Training of Lawyers on European Data Protection Law 2 (TRADATA 2)

Dimitris Anastasopoulos

The EU Directive 2016/80, its implementation thus far and its incorporation into Greek law

Warsaw, 17 February 2023

The project is co-financed with the support of the European Union's Justice programme

I. Introduction to the Directive (EU) 2016/80

DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016

"on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA"

FA LAWYERS

Why do we need a separate legal framework from the GDPR for the processing of data by police and judicial authorities?

FA LAWYERS

Point 3 of the explanatory memorandum: *"Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows personal data to be processed on an unprecedented scale in order to pursue activities such as the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.*"

Recital 4 of the explanatory memorandum: "*The free flow of personal data between competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security within the Union and the transfer of such personal data to third countries and international organisations, should be facilitated while ensuring a high level of protection of personal data. Those developments require the building of a strong and more coherent framework for the protection of personal data in the Union, backed by strong enforcement.".*

LAWYERS

Legal regime prior to the adoption of the Directive:

→ ***Framework Decision 2008/977/JHA***

- processing of personal data by police and judicial authorities
- explicitly repealed by Article 59 of the Directive

Why was this legal framework established through the adoption of an EU Directive instead of an EU Regulation?

FA LAWYERS

→ The competent institutions took into account that each Member State has different legal traditions and functions at the level of police and judicial authorities

Point 11 of the explanatory memorandum: *"It is therefore appropriate for those fields to be addressed by a directive that lays down the specific rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, respecting the specific nature of those activities. [...]".*

II. The main provisions of Directive EE2016/80

1st Chapter

Scope of application

- The activities of European organizations are not covered by the Directive.
- The Directive does not apply to the processing of personal data in the context of an activity which falls outside the scope of Union law.
- Activities relating to national security do not fall under the scope of Union law.
- Member States have legislative flexibility in the sensitive issue of national security.
- There is no clear distinction between public security and national security.

LAWYERS

Key definitions of the Directive – Article 3

(1) ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

(2) ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(6) ‘filing system’ means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.

(7) **‘competent authority’** means:

(a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or

(b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

<u>The definition of 'competent authority' encompasses:</u>

- Police
- Judicial authorities
- Other public authorities that undertake preliminary investigations

2nd Chapter

General principles of data processing

- ***(Art. 4)*** The fundamental principles of data minimization, purpose limitation, lawfulness, transparency, accuracy, integrity and confidentiality of the GDPR are reiterated in Art. 4 of the Directive.
- ***(Art. 5)*** Establishment of appropriate time limits for data erasure and storage.
- ***(Art.6)*** Distinction between different categories of data subject.
- ***(Art. 7)*** Distinction between personal data and verification of quality of personal data.
- ***(Art. 8)*** Lawfulness of processing.
- ***(Art. 9)*** Establishment of specific processing conditions.
- ***(Art. 10)*** Processing of special categories of personal data.

LAWYERS

Automated individual decision-making

1. Member States shall provide for a decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, to be prohibited unless authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller.

2. Decisions referred to in paragraph 1 of this Article shall not be based on special categories of personal data referred to in Article 10, unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

3. Profiling that results in discrimination against natural persons on the basis of special categories of personal data referred to in Article 10 shall be prohibited, in accordance with Union law.

3rd Chapter
Rights of the data subject

- ***(Art. 12)*** Communication and modalities for exercising the rights of the data subject

→ *The Directive provides that Member States should facilitate the exercise of rights by citizens without imposing bureaucratic difficulties and financial costs on them, by providing them with information in simple and comprehensible language so that they can effectively exercise the rights provided for.*

- ***(Art. 13)*** Information to be made available or given to the data subject

→ *It provides, inter alia, that information should be given on the identity and contact details of the controller, the contact details of the data protection officer, where applicable, the purposes of the processing for which the personal data are intended, the right to lodge a complaint with a supervisory authority and the contact details of the supervisory authority.*

LAWYERS

- ***(Art. 14)*** Right of access by the data subject
- ***(Art. 15)*** Limitations to the right of access
- ***(Art. 16)*** Right to rectification or erasure of personal data and restriction of processing
- ***(Art. 17)*** Exercise of rights by the data subject and verification by the supervisory authority

→ Article 17 provides that in cases where the rights of information, access, rectification or erasure of personal data of the data subjects are limited or not met, the data subject may apply to the Supervisory Authority, provided for in Article 41. This arrangement introduces an additional safeguard to ensure that competent authorities do not act arbitrarily when processing data subjects' data and are subject to the necessary control.

- ***(Art. 18)*** Rights of the data subject in criminal investigations and proceedings

LAWYERS

Remaining Chapters

Obligations of data controllers and data processors

- Data controllers under the Directive must implement appropriate technical and organizational measures, taking into account the nature and purpose of the processing they carry out and the risks to the rights and freedoms of data subjects arising from such processing.

- Competent authorities are obliged to apply the principles of data protection by design and by default.

- Triple supervision mechanism in the process of processing of personal data by the competent authorities:
  - DPO
  - Independent Supervisory Authorities
  - European Data Protection Board

LAWYERS

III. Incorporation of the Directive in the national laws of Member States

- The incorporation of the Directive into the national laws of the Member States is significantly delayed.

- The Commission is also required to ensure that the Directive has been adequately transposed.

- In its first report on the implementation and functioning of the Data Protection Directive in the context of law enforcement (EU) 2016/680 dated July 2022, the Commission found the implementation of the Directive satisfactory.

- Thus far the Commission has taken legal action against Spain, Germany and Greece.

IV. Jurisprudence of the ECJ

1. *WS v Bundesrepublik Deutschland, C-505/19, EU:C:2021:376*

The Court did not rule out the lawfulness of the processing of personal data contained in a red alert issued by Interpol until it is established, by a final judicial decision, that the *ne bis in idem* principle applies to the acts on which that alert is based. The Court concluded with this judgment, reasoning *inter alia* that *"In particular, on the one hand, the transmission of the data in question by Interpol does not constitute processing of personal data falling within the scope of Directive 2016/680, since that body is not a 'competent authority' within the meaning of Article 3(7) of that directive"*, while on another point it held that *"It must, however, be recalled that, where it has been established, by means of a final judgment delivered in a Contracting State or in a Member State, that a red notice issued by Interpol in fact relates to the same acts as those for which the person concerned by that notice has already been finally judged and that, consequently, the principle of ne bis in idem applies, that person (. .) can no longer be prosecuted for the same acts and, consequently, can no longer be arrested in the Member States for those acts."*.

AA LAWYERS

2. B v Latvijas Republikas Saeima, C-439/19, EU:C:2021:504

The Court interpreted "competent authority" by excluding the Latvian Road Safety Directorate from the concept of competent authority under Article 3(7) of the Directive. Furthermore, in that judgment the Court set out the following criteria for the classification of an infringement as a criminal offence: (1) whether the infringement is classified as a criminal offence under national law; (2) the nature of the infringement itself; and (3) the degree of severity of the sanction which is threatened against the person concerned.

3. ECJ C-205/21

The Court of Justice has, *inter alia*, interpreted Article 10 of the Directive by providing, that the processing of biometric and genetic data by police authorities in the course of their investigative activities for the purposes of combating crime and maintaining public order is permitted under the law of a Member State within the meaning of Article 10(a) of the Directive where the law of the Member State provides for a sufficiently clear and precise legal basis for the processing of biometric and genetic data.
Furthermore, the Court of Justice has interpreted Article 6 in that regard, stating that said provision does not preclude national legislation which provides that, where a person accused of intentionally committing an offence which is prosecuted ex officio refuses to cooperate voluntarily in the collection of biometric and genetic data relating to him or her for the purpose of recording them, the competent criminal court is obliged to order the compulsory collection of that data, without having the power to assess whether there are serious grounds for considering that the data subject has committed the offence of which he is accused, provided that national law subsequently ensures effective judicial control of the conditions on which the accusation on the basis of which the authorization to collect the data was granted was based.

LAWYERS

However, the Court of Justice, making a combined assessment of Articles 10, 4(1)(a)-(c) and 8(1) and 2 of the Directive, held that those rules preclude national legislation which provides for the systematic collection of biometric and genetic data from any person accused of intentionally committing an offence against the law for the purpose of recording them, without providing that the competent authority must establish and demonstrate, first, that such collection is strictly necessary for the fulfilment of the specific purposes pursued and, second, that it is not possible to achieve those purposes by means of a moderate collection of biometric and genetic data.

V. The incorporation of the Directive in Greece

LAWYERS

Greece has not managed to transpose the Directive into its national law in time. The transposition of the Directive was done in 2019 in a single law with the provisions for the transposition of the GDPR into national law, Law 4624/2019. The national law incorporated the Directive for the most part but unfortunately did not fully comply with its provisions. This was also noted by the Commission, which in April 2022 initiated an infringement procedure against our country on the grounds that the national transposition legislation in question does not comply with the Directive.

In December 2022, Greece has largely amended the relevant national law to meet the Commission's criteria, thus offering greater security to data subjects. So far there is no feedback from the Commission's expert team

AA LAWYERS

Concluding Remarks

Thank you very much!

FA LAWYERS

Training of Lawyers on European Data Protection Law 2 (TRADATA 2)

Rights of the data subject, including rights in criminal investigations and proceedings

Giovanni Battista Gallus

Warsaw, 17 February 2023

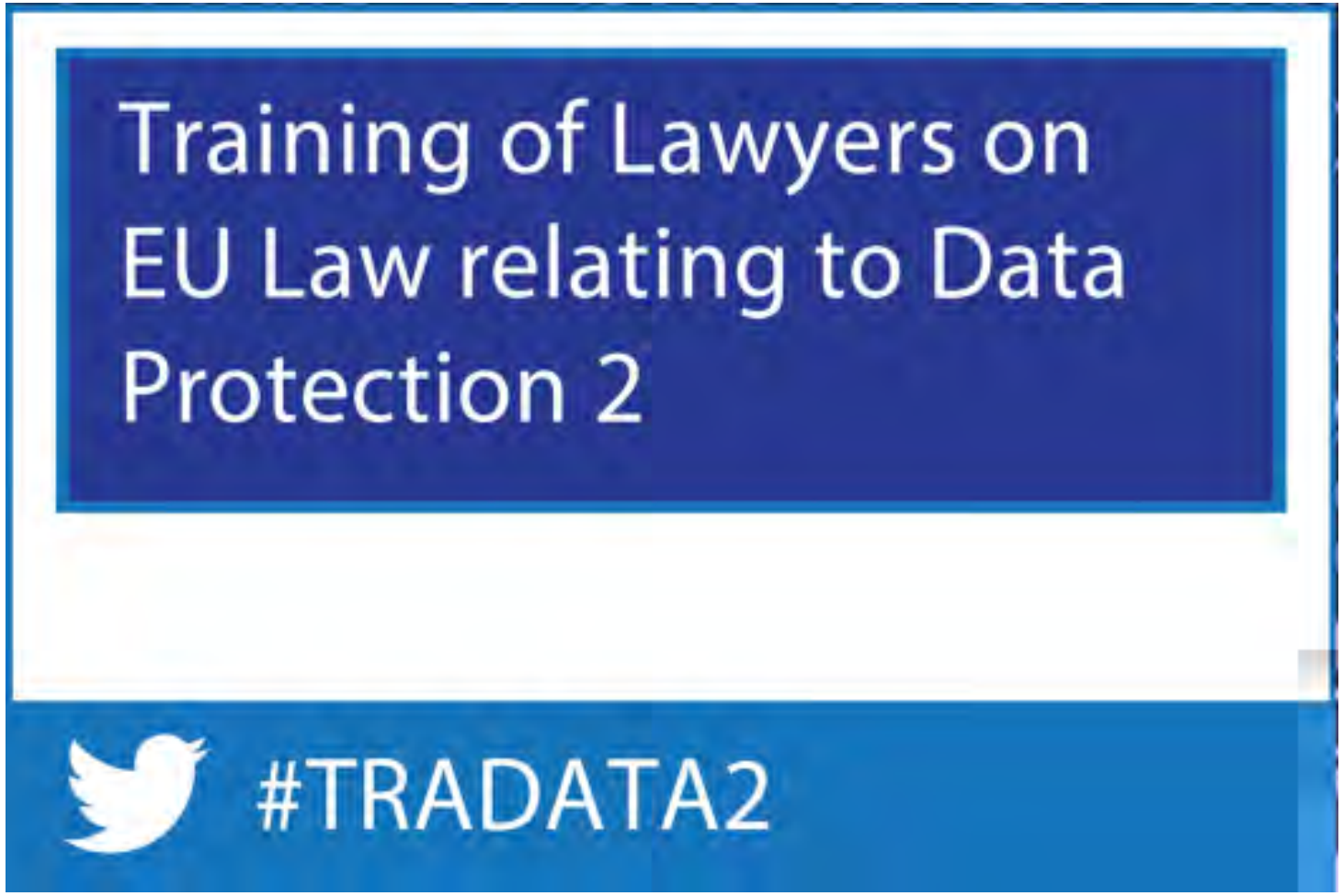
The project is co-financed with the support of the European Union's Justice programme

