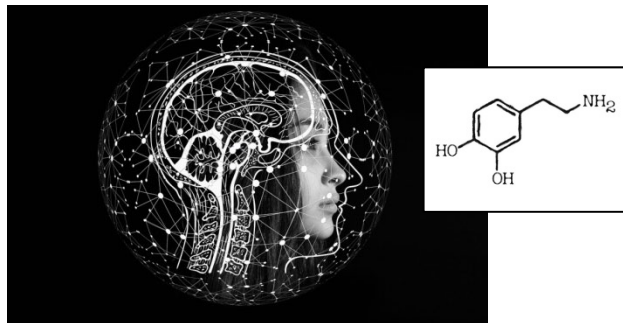


Source: Gerd Altmann via Pixabay

ICT design with data protection?

- “Data protection” as the starting point? (Art. 25 (2) GDPR)
 - Rarely done

- “Addictive Design”



 Source: Gerd Altmann via Pixabay

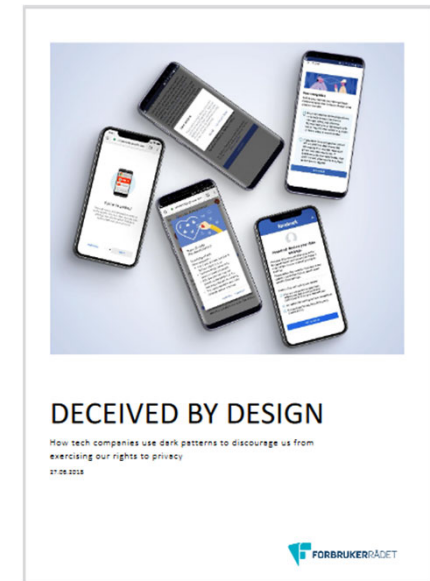
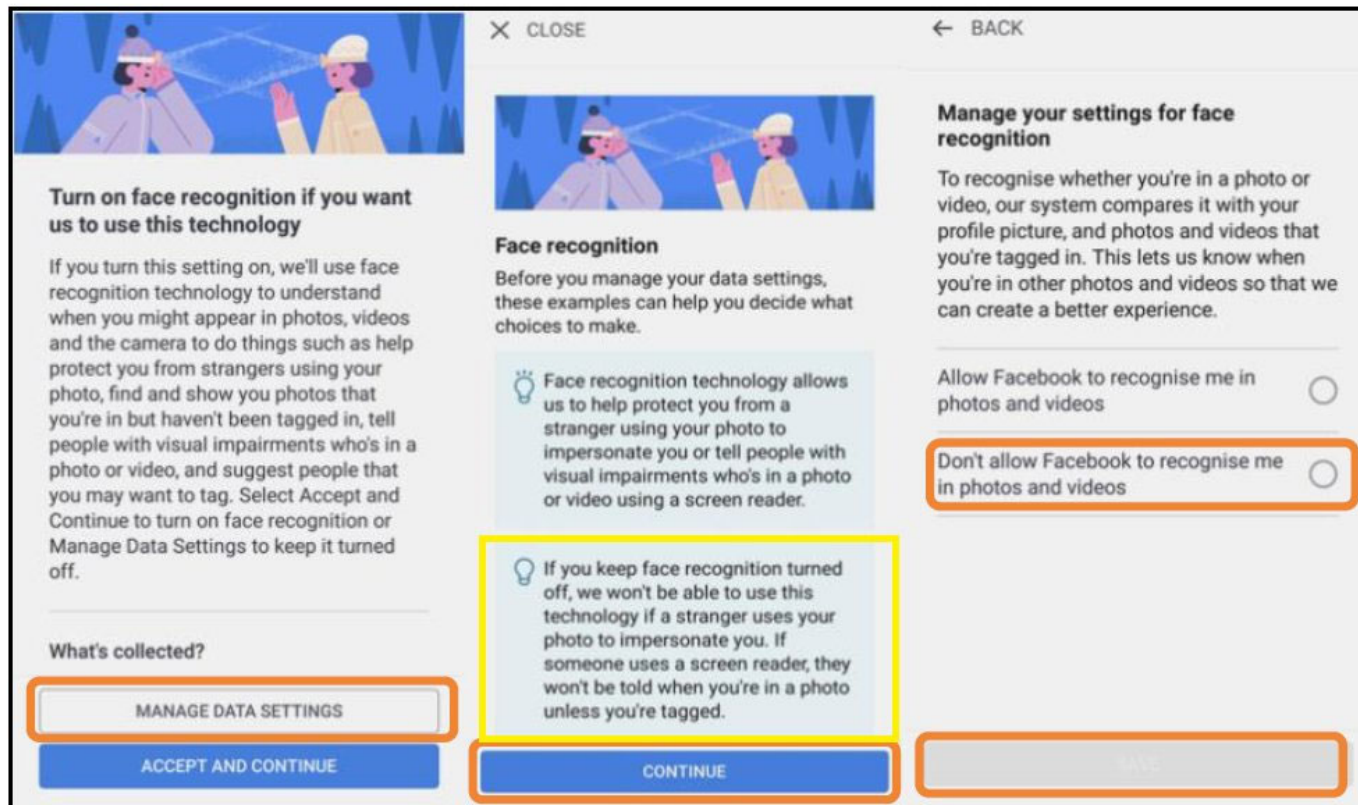