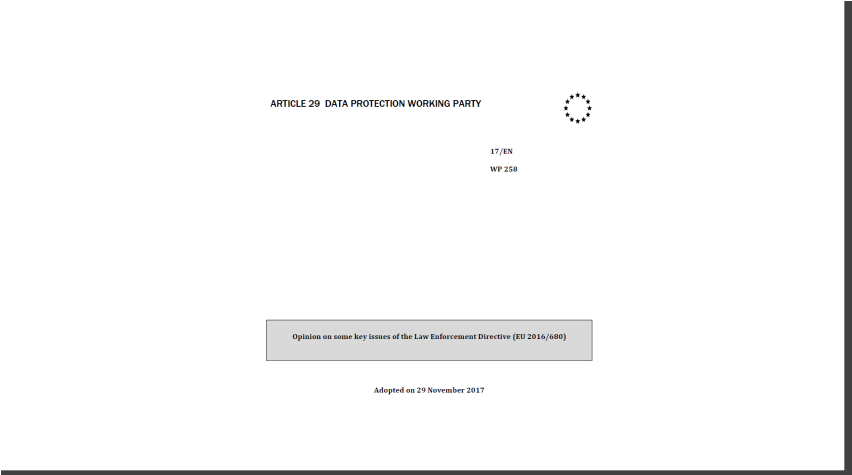
Who am I

- Lawyer - array.eu
- Master of Laws in Maritime Law and Information Technology Law - University College London
- Working group member – Italian Foundation legal Innovation (FIIF
- Member of Surveillance Commission - CCBE (Council of Bars and Law Societies of Europe)
- Fellow of NEXA Center – Polytechnic of Turin
- Advisory Board Member – Drone Observatory on Drones and Advanced Air Mobility – Polytechnic of Milan
- Data protection officer

Main topics

- Data subject rights (DSR) – introduction
- Common principles
- DSR & accountability
- A quick overview of the rights
- Focus on the right of access
- DSR and law enforcement directive
- DSR in the context of the European Data Strategy and the Digital services package




ARTICLE 29 DATA PROTECTION WORKING PARTY

17/EN
WP 258

Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)

Adopted on 29 November 2017

Guidelines 3/2019 on processing of personal data through video devices

Version 2.0

Adopted on 29 January 2020


ARTICLE 29 DATA PROTECTION WORKING PARTY

17/EN

WP260 rev.01

Article 29 Working Party

Guidelines on transparency under Regulation 2016/679

Adopted on 29 November 2017

As last Revised and Adopted on 11 April 2018

Guidelines 01/2022 on data subject rights - Right of access

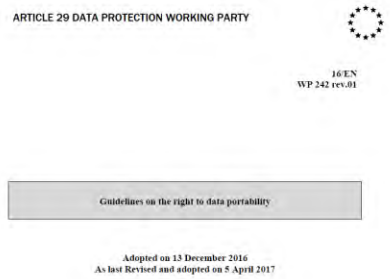
Version 1.0

Adopted on 18 January 2022

Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1)

Version 2.0

Adopted on 7 July 2020


ARTICLE 29 DATA PROTECTION WORKING PARTY

16/EN
WP 242 rev.01

Guidelines on the right to data portability

Adopted on 13 December 2016
As last Revised and adopted on 5 April 2017

Useful guidelines

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

Common principles

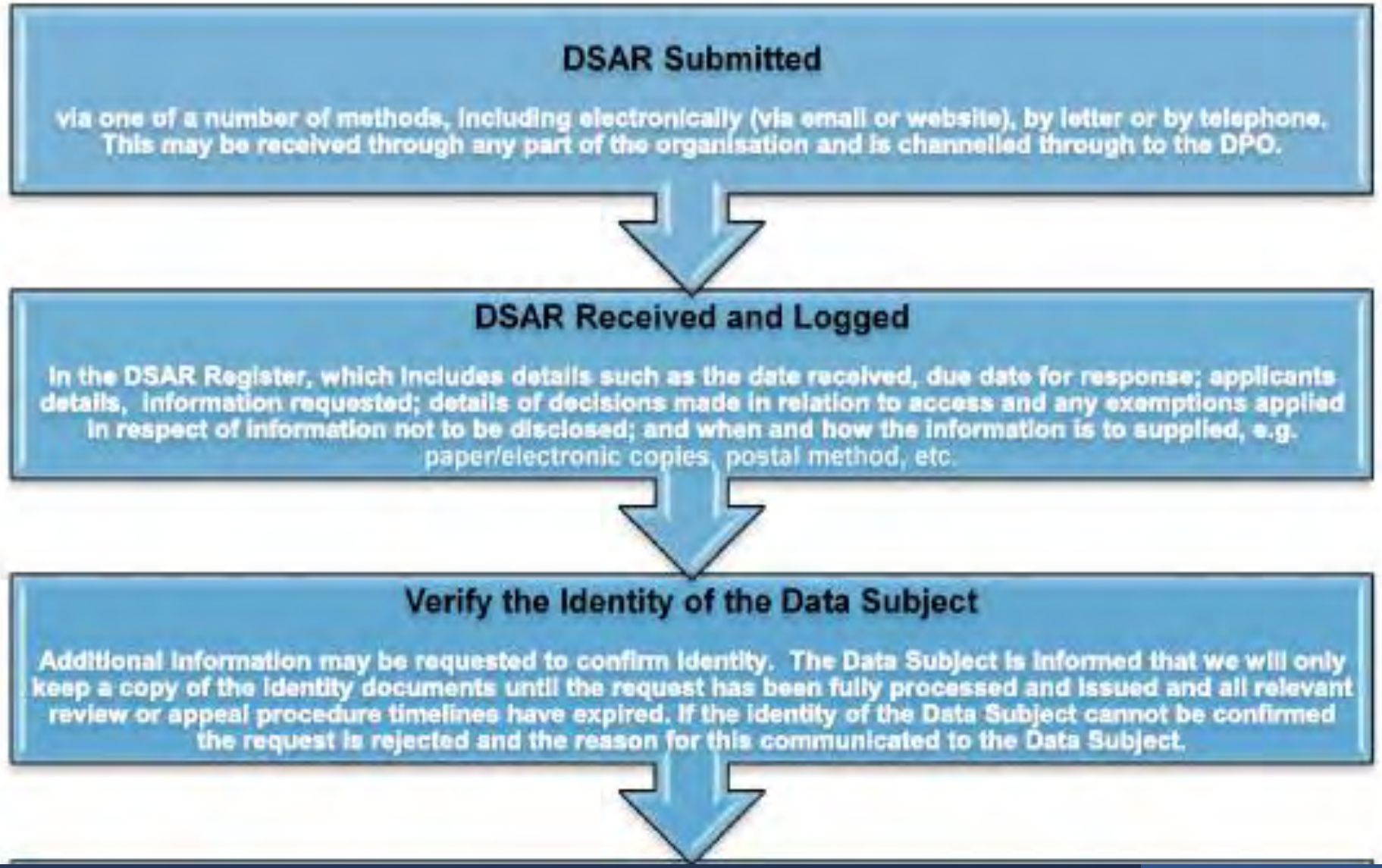
Data Subject rights - definitions

We all know the definition of Personal data…

We all know who the Data subject is…

Training of Lawyers on EU Law relating to Data Protection 2

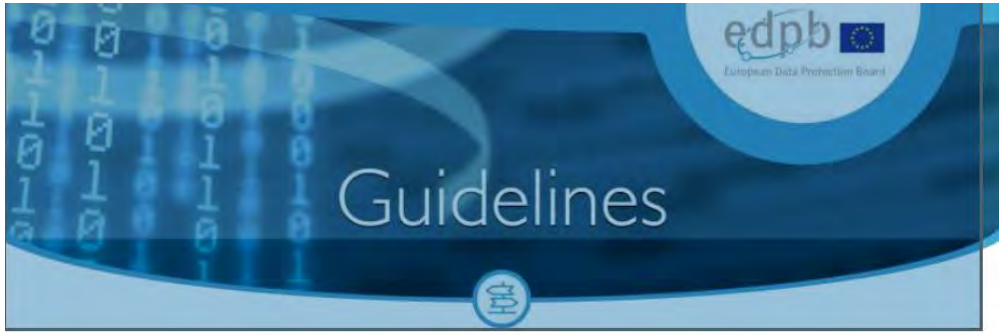
#TRADATA2



Source: **Data Subject Rights Policy Operational Guide for Personnel**
The Adoption Authority of Ireland

Identification?

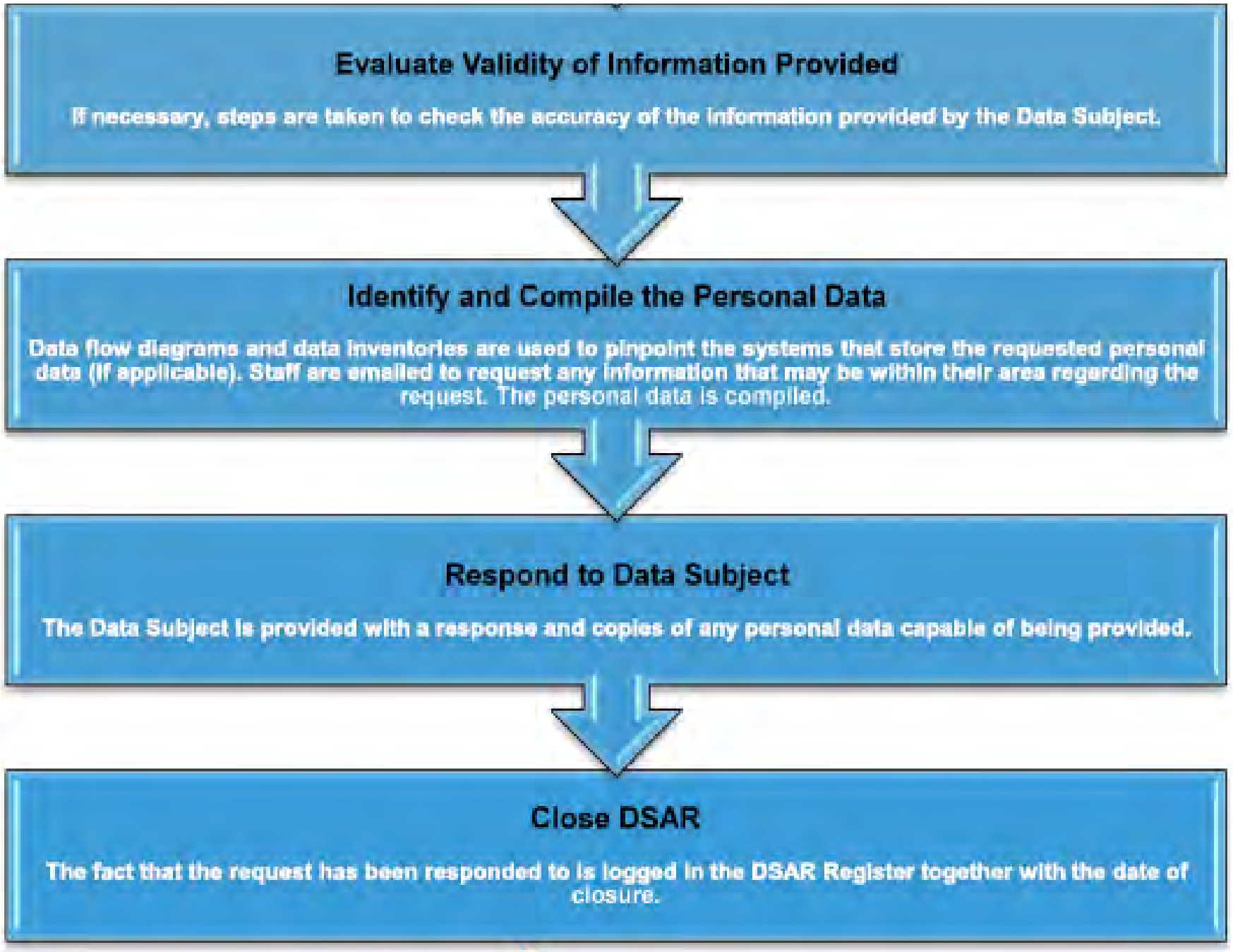
- Need for identification
- if the controller has doubts about whether the data subject is who they claim to be, the controller must request additional information in order to confirm the identity of the data subject. The request for additional information The request for additional information must be proportionate to the type of data processed, the damage that could occur etc. in order to avoid excessive data collection.



Guidelines 01/2022 on data subject rights - Right of access

Version 1.0

Adopted on 18 January 2022



Source: **Data Subject Rights Policy Operational Guide for Personnel The Adoption Authority of Ireland**

Time limit to respond (art. 12)

As soon as possible - one month maximum

It can be extended by two further months where necessary, taking into account the complexity and number of the request

The data subject has to be informed about the reason for the delay

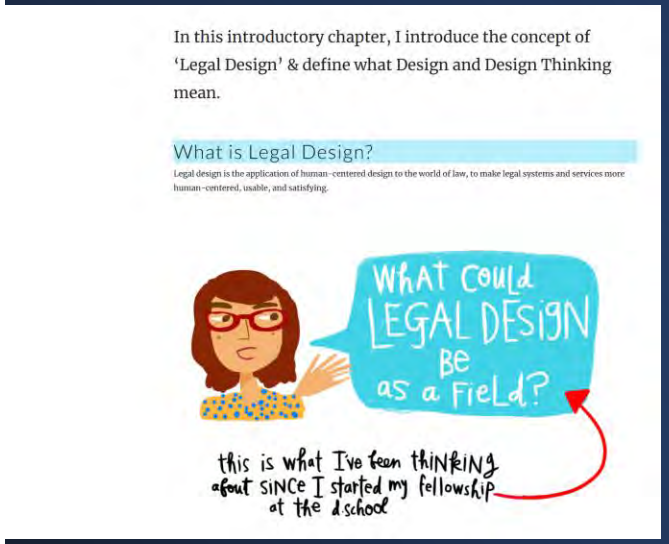
Formalities for the answer (art. 12)

Concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.

In writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally

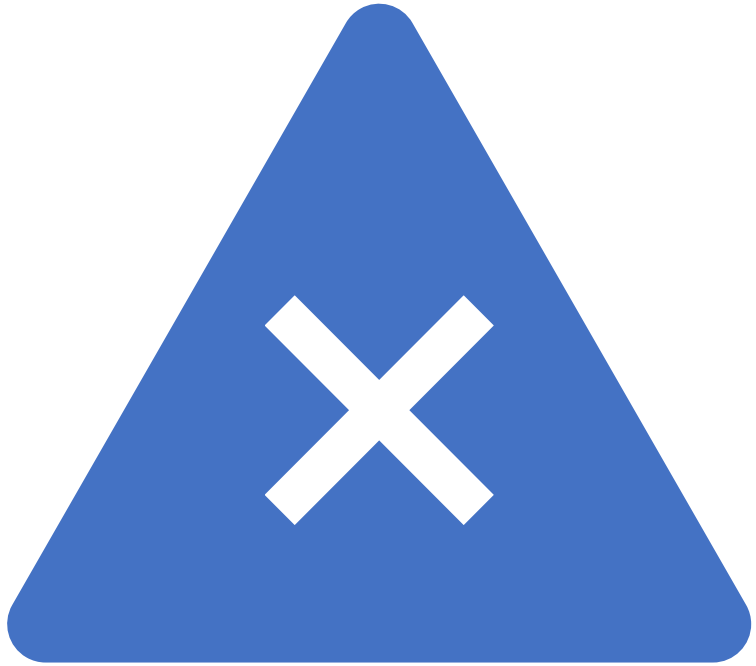
Importance of Legal Design

- Legal design is the application of human-centered design to the world of law, to make legal systems and services more human-centered, usable, and satisfying (M. Hagan)



Can the request be refused (art. 12)?

- Yes, when it is manifestly unfounded or excessive;
- In such cases, a reasonable fee for such requests can be applied instead of the refusal
- These concepts have to be interpreted narrowly
- Burden of proof rests on the controller
- Restrictions may also exist in Member States' national law as (Art. 23 GDPR)



Video surveillance

- Given that any number of data subjects may be recorded in the same sequence of video surveillance a screening would then cause additional processing of personal data of other data subjects. If the data subject wishes to receive a copy of the material (article 15 (3)), this could adversely affect the rights and freedoms of other data subject in the material.
- If the video footage is not searchable for personal data, (i.e. the controller would likely have to go through a large amount of stored material in order to find the data subject in question) the controller may be unable to identify the data subject.
- Guidelines 3/2019

A quick overview of the rights

A quick summary of DSR (from the Handbook on European data protection law)

EU	Issues covered	CoE
Right to be informed		
General Data Protection Regulation, Article 12 CJEU, C-473/12, *Institut professionnel des agents immobiliers (IPI) v. Englebert*, 2013 CJEU, C-201/14, *Smaranda Bara and Others v. Casa Națională de Asigurări de Sănătate and Others*, 2015	Transparency of information	Modernised Convention 108, Article 8
General Data Protection Regulation, Article 13 (1) and (2) and Article 14 (1) and (2)	Content of information	Modernised Convention 108, Article 8 (1)
General Data Protection Regulation, Article 13 (1) and Article 14 (3)	Time of providing information	Modernised Convention 108, Article 9 (1) (b).
General Data Protection Regulation, Article 12 (1), (5) and (7)	Means of providing information	Modernised Convention 108, Article 9 (1) (b).
General Data Protection Regulation, Article 13 (2) (d) and Article 14 (2) (e), Articles 77, 78 and 79	Right to lodge a complaint	Modernised Convention 108, Article 9 (1) (f)

A quick summary of DSR (from the Handbook on European data protection law)

EU	Issues covered	CoE
Right of access		
General Data Protection Regulation, Article 15 (1) CJEU, C-553/07, *College van burgemeester en wethouders van*	Right of access to one's own data	Modernised Convention 108, Article 9 (1) (b) ECtHR, *Leander*
CJEU, Joined cases C-141/12 and C-372/12, *YS v. Minister voor Immigratie, Integratie en Asiel* and *Minister voor Immigratie, Integratie en Asiel v. M and S*, 2014 CJEU, C-434/16, *Peter Nowak v. Data Protection Commissioner*, 2017		
Right to rectification		
General Data Protection Regulation, Article 16	Rectification of inaccurate personal data	Modernised Convention 108, Article 9 (1) (e) ECtHR, *Cemalettin Canli v. Turkey*, No. 22427/04, 2008 ECtHR, *Ciubotaru v. Moldova*, No. 27138/04, 2010

A quick summary of DSR (from the Handbook on European data protection law)

Right to rectification		
General Data Protection Regulation, Article 16	Rectification of inaccurate personal data	Modernised Convention 108, Article 9 (1) (e) ECtHR, *Cemalettin Canli v. Turkey*, No. 22427/04, 2008 ECtHR, *Ciubotaru v. Moldova*, No. 27138/04, 2010
Right to erasure		
General Data Protection Regulation, Article 17 (1)	The erasure of personal data	Modernised Convention 108, Article 9 (1) (e) ECtHR, *Segerstedt-Wiberg and Others v. Sweden*, No. 62332/00, 2006
CJEU, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014 CJEU, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, 2017	The right to be forgotten	

A quick summary of DSR (from the Handbook on European data protection law)

Right to restriction of processing		
General Data Protection Regulation, Article 18 (1)	Right to restrict use of personal data	
General Data Protection Regulation, Article 19	Notification obligation	
Right to data portability		
General Data Protection Regulation, Article 20	Right to data portability	
Right to object		
General Data Protection Regulation, Article 21 (1) CJEU, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, 2017	Right to object due to the data subject's particular situation	Profiling Recommendation, Article 5.3 Modernised Convention 108, Article 9 (1) (d)

A quick summary of DSR (from the Handbook on European data protection law)

EU	Issues covered	CoE
General Data Protection Regulation, Article 21 (2)	Right to object to use of data for marketing purposes	Direct Marketing Recommendation, Article 4.1
General Data Protection Regulation, Article 21 (5)	Right to object by automated means	
Rights related to automated decision-making and profiling		
General Data Protection Regulation, Article 22	Rights related to automated decision-making and profiling	Modernised Convention 108, Article 9 (1) (a)
General Data Protection Regulation, Article 21	Rights to object automated decision-making	
General Data Protection Regulation, Article 13 (2) (f)	Rights to a meaningful explanation	Modernised Convention 108, Article 9 (1) (c)

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

Let's not forget data breaches

- Right to be informed in the event of a data breach, if the breach is likely to result in a high risk to the rights and freedoms of natural persons

DSR & accountability

Training of Lawyers on EU Law relating to Data Protection 2

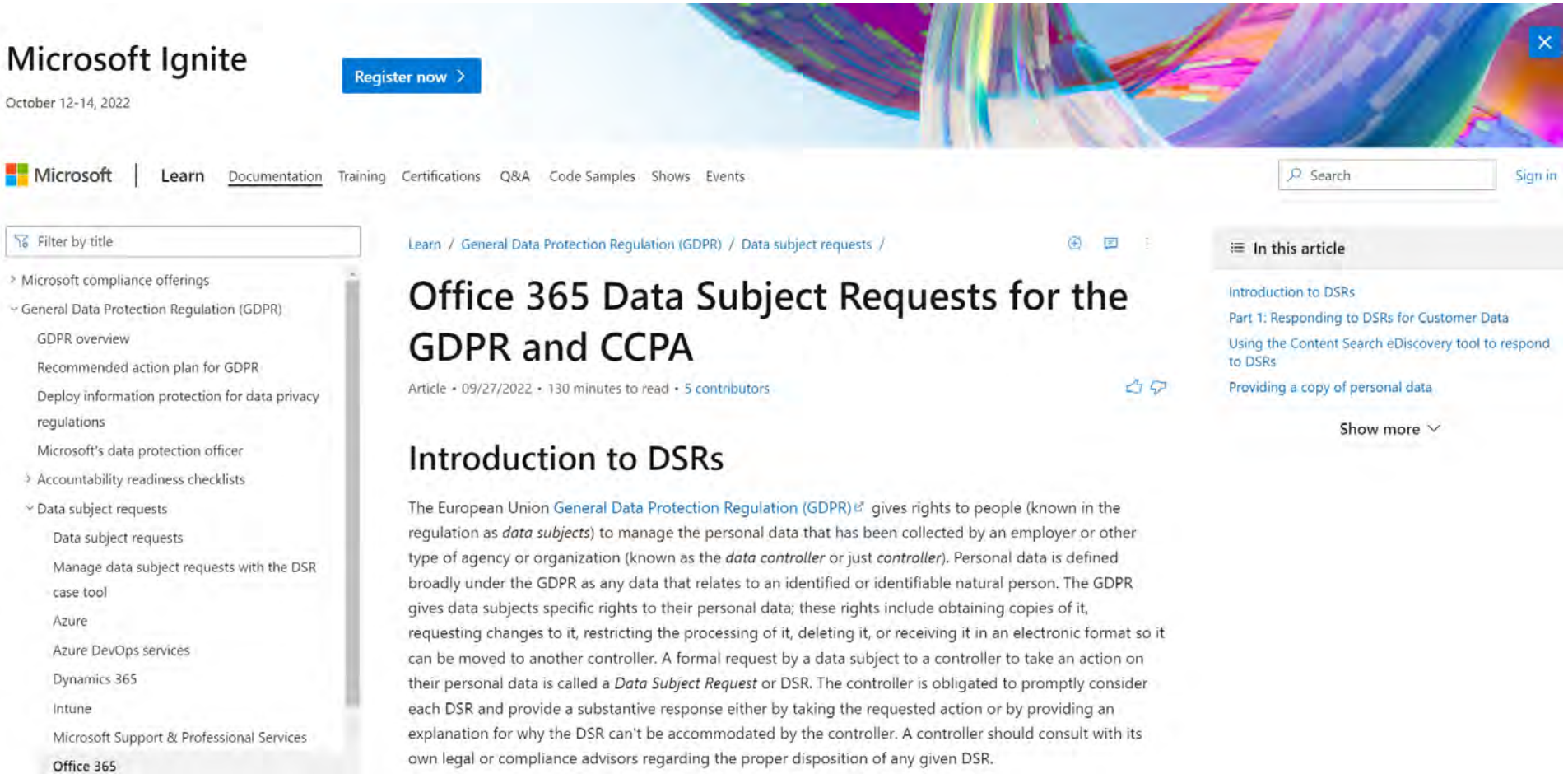
#TRADATA2

DSR & accountability

- A question:
- What are the accountability measures to be taken for compliance with DSRs?