 Source: rawpixel via Pixabay

- “Dark Patterns”

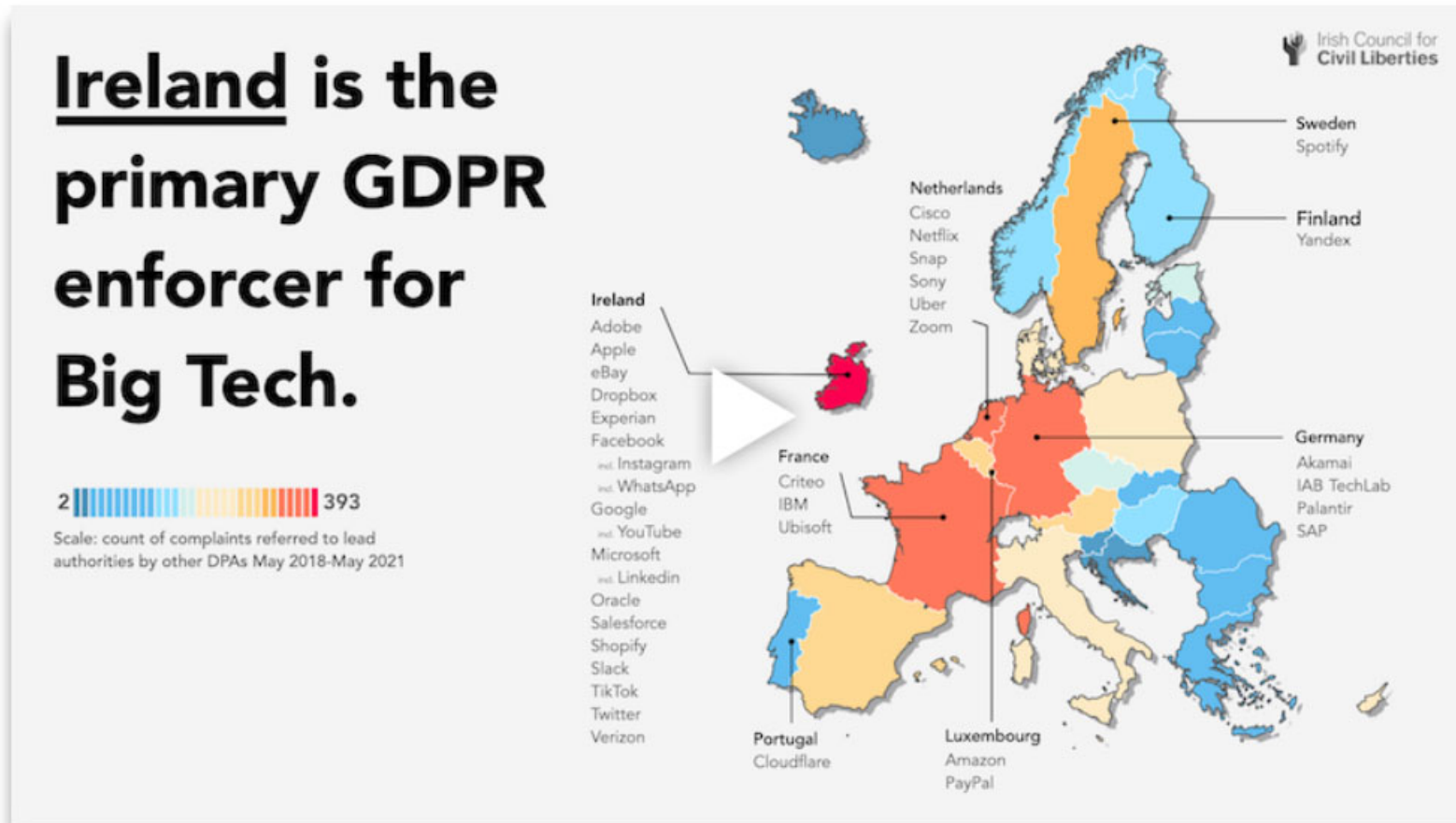
Unfair „Dark Patterns” – Report of Forbrukerrådet