DSR and accountability

ICT systems able to respond quickly to DSRs (access, portability, erasure etc…) – art. 25



Adequate DSR policies (art. 24)

DSR and accountability

Data Subject Rights Policy

Operational Guide for Personnel

The Adoption Authority of Ireland

ÚDARÁS UCHTÁLA na hÉIREANN
THE ADOPTION AUTHORITY of IRELAND

Revision and Approval History					
Version	Revised By	Revision Date	Approved By	Approval Date	Comments
Draft	DPO	9/4/2019			
Reviewed	DPO	22/01/2020			
Reviewed	Matheson	19/10/2020			
Reviewed	DPO	28/01/2021			
Reviewed	DPO	1/04/2021			
Approved	Board	April 2021			

DSR and accountability

- Regulation of DSR requests in Data protection agreements (art. 28) & joint controller agreements (art. 26)
- Instructions and training for any person acting under the authority of the controller or of the processor who processes personal data
- …

Focus on the right of access

The right of access

enshrined in Art. 8 of the EU Charter of Fundamental Rights.

Part of the European data protection legal framework since its beginning

Further developed by more specified and precise rules in Art. 15 GDPR.

Guidelines 01/2022 on data subject rights - Right of access

Version 1.0

Adopted on 18 January 2022

The right of access under the GDPR vs other access rights

Access to public documentation

FOIA requests

Does the request need a specific format?

- Controller must provide appropriate and user-friendly channels
- the data subject is not required to use these specific channels and may instead send the request to an official contact point of the controller
- No need for motivation

Employees' right of access: Italian SA fines Unicredit S.p.A. and orders corrective measures

20 September 2022 Italy

Background information

- Date of final decision: 16 June 2022
- Controller: Unicredit S.p.A
- Legal Reference: transparency and fairness of processing (Article 5.1(a)), transparency in and arrangements for exercise of DSR (Art.12), right of access (Art.15)
- Decision: the Italian SA imposed an EUR 70,000 administrative fine and ordered the controller to grant the access request by the data subject
- Key words: processing of data in the employment sector, right of access to one's personal data, transparency and fairness of processing

Summary of the Decision

Latest news

Third fine imposed by Polish SA on the Surveyor General of Poland for failure to notify the personal data breach
23 September 2022 Poland

Employees' right of access: Italian SA fines Unicredit S.p.A. and orders corrective measures
20 September 2022 Italy

September plenary - adopted documents
20 September 2022 EDPB

New EDPB opinion on certification criteria

The right of access – overall aim

Provide individuals with sufficient, transparent and easily accessible information about the processing of their personal data so that they can be aware of and verify the lawfulness of the processing and the accuracy of the processed data.

Will facilitate the exercise of other rights such as the right to erasure or rectification.

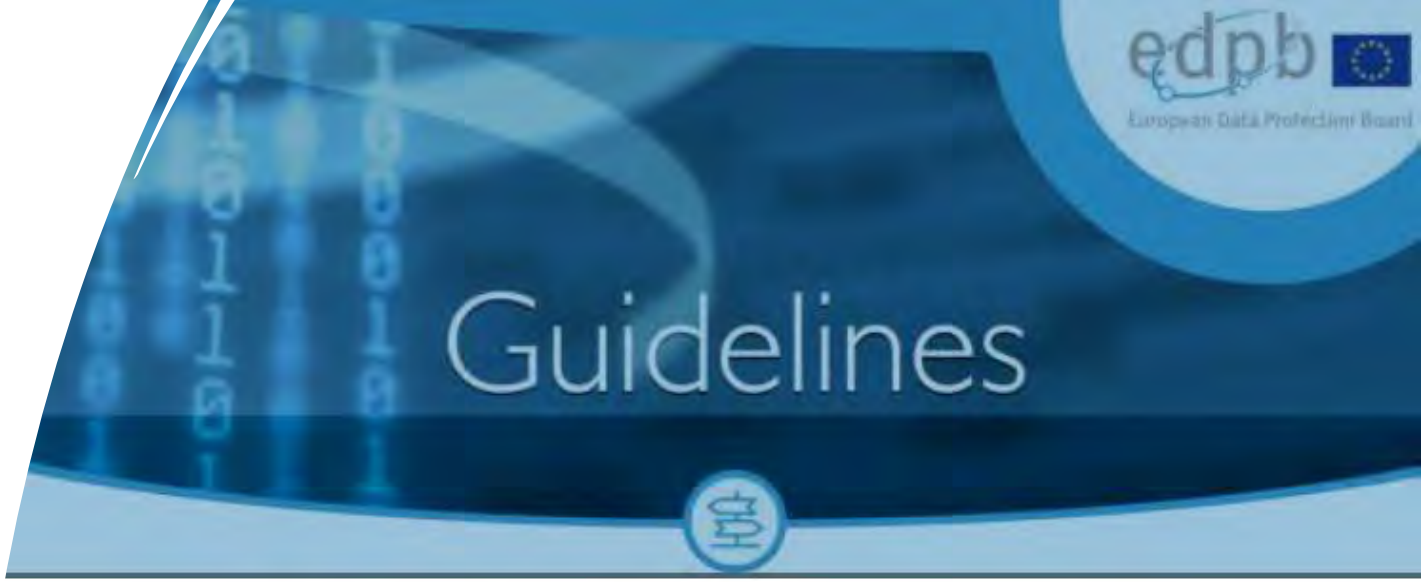
The right of access

three different components:

Confirmation as to whether data about the person is processed or not,

Access to this personal data and

Access to information about the processing, such as purpose, categories of data and recipients, duration of the processing, data subjects' rights and appropriate safeguards in case of third country transfers



Does the data subject has the right to know the specific identity of the recipients? ECJ, case 154/21

- By its question, the referring court asks, in essence, whether Article 15(1)(c) of the GDPR must be interpreted as meaning that the data subject's right of access to personal data concerning him or her, provided for by that provision, entails, where those data have been or will be disclosed to recipients, an obligation on the part of the controller to provide the data subject with the specific identity of those recipients.
- Recital 63 of that regulation states that the data subject is to have the right to know and obtain communication in particular with regard to the recipients of the personal data and does not state that that right may be restricted solely to categories of recipients
- Data controllers must comply with the principle of transparency
- Article 15 of the GDPR lays down a genuine right of access for the data subject, with the result that the d**ata subject must have the option of obtaining either information about the specific recipients to whom the data have been or will be disclosed, where possible, or information about the categories of recipient.**
- **The right of access is necessary to enable the data subjects to exercise the other rights (erasure, rectification etc.)**

InfoCuria
Giurisprudenza

italiano (it)

Pagina iniziale > Formulario di ricerca > Elenco dei risultati > Documenti

Lingua del documento : inglese ECLI:EU:C:2023:3

Avvia la stampa

Provisional text

JUDGMENT OF THE COURT (First Chamber)

12 January 2023 (*)

(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Article 15(1)(c) – Data subject's right of access to his or her data – Information about the recipients or categories of recipient to whom the personal data have been or will be disclosed – Restrictions)

In Case C-154/21,

REQUEST for a preliminary ruling under Article 267 TFEU from the Oberster Gerichtshof (Supreme Court, Austria), made by decision of 18 February 2021, received at the Court on 9 March 2021, in the proceedings

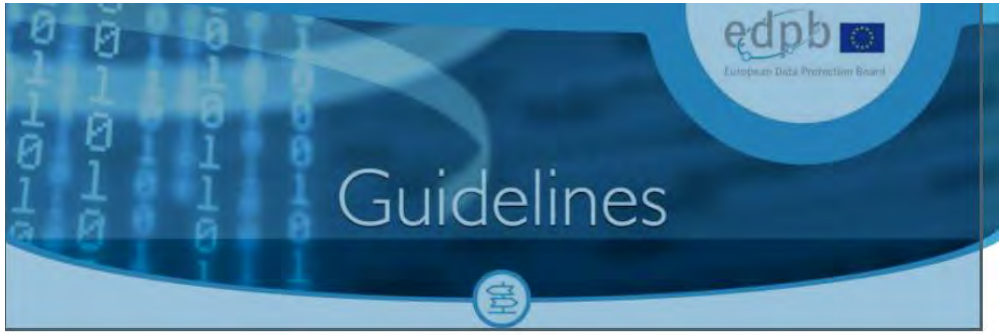
RW

Does the data subject has the right to know the specific identity of the recipients? ECJ, case 154/21

- Article 15(1)(c) of the GDPR must be interpreted as meaning that the data subject's right of access to personal data concerning him or her, provided for by that provision, entails, where those data have been or will be disclosed to recipients, **an obligation on the part of the controller to provide the data subject with the actual identity of those recipients**, unless it is impossible to identify those recipients or the controller demonstrates that the data subject's requests for access are manifestly unfounded or excessive within the meaning of Article 12(5) of the GDPR, in which cases the controller may indicate to the data subject only the categories of recipient in question.

Access to information about the processing vs transparency obligations of art. 13-14 GDPR

- Any information on the processing available to the controller may therefore have to be updated and tailored for the processing operations actually carried out with regard to the data subject making the request. Thus, referring to the wording of its privacy policy would not be a sufficient way for the controller to give information required by Art. 15(1)(a) to (h) and (2) unless the « tailored » information is the same as the « general » information.



Guidelines 01/2022 on data subject rights - Right of access

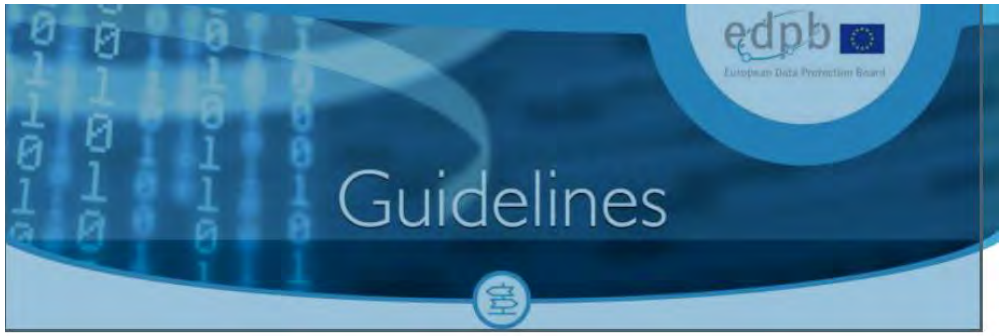
Version 1.0

Adopted on 18 January 2022

Which data?

- Unless explicitly stated otherwise, the request should be understood as referring to **all personal data concerning the data subject** and the controller may ask the data subject to specify the request if they process a large amount of data

- The communication of data and other information about the processing must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language
- Layered approach



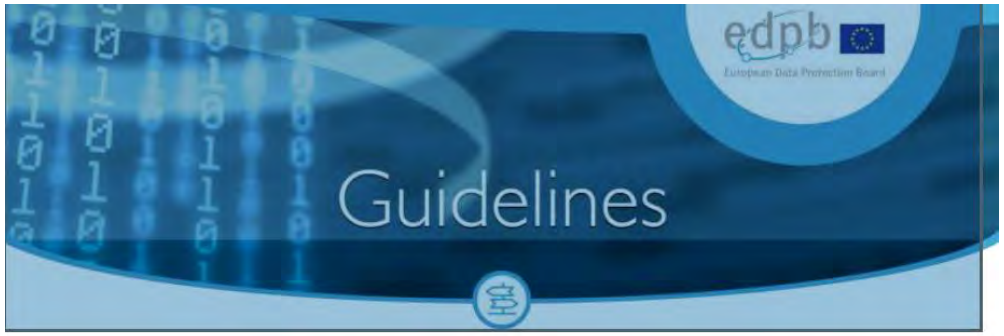
Guidelines 01/2022 on data subject rights - Right of access

Version 1.0

Adopted on 18 January 2022

Does it include inferred data?

- Data inferred from other data, rather than directly provided by the data subject (e.g. to assign a credit score or comply with anti-money laundering rules, algorithmic results, results of a health assessment or a personalization or recommendation process
- the right of access includes both inferred and derived data, including personal data created by a service provider, whereas the right to data portability only includes data provided by the data subject.
- Therefore, in case of an access request and unlike a data portability request, the data subject should be provided not only with personal data provided to the controller to make a subsequent analysis or assessment about these data but also with the result of any such subsequent analysis or assessment.



Guidelines 01/2022 on data subject rights - Right of access

Version 1.0

Adopted on 18 January 2022

OPINION OF ADVOCATE GENERAL
PITRUZZELLA
delivered on 15 December 2022(1)

Case C-487/21

F.F.
interested parties:
Österreichische Datenschutzbehörde,
CRIF GmbH

(Request for a preliminary ruling lodged by the Bundesverwaltungsgericht (Federal Administrative Court, Austria))

›reliminary ruling – Protection of personal data – Regulation (EU) 2016/679 – Article 15(3) – Right of access by the data subject to personal data undergoing processing – Right to receive a copy of personal data – (Concept of 'information')

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

The exact boundaries of the right to obtain a copy according to the Advocate general (Case C-487/21)

- the concept of 'copy' referred to in that provision must be understood as a faithful reproduction in intelligible form of the personal data requested by the data subject, in material and permanent form, that enables the data subject effectively to exercise his or her right of access to his or her personal data in full knowledge of all his or her personal data that undergo processing – including any further data that might be generated as a result of the processing, if those also undergo processing – in order to be able to verify their accuracy and to enable him or her to satisfy himself or herself as to the fairness and lawfulness of the processing so as to be able, where appropriate, to exercise further rights conferred on him or her by the GDPR; the exact form of the copy is determined by the specific circumstances of each case and, in particular, the type of personal data in respect of which access is requested and the needs of the data subject;
- that provision does not confer on the data subject a general right to obtain a partial or full copy of the document that contains his or her personal data or, if the personal data are processed in a database, an extract from that database;
- that provision does not rule out, however, the data subject having to be provided with portions of documents, or entire documents or extracts from databases, if that were necessary to ensure that the personal data undergoing processing and in respect of which access is requested are fully intelligible.

OPINION OF ADVOCATE GENERAL
PITRUZZELLA
delivered on 15 December 2022(1)

Case C-487/21

F.F.
interested parties:
Österreichische Datenschutzbehörde,
CRIF GmbH

(Request for a preliminary ruling lodged by the Bundesverwaltungsgericht (Federal Administrative Court, Austria))

›reliminary ruling – Protection of personal data – Regulation (EU) 2016/679 – Article 15(3) – Right of access by the data subject to personal data undergoing processing – Right to receive a copy of personal data – (
Concept of 'information')

Training of Lawyers on EU Law relating to Data Protection 2

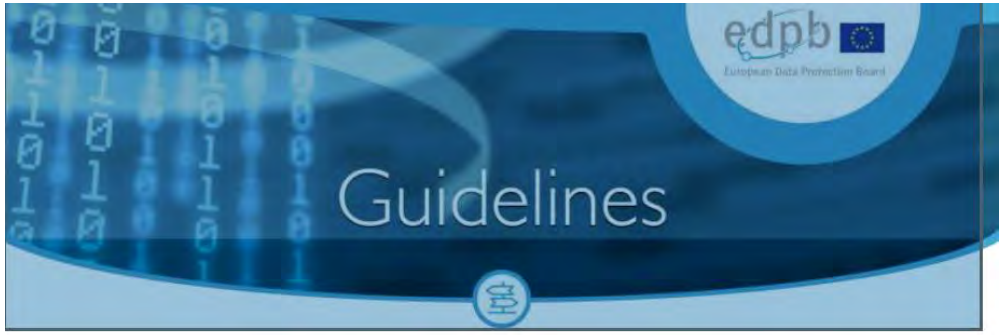
#TRADATA2

The exact boundaries of the right to obtain a copy according to the Advocate general (Case C-487/21)

- With the fourth question it has referred for a preliminary ruling, the referring court asks the Court whether the concept of 'information' in the third sentence of Article 15(3) of the GDPR refers only to the 'personal data undergoing processing' referred to in the first sentence of that paragraph or whether, in addition to those, it also includes the information referred to in Article 15(1)(a) to (h) (fourth question under (a)) or even other information such as, for example, metadata about data (fourth question under (b)).
- Conclusion of the Advocate general:
- The concept of "information" in the third sentence of Article 15(3) of Regulation 2016/679 **must be interpreted as referring exclusively to the "copy of personal data undergoing processing" referred to in the first sentence of that paragraph.'**

Limits and restrictions

- The right to obtain a copy shall not adversely affect the rights and freedoms of others (e.g. trade secrets, intellectual property, rights of other data subjects)
- Applying Art. 15(4) should not result in refusing the data subject's request altogether; it would only result in leaving out or rendering illegible those parts that may have negative effects for the rights and freedoms of others.



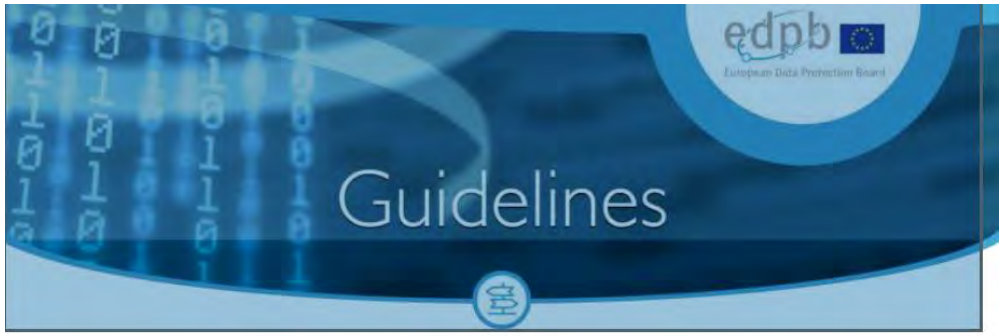
Guidelines 01/2022 on data subject rights - Right of access

Version 1.0

Adopted on 18 January 2022

Security!

- the controller is always obliged to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing
- Encryption is paramount, but access to data must be guaranteed



Guidelines 01/2022 on data subject rights - Right of access

Version 1.0

Adopted on 18 January 2022

Can DSR become a threat?

GDPR: When the Right to Access Personal Data Becomes a Threat

Luca Bufalieri, Massimo La Morgia, Alessandro Mei, Julinda Stefa
Department of Computer Science, Sapienza University of Rome, Italy

Email: bufalieri.1430586@studenti.uniroma1.it, {lamorgia, mei stefa}@di.uniroma1.it

***Abstract*—After one year since the entry into force of the GDPR, all web sites and data controllers have updated their procedure to store users' data. The GDPR does not only cover how and what data should be saved by the service providers, but it also guarantees an easy way to know what data are collected and the freedom to export them.**

In this paper, we carry out a comprehensive study on the right to access data provided by Article 15 of the GDPR. We examined more than 300 data controllers, performing for each of them a request to access personal data. We found that almost each data controller has a slightly different procedure to fulfill the request and several ways to provide data back to the user, from a structured file like CSV to a screenshot of the monitor. We measure the time needed to complete the access data request and the completeness of the information provided. After this phase of data gathering, we analyze the authentication process followed by the data controllers to establish the identity of the requester. We find that 50.4% of the data controllers that handled the request, even if they store the data in compliance with the GDPR, have flaws in the procedure of identifying the users or in the phase of sending the data, exposing the users to new threats. With the undesired and surprising result that the GDPR, in its present deployment, has actually decreased the privacy of the users of web services.

***Index Terms*—GDPR, Law Compliance, Privacy, Data Controllers, Web services**

to a data controller. In our study, we target 334 of the most popular web sites according to the Alexa ranking. For the best of our knowledge, we are the first to conduct a comprehensive study on this topic with a world distribution of web sites, so our finding are also useful to refine previous works that took into account only one phase of the SAR [2], or used less rigorous methodologies to select the organizations [3], or could be biased by the small set of data controllers put under the lens [4].

We find that 19.6% of privacy policy pages are not compliant with the actual regulation. Then, we inquiry all the targeted web sites requiring our personal data. We study how the collectors identify the requester, we collect the response, and monitor the response time. In the end, we obtain our personal data from almost 65% of the targeted web sites, with a average time to fulfill the request of 16.4 days. Lastly, we checked the procedures used by the data controllers to fulfill the request. In this phase, we find several flaws that affect more than 32% of targeted data controller, and that could transform a fundamental right into a new and unpleasant threat.

This paper makes the following contributions:

- **World-wide snapshot:** We makes a world-wide snapshot of the actual deployment of the GDPR. We report on the

GDPArrrrr: Using Privacy Laws to Steal Identities

James Pavur*
DPhil Researcher
Oxford University

Casey Knerr
Security Consultant
Dionach LTD

DSR and law enforcement directive

DSR & Directive 2016/680

ARTICLE 29 DATA PROTECTION WORKING PARTY

17/EN

WP 258

Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)

Adopted on 29 November 2017

Recommendations of the WP29

1. The Directive provides for a new architecture of the rights of data subjects, the principle being that they have a right to information, access, rectification, erasure or restriction of processing, unless these rights are restricted. Such restrictions shall only be possible where they constitute a necessary and proportionate measure and interpreted in a restrictive manner. Where these rights will have been restricted, Member States shall provide for the possibility for data subjects to exercise their rights through the competent supervisory authority which constitutes an additional safeguard for the data subjects.

2. The Directive states that Member States must provide for data subjects to have the right to obtain confirmation of processing and access to personal data being processed from the controller. The Directive does not allow for blanket restrictions to data subject rights.

DSR & EUROPOL REGULATION

EUROPEAN DATA PROTECTION SUPERVISOR

Decision of the European Data Protection Supervisor in complaint case 2020-0908 against the European Union Agency for Law Enforcement Cooperation (Europol)

DSR in the context of the European Data Strategy and the Digital services package

Enhanced portability?

Digital Markets Act (REGULATION (EU) 2022/1925)	• provide effective portability of data generated through the activity of a business user or end user –applies to gatekeepers;
Data governance Act (REGULATION (EU) 2022/868)	• Data intermediation services (providers of secure environment for individual and companies to share data) • Personal data spaces (data wallets) for individuals to share their data
Data Act	• Measures to allow users of connected devices to gain access to data generated by them (freeing IoT data) • Reinforced data portability right, both for personal and non-personal data

Questions?

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

Avv. Giovanni Battista Gallus – gallus@array.law

Training of Lawyers on European Data Protection Law 2 (TRADATA 2)

Maciej Gawroński and Michał Ćwiakowski

Introduction to the GDPR

Warsaw, 17 February 2023

The project is co-financed with the support of the European Union's Justice programme

GP Partners

Introduction to the GDPR …in 50 minutes

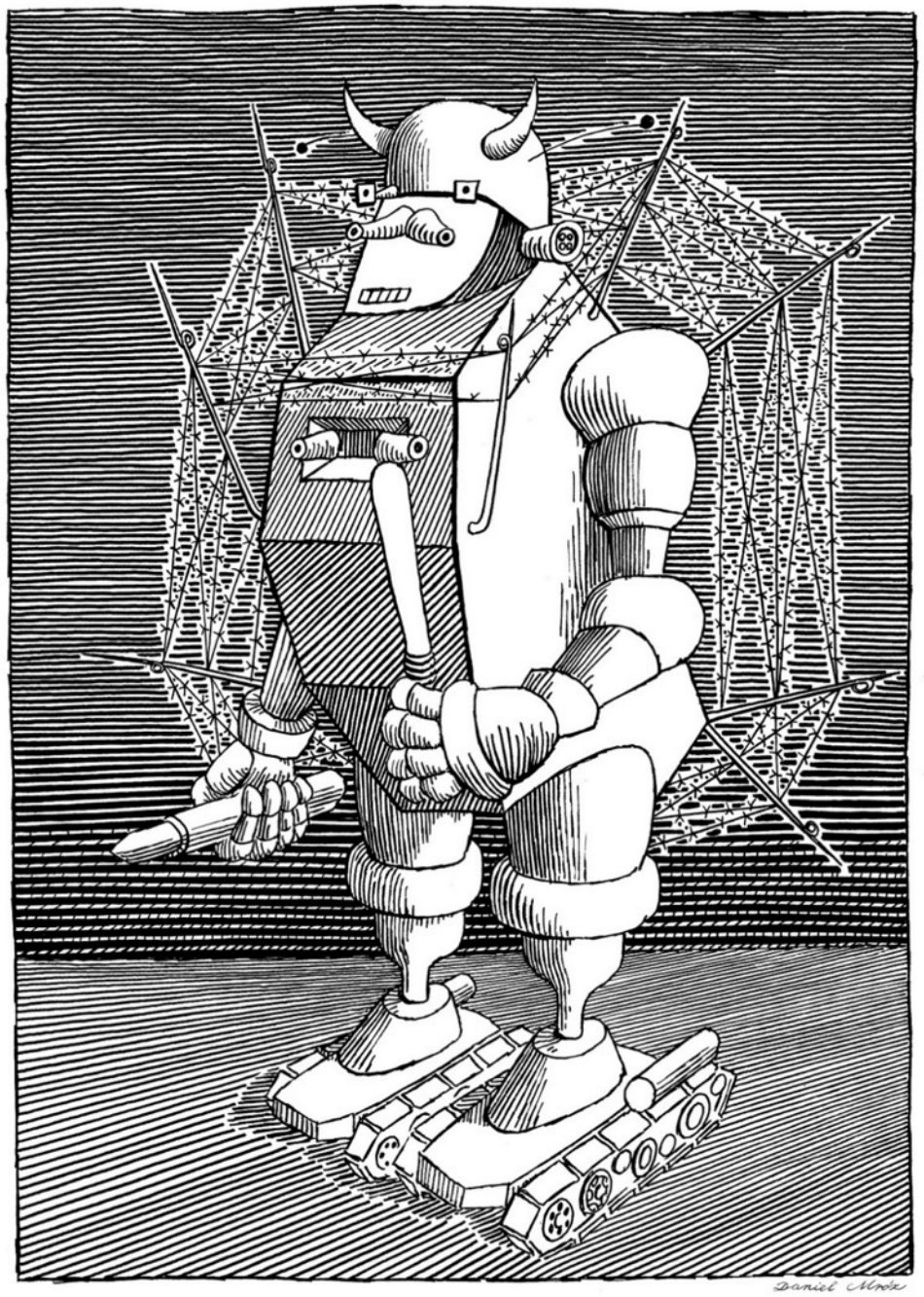
TRADATA 2
Training Lawyers on EU Data Protection Law