Example: Facebook’s face biometrics configuration



Forbrukerrådet: "Deceived by Design", 2018 (p. 23)
<https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/>

Problems in Enforcement: Big Players



Video: play above, or share from <https://vimeo.com/601138490>.

Problems in Enforcement: Big Players

Too few tech specialist staff to police tech

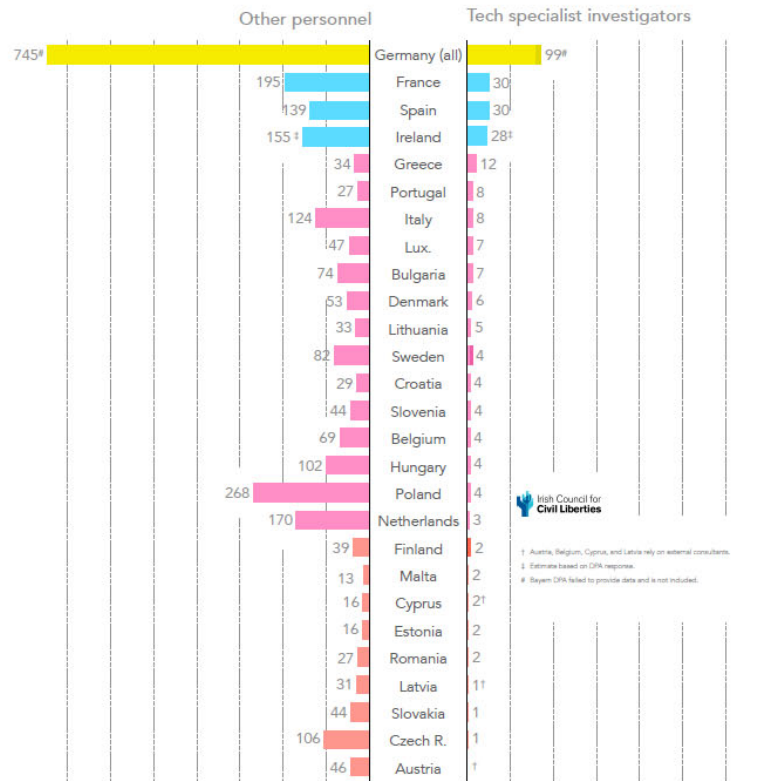
Europe's DPAs are not configured for the digital era, and continue to lack the capacity to investigate and understand what tech companies do with people's data.

The findings

- EU Member State DPAs claim a **combined total of 293 tech specialists**. This number does not include IT support staff.
- **Only 5 EU Member States** have **more than 10** tech specialists, but **more than half (15)** have **only 4 or fewer**.
- The **UK ICO** (not in chart because of Brexit) is the largest single DPA, but **only 13 people** (1.7% of its full time staff) are in its "cyber" investigations team.