Maciej Gawroński
attorney-at-law, CIPP/E

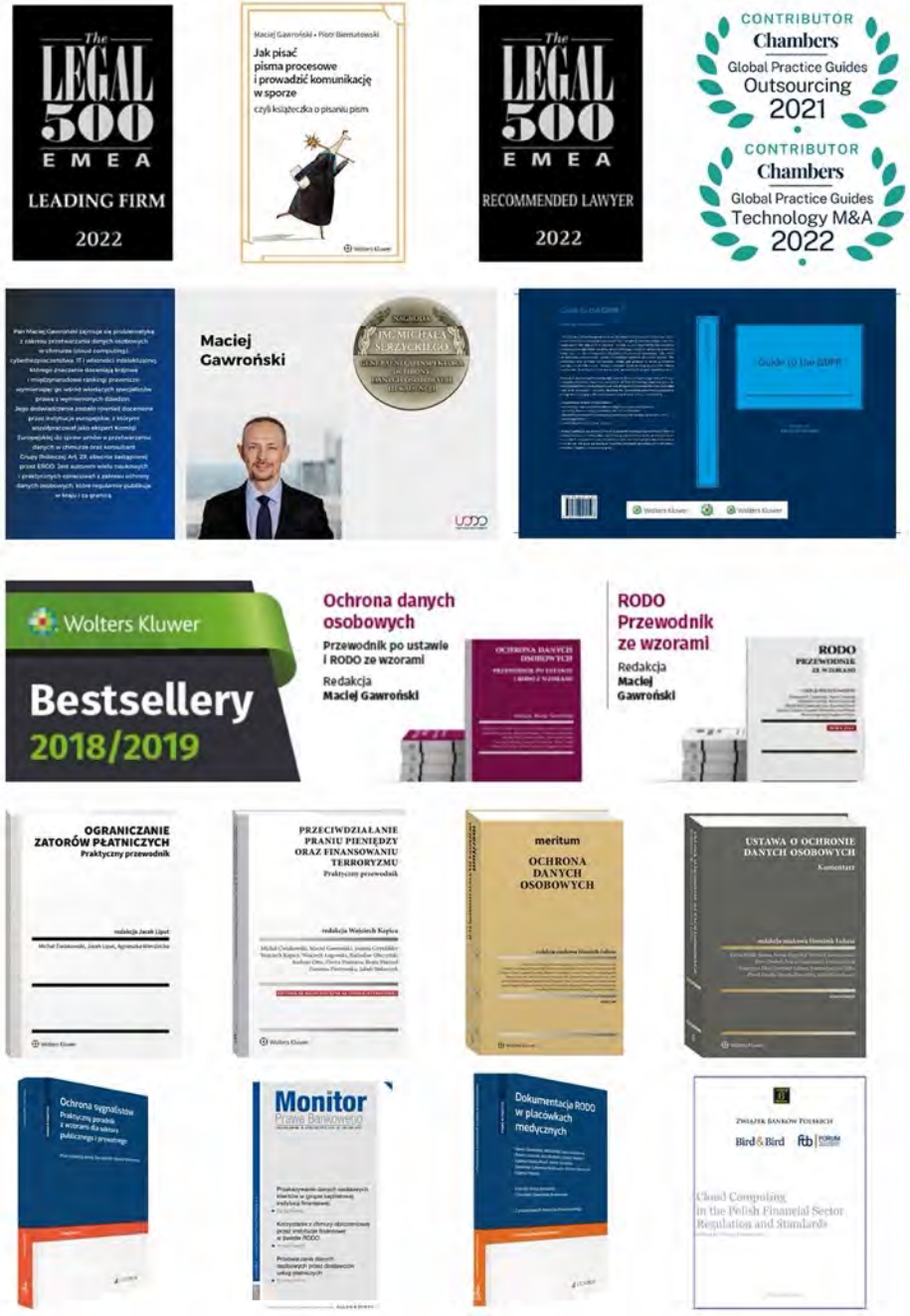
Michał Ćwiakowski
advocate, ISO 27001 Lead Auditor

17 February 2023

gdps Good Data Protection Standard

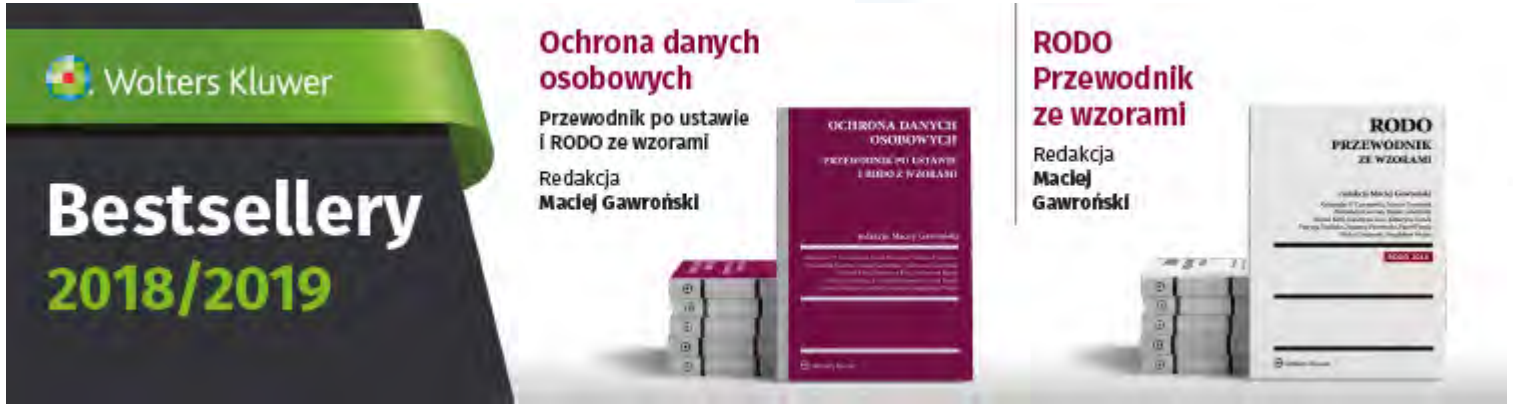


Introduction to the GDPR in 50 minutes 😅



Maciej Gawroński

- „Guide to the GDPR” over 15 000 copies sold
- Polish Data Protection Office Award 2021
- Supporting Expert of the European Data Protection Board
- Good Data Protection Standard system (gdpstandard.com) creator
- Proposed data portability (GDPR 20), sub-processors liability (GDPR 82) and
- EC Cloud Computing Contract Expert (2014)
- Article 29 Working Party Consultant on data transfers (2014)
- Recommmended by Rzeczpospolita, Chambers & Partners, Legal 500, Who’s Who Legal 100, Best Lawyers, Guide to the World's Leading Lawyers
- bla bla (meaning other books, lectures and conferences)



Enter search phrase

Infolinia Urzędu

News | About us | What we do | Legislatic

28.01.2021

We already know this year's winners of the 'Michał Serzycki' Data Protection Award

Barbara Grądkowska, Jen Persson and Maciej Gawroński joined the group of laureates of the 'Michał Serzycki' Data Protection Award. The winners were distinguished for their activities in the field of education about personal data protection.

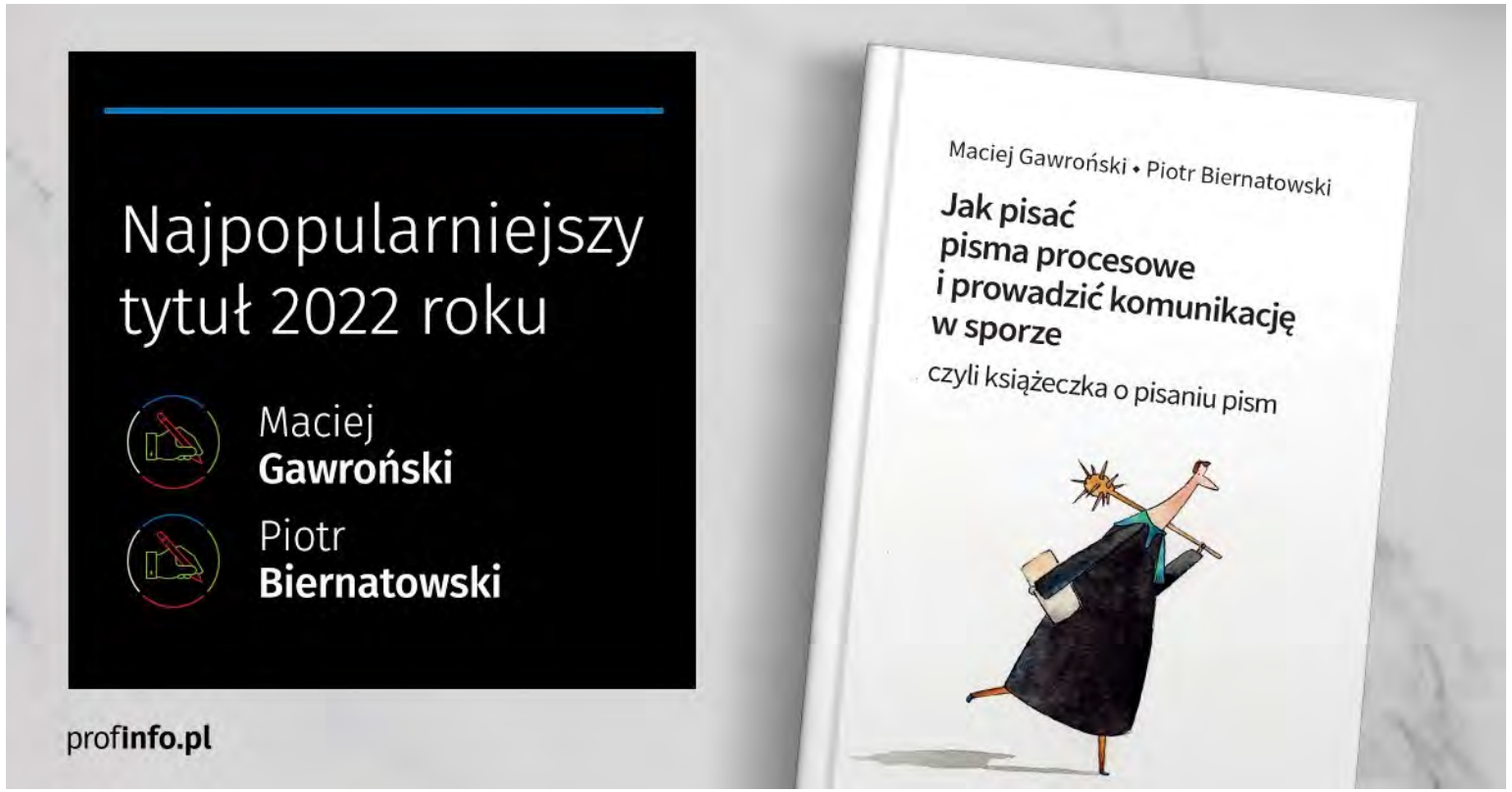
The award ceremony was held in Warsaw on 27th January 2021, on the eve of the 15th Data Protection Day.