Tech specialists at EU data protection authorities

full time equivalents, rounded (vacancies are not counted, but are shown in darker colour)



Big Tech = Infrastructures – which competent authority?



Big Tech: Data hungry business models – "Re-interpretation of the GDPR?"

Example: ECJ case on **Facebook Fanpages**

- More than 10 years, 6 instances
- Decision in 2022 on case from 2011: still valid? How to translate?

Court cases also
for consumer
protection
organisations



Abstract wording in the GDPR needs clarification – building stable pathes



Overview



1. Data protection law and its objectives
2. Enforcement of the GDPR: task of the Data Protection Authorities
3. Art. 25 GDPR: Data Protection by Design & by Default
4. Status quo & difficulties
5. **Further levers & wishlist**
6. Conclusion



Source: Gerd Altmann via Pixabay

Compensation under Art. 82 GDPR

Data breach,
33.200
persons
concerned.


33.200 *
2.500 € =
83.000.000 €

[LG München I, Urteil vom 9. Dezember 2021 – 31 O 16606/20](#), BeckRS 2021, 41707

(Klagewelle wegen Schadensersatz nach Datenschutzverstoß?)

Ergebnis	<input checked="" type="checkbox"/> EUR 2.500
Sachverhalt	Datenabfluss aufgrund eines Datenlecks, u.a. von Konto- und Ausweisdaten, bei einem Finanzdienstleistungsunternehmen.
DSGVO-Verstoß	<input checked="" type="checkbox"/> Verstoß gegen Art. 32 DSGVO (Sicherheit der Verarbeitung), da keine ausreichenden organisatorischen Maßnahmen vorgenommen worden seien, um den Datenabfluss zu verhindern.
Schadensersatz	<input checked="" type="checkbox"/> Bei Einhaltung der Maßstäbe der DSGVO wäre der Schaden, dass dem Kläger u.a. Identitätsmissbrauch droht, vermeidbar gewesen.
Verantwortlichkeit	<input checked="" type="checkbox"/> / — Da die Beklagte selbst keine ausreichenden organisatorischen Maßnahmen vorgenommen habe, ließ das Gericht eine etwaige Zurechnung ähnlicher Unterlassungen bei Drittunternehmen offen.

Structural complaints with Legal Tech initiatives



You HATE cookie banners too?
WE TAKE ACTION!


Reject More options...

noyb aims to end “cookie banner terror” and issues more than 500 GDPR complaints

May 31, 2021

Today, noyb.eu sent over 500 draft complaints to companies who use unlawful cookie banners - making it the largest wave of complaints since the GDPR came into force.

[Read more](#)

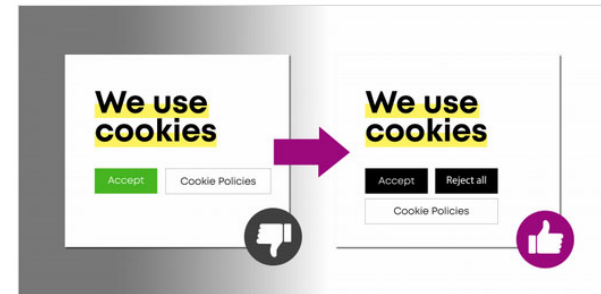


noyb files 422 formal GDPR complaints on nerve-wrecking “Cookie Banners”

Aug 10, 2021

Today we filed 422 + 36 complaints on "cookie banners" with ten European Data Protection Authorities.

[Read more](#)



More Cookie Banners to go: Second wave of complaints underway

Mar 04, 2022

noyb launched the second round of its action against deceptive cookie banners. The first wave already brought visible improvements in banner design.