Laureates of the 'Michał Serzycki' Data Protection Award in 2021

This year, the award was presented for the fourth time and went to:

- **Barbara Grądkowska, Director of the Special School and Educational Center in Zamość,** for many years the coordinator of the national educational program of the Personal Data Protection Office "Your data - Your concern". She included the subject of personal data protection in the area of the Center's activities, meeting the educational needs of students in this area. Thanks to her commitment to protect the privacy of students with intellectual disabilities and the educational activities in the field of personal data protection, those who are the most vulnerable in the world of modern technologies have the opportunity to learn how to safely navigate in the digital world and avoid threats. Her achievements in this area also attracted the attention of local authorities and the media, contributing to the promotion of the principles of personal data protection and the right to privacy.
- **Jen Persson, Director of the NGO DefendDigitalMe**, founded in England, working for civil liberties, and in particular supports the safe, fair and transparent processing of children's data in the education sector. The laureate cooperates with UK government bodies, educational institutions, industry, children's rights and international organizations such as the Council of Europe, which is particularly important in times of rapid technological development in education. The excellent cooperation undertaken by the Personal Data Protection Office in 2020 with Ms. Jen Persson resulted in organising a seminar for teachers from European countries on remote education.
- **Maciej Gawroński, legal advisor, experienced lawyer, expert and very good practitioner** who has been actively supporting the protection of personal data for many years. He is an authority dealing with the issues of personal data processing in the cloud (cloud computing), cybersecurity, IT and intellectual property. He is appreciated by national and international legal rankings, listing Mr. Gawroński among the leading law specialists in these areas. By participating in numerous conferences and other events related to the protection of personal data, both in the country and abroad, he adds his invaluable voice to the discussion on the directions of activities in this area. In terms of popularizing public awareness of personal data protection, it is also worth appreciating his active participation in social media with a valuable voice on issues related to the protection of personal data.

gppartners.pl



gdps
Good Data
Protection
Standard

Agenda

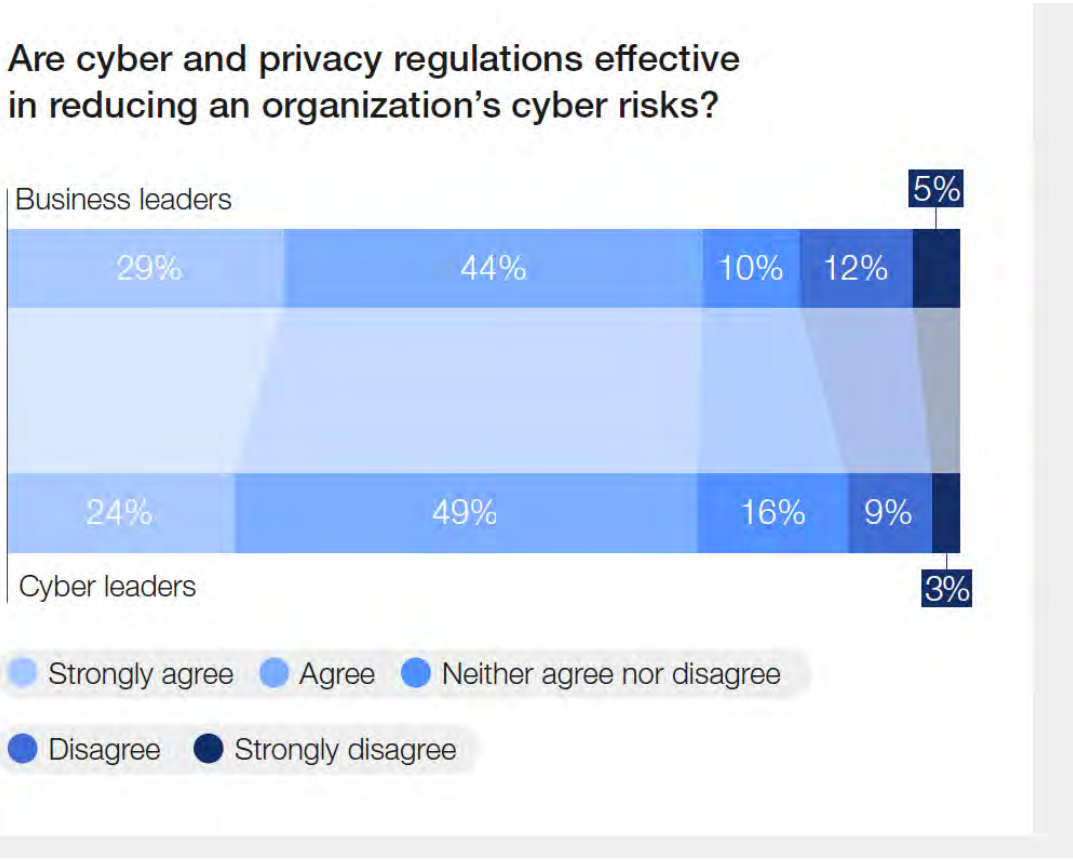
1. **GDPR - general characteristics**, basic concepts
2. **Sprint through the rules** for controllers:
   (1) basic legality
   (2) rights of individuals (DSRs)
   (3) security
   (4) entrustment of data, joint controlling, data sharing
   (5) data export / data transfers
   (6) liability - remedies
3. **Wrap up – end of presentation**
4. **Additional slides**

Technology vs regulation

https://www.youtube.com/watch?v=5oPsvq81n2A

Good news– GDPR recognized effective

The 2023 Outlook shows a significant shift in the perception of how regulations affect cyber risk. In the 2022 report, more than half of respondents did not agree that cyber and privacy regulations are effective in reducing their organizations' cyber risks. This year's outlook indicates that 73% of respondents agree with the same statement.



GDPR - General Characteristics

GDPR – subject matter and objectives

1. This Regulation lays down **rules relating to the protection** of natural persons with regard to the **processing** of **personal data** and rules relating to the **free movement** of personal data.

2. This Regulation **protects fundamental rights and freedoms** of natural persons and in particular their **right to the protection of personal data**.

There is no security in digital world therefore there must be security regulation

GDPR – TOWARDS UNIFORM RULES

GDPR - what's new?

- Risk-based approach?
- Accountability – presumption of guilt
- Data retention
- Data Subject Rights - many
- Privacy by design, Privacy by default
- Register of Data Processing Activities
- Breach notification
- Data Protection Impact Assessment (DPIA)
- Data Protection Officer (DPO)
- Direct liability of processors (I am sorry, my fault)
- Fines and liability
- TFD data export

What does GDPR consist of?

gdps Good Data Protection Standard

The GDPR is divided into the following chapters:

0. Recitals (173 recitals take up about 35% of the GDPR text)

I. General provisions - including territorial and material scope

II. Principles

III. Rights of the data subject

IV. Controller and processor

V. Transfer of personal data to third countries or international organisations

VI. Independent supervisory authorities

VII. Cooperation and consistency

VIII. Remedies, liability and penalties

+ Exceptions Provisions for specific processing situations

+ Delegated and implementing acts

GDPR - Functional breakdown

gdps Good Data Protection Standard

PILLARS

Legality – obligations to implement

Rights – data subject requests to respond

Security - processes to design and maintain

FOUNDATIONS

Risk - risk (for data subjects) a measure of required dilligence

Accountability - duty to explain (presumption of guilt)

OTHER

Data processing supply chain management

Transfers - outside the EU

Table of Contents	Functional Breakdown
Recitals	Interpretation
CHAPTER 1. General provisions	Compliance I
CHAPTER 2. Principles	
CHAPTER 3. Rights of data subject 12, 13, 14	
CHAPTER 3. Rights of data subject 12, 15-22	Complaints management
CHAPTER 4. Controller and processor 24, 25.1, 26-30, 35, 36, 37-39	Compliance II
CHAPTER 4. Controller and processor 32, 25.2	Security
CHAPTER 4. Controller and processor 33, 34	Consequences – Breach management
CHAPTER 5. Transfers of personal data to third countries or international organizations	Compliance III – Data exports TFD
CHAPTER 6. Independent supervisory authorities	For Authorities
CHAPTER 7. Cooperation and consistency	
CHAPTER 8. Remedies, liability and penalties	Consequences – Legal proceedings
CHAPTER 9. Provisions relating to specific processing situations	Exceptions (e.g. journalists)
CHAPTER 10. Delegated acts and implementing acts	For Authorities
CHAPTER 11. Final provisions	

GDPR - THREE PILLARS AND TWO FOUNDATIONS

OBLIGATIONS

Article 5
Article 6
Article 7
Article 8
Article 9
Article 10
Article 11
Article 12
Article 13
Article 14
Article 15
Article 16
Article 17
Article 18
Article 19
Article 20
Article 21
Article 22
Article 24
Article 25
Article 26
Article 27
Article 28
Article 29
Article 30
Article 32
Article 33
Article 34
Article 35
Article 36
Article 37
Articles 46
Articles 49

Proactive obligations

1) **Inventory** of data processing operations,
2) **Design and documentation** (i.a. data processing policy, records of processing activities, specific procedures, LIA, DPIA, consents, information obligation, data processing agreements, SCCs, transfer impact assessment),
3) **Security** (security policy, data processing risk analysis,, TOMs).

Reactive obligations

Rights of data subjects

- to access data and to a copy of data
- to rectify data
- to erasure
- to restrict processing
- to data portability
- to object to processing due to particular situation
- to object to processing for marketing purposes
- to a human intervention in automated processing

and many more…

Reactive obligations

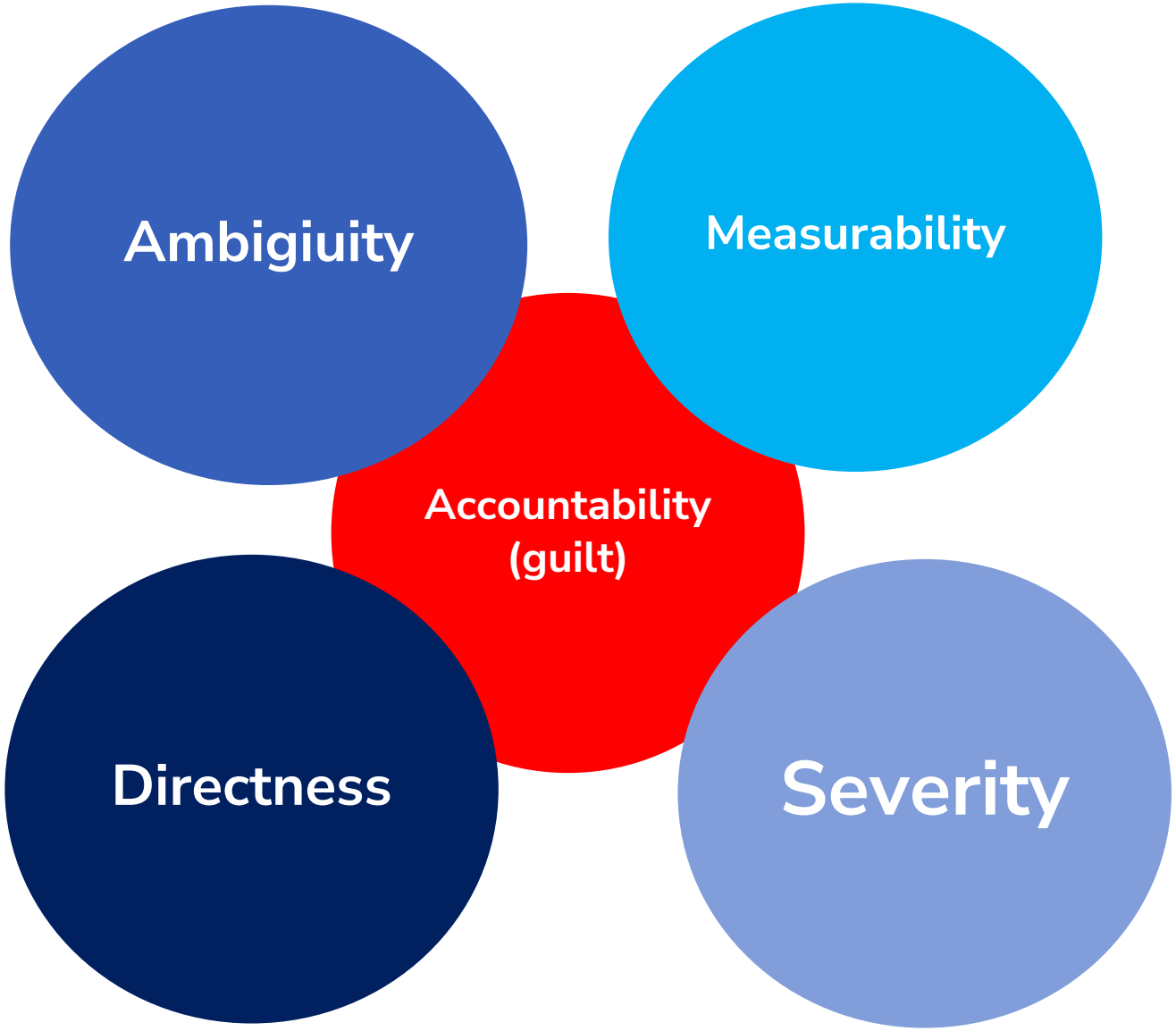
Breach Management

- breach **notification** (supervisory authority)
- breach **communication** (data subjects),
- a need for speed 72h

Legal Proceedings

https://gazelleconsulting.org/10-gdpr-memes-that-will-make-you-cry-with-laughter/

MAIN CHARACTERISTICS



Ambiguity

GDPR is built on a set of principles →

1) lawfulness, fairness and transparency (5.1.a GDPR)
2) purpose limitation (5.1.b GDPR)
3) data minimisation (5.1.c GDPR)
4) accuracy (5.1.d GDPR)
5) storage limitation (5.1.e GDPR)
6) integrity and confidentiality (5.1.f GDPR)
7) Accountability (5.2 GDPR)

- art. 32 GDPR – security obligation

*…the controller and the processor shall implement **appropriate** technical and organisational **measures** to ensure a level of security appropriate to the risk*

24.1, 25.1

AMBIGIUITY

Not by accident the guidelines are vague

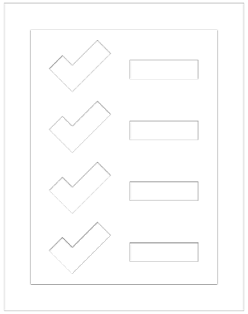
"It's a question of which side of the table you're sitting on. As a regulator, we have tasks too. You don't have to fulfill my tasks, so don't expect me to fulfill yours."