[Read more](#)

Structural complaints with Legal Tech initiatives



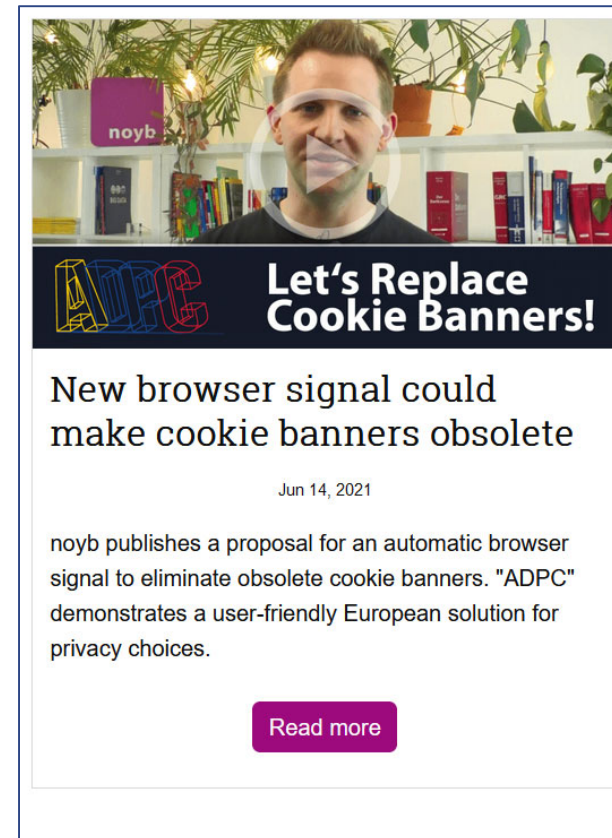
noyb



EN Q ☰

HOME > NATIONAL ADMINISTRATIVE PROCEDURE

National Administrative Procedure

noyb is currently reviewing the national procedures before Data Protection Authorities (DPAs), as they are often fundamentally different (e.g. access to documents, right to apply for certain actions by the DPAs). It is crucial for strategic litigation to ensure that we have a full overview of national procedural options.



Let's Replace Cookie Banners!

New browser signal could make cookie banners obsolete

Jun 14, 2021

noyb publishes a proposal for an automatic browser signal to eliminate obsolete cookie banners. "ADPC" demonstrates a user-friendly European solution for privacy choices.

[Read more](#)

<https://noyb.eu/en/project/national-administrative-procedure>
<https://noyb.eu/en/project/cookie-banners>

*Translating the **GDPR** into practice with data protection by design*



Ad-Hoc Working Group on Data Protection Engineering

Scope

The scope of the work of this ENISA Ad Hoc Working Group (AHWG) on Data Protection Engineering concerns the analysis of available or emerging technologies and techniques on engineering data protection principles (as stipulated by the GDPR) into practise.

My wish list



Researchers and DPAs:

Publish! Communicate!
Advance the state of the art!

- Data protection by design and by default to be demanded by controllers
- Effects on manufacturers
- International enforcement
- Fast track court decisions
- Easy solutions for ~99 % of the cases
- Invest in ...
 - Education
 - Mature alternatives
 - Supportive tools & environments for development
 - Standardisation

Overview



1. Data protection law and its objectives
2. Enforcement of the GDPR: task of the Data Protection Authorities
3. Art. 25 GDPR: Data Protection by Design & by Default
4. Status quo & difficulties
5. Further levers & wishlist
6. **Conclusion**



Source: Gerd Altmann via Pixabay

Conclusion



Source: congerdesign via Pixabay

- The GDPR exists. And **won't go away**.
- DPA investigations currently **driven by individual complaints** – often less structural relevance
- DPA decisions are legally challenged especially by big players → **slowing down** compliance and demotivating role models
- Data protection by design needs **further support**
- Translation of the GDPR needs knowledge about **risks and solutions**

Our joint task: Bridging the gap between technology and (data protection) law



Source: Free-Photos via Pixabay



Looking forward to our Q & A

Further information

- Datatilsynet (Norwegian Data Protection Authority):
Software development with Data Protection by Design and by Default, 28.11.2017,
<https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/>
- Jaap-Henk Hoepman: Privacy Design Strategies (The Little Blue Book), 2018-2019,
<https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf>
- European Data Protection Board: Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, 20.10.2020,
https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en
- Standard Data Protection Model: A method for Data Protection advising and controlling on the basis of uniform protection goals, 2020 (last revision: V 2.0b),
https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V2.0b.pdf
- European Union Agency for Cybersecurity (ENISA) on Data Protection:
<https://www.enisa.europa.eu/topics/data-protection>