Andrea Jelinek
Chair of the European Data Protection Board

approx. 60 separate sets of guidelines

https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en?f%5B0%5D=opinions_publication_type%3A64

https://iapp.org/news/a/new-wp29-chair-talks-enforcement-role-of-the-dpo/ accessed 26.04.2018



Risk-based approach // Risk assessment

GDPR 24.1.

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.

GDPR 32.1.

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the **risk of varying likelihood and severity** for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a **level of security appropriate to the risk**

DIRECTNESS

The GDPR applies to everyone across the Union, in **fact every entity except ordinary consumers …at home, ie**:

- **individuals running businesses**,
- **legal persons**: joint-stock company, limited liability company, cooperative, foundation, registered association, state enterprise, religious association, research institute, political party, trade union, ecclesiastical legal person,
- **public authorities**
- **other entities**, e.g. partnership, limited partnership, association, university...
- **neighbours…**
- **bloggers, influencers…**

Full implementation of GDPR means hundreds of obligations imposed on Controllers.

MEASURABILITY

1 month to respond to a data subject's request, indirectly collected data IO

3 months (max) to comply with the person's request

72 hours to notify the SA of a security breach

low risk/risk/high risk, residual risk, risk assesement, fines calculator ;-)

0/1/2/3/4/5 – levels of data processing risk? 🤔

0 – no risk no processing, 1 – minimum, 2 – low, 3- risk, 4 – high, 5 – unacceptable?

SEVERITY

Astronomical fines "effective, proportionate and dissuasive" (GDPR 83.1.).

- **up to € 20/10 M**
- **up to € 4/2%** of the worldwide turnover when it's > €500M

Penalty matrix - 18+ criteria (83.2. GDPR)

"**Confiscation" of benefits and savings:**

Article 83.2.k GDPR: any other aggravating or mitigating factors applicable to the circumstances of the case, such as financial benefit derived directly or indirectly from the breach or loss avoided.

PRESUMPTION OF GUILT a.k.a. ACCOUNTABILITY

GDPR 5.2.

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

GDPR 24.1.

…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

GDPR 82.3.

The controller or processor shall be exempted from liability pursuant to paragraph 2 if the controller or processor proves that they are in **no way at fault** for the event giving rise to the damage.

Private enforcement

82.1. Any person who has suffered material or non-material damage […] shall have the **right to receive compensation from the controller or processor** for the damage suffered

82.2. Any controller involved shall be liable […]. A processor shall be liable […] where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to **lawful instructions** of the controller

82.4. A controller or processor shall be exempt from liability […] if it **proves that it is not in any way responsible** for the event giving rise to the damage

Great Absent?

PRINCIPLE OF PROPORTIONALITY

Where are we?

GDPR:

- no full unification of data protection rules

- BUT a step towards

GDPR 2?

2 big 2 B liable?

The Darth Vader of GDPR


Guide to the GDPR
Kluwer
CIPP/E
Helen
Dixon
Data Protection Commission
KEYNOTE SPEAKER
SPEAKER

END OF GDPR CHARACTERISTICS

NEXT – OBLIGATIONS OF CONTROLLERS

Sprint through obligations of controllers

GDPR – Basic concepts

Personal data

personal data – every information we can attribute to a person, including so-called content and metadata (IP)

(content, membership file, employee file, paper list of employees, decisions on granting allowances, data of employees and their families for the purpose of granting allowances, data of employees for the purpose of holding a pre-trade union referendum, data obtained within the framework of trade union consultations).

- Personal data can be "ordinary" (regular) or "special categories" (sensitive) and also criminal.

"**personal data**" means **any information relating to an identified or identifiable natural person** ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

"**special categories of data**" are listed in Article 9.1 of the GDPR.

The processing of personal data revealing **racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of genetic data, biometric data for the** purpose of uniquely identifying a natural person or **data concerning a person's health, sexuality or sexual orientation shall be** prohibited.

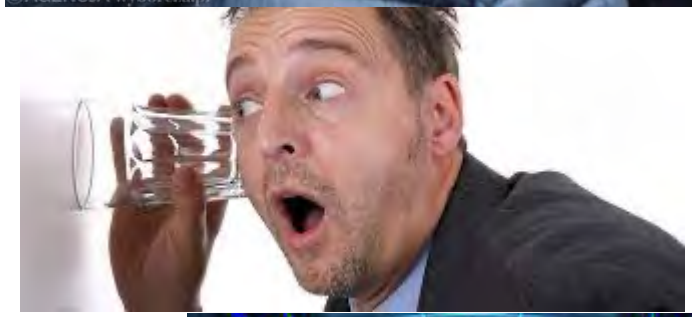
Examples of data categories

- ***Basic identification data***
- *Identification data allocated by public authorities*
- *Electronic identification data*
- *Electronic location data*
- *Biometric identification data*
- *Financial identifying information*
- ***Information on financial resources***
- *Commitments and expenses*
- *Solvency*
- *Loans, mortgages, lines of credit*
- ***Financial assistance***
- *Insurance policy details*
- *Pension plan details*
- *Financial transactions*
- *Compensation*
- *Official acts*
- *Agreements and settlements*
- *Permits*
- *Personal details*
- *Military service status*
- *Immigrant status*
- *Description of appearance*
- *Private habits*
- *Addictions*
- *Lifestyle*
- *Travel and movement data*
- *Contacts with others*
- *Holdings*
- *Social functions*
- *Complaints, incidents and accidents*
- *Awards*
- *Use of media*
- *Psychological data*
- *Marriage or other form of relationship*
- *Marriage history*
- *Details of other family members or household members*
- *Hobbies and interests*
- *Membership (other than service, political, trade union)*
- *Legal information on suspicions*
- *Information regarding convictions and sentences.*
- *Information on judicial action*
- *Data on administrative penalties*
- *Consumption habits*
- ***Residence data***
- *Physical health data*
- *Mental health data*
- *Data on risky situations and behaviour*
- *Genetic data relating to population studies, gene testing, etc.*
- *Recovery data*
- *Education and training*
- *Academic teaching*
- *Publications*
- ***Occupation and employment***
- *Current employment*
- *Recruitment*
- *Completion of work*
- *Career*
- *Absences and adherence to work order*
- *Occupational medicine*
- ***Remuneration***
- *Assets held by the employee*
- *Organisation of work*
- *Evaluation*
- *Training for the position*
- *Credentials,*
- *Levels of competence*
- *Use of technology*
- *Data on racial or ethnic origin*
- *Data on sex life*
- *Political views*
- *Political connections*
- *Membership of advocacy groups, paramilitary organisations*
- ***Trade union membership***
- *Religious or philosophical beliefs*
- *Beliefs*
- *Video recordings*
- *Image*
- *Sound recordings*

Processing of personal data

"**processing**" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Can data controller process data unconciously?
Unwillingly?



- GP Partners

When does GDPR apply?

2.1 GDPR

This Regulation applies to (1) the processing (2) of personal data by (3) wholly or partly automated means and (4) to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

Controller

Controllers use data for themselves

Every organization is a data controller

> *"**controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, **determines the purposes and means of the processing** of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law*

Processor

Processor has data on behalf of somebody else, usually for money.

*"**processor**" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*

Data sharing – defined only indirectly

a) recipient:

- controller
- processor
- natural person

b) „not recipient" – authority conducting particular legal proceedings (*particular enquiry*)

> *'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.* ***However****,* ***public authorities*** *which may receive personal data in the framework of a* ***particular inquiry in accordance with*** *Union or Member State* ***law*** *shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;*

bad legislation

Data breach

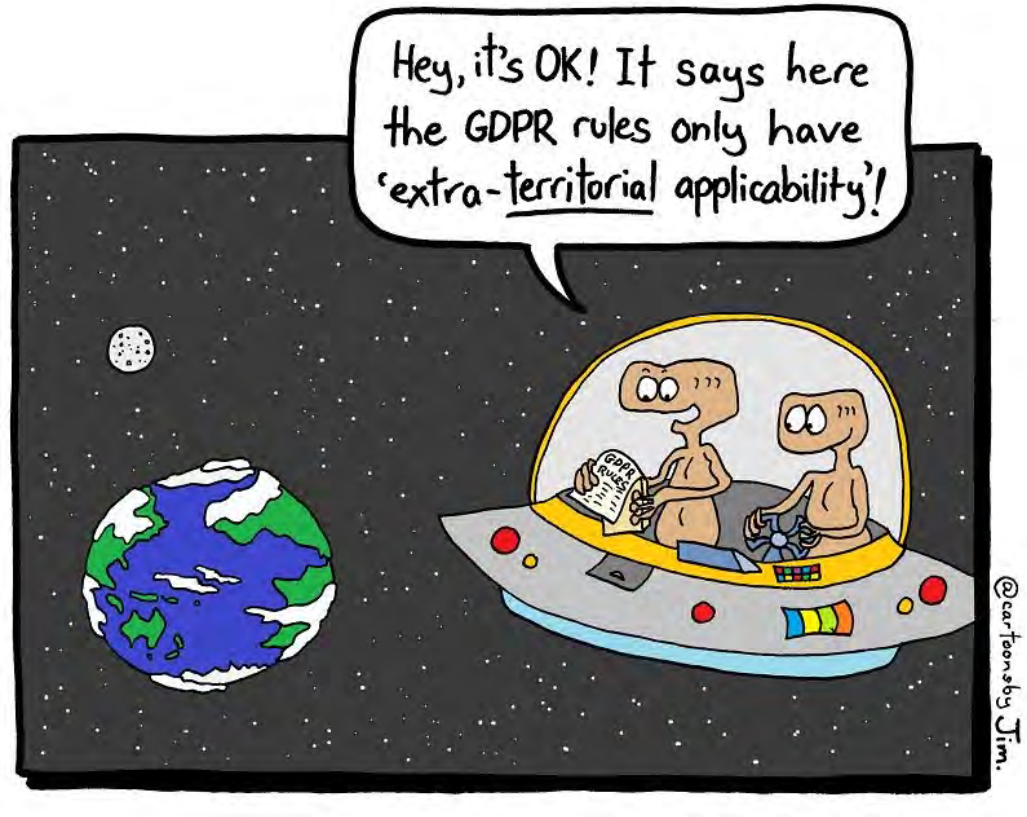
effective loss of control over data

„Personal data breach" means a [1] ***breach of security*** *[2]* ***leading to*** *[consequences] the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;*

Where does GDPR apply? EVERYWHERE

- If your organisation is based in EU (regardless where the processing takes place
- Wherever you are If your organisation:
    1) addresses your offer to EU residents
    2) monitors people behaviour in EU

No, ETs should not be so happy. GDPR DOES have an extra-terrestial effect.



https://twitter.com/cartoonsbyjim/status/1002450296834912256

What is missing – GDPR 2 ideas

- **imperfect definition of processing –** the issue of unsolicited data, unaware data processing (subconscious?)

- **Parallel control** - The CJEU's judgement in Fashion ID case created an unnatural situation in which two or more unrelated controllers with unrelated goals and different power are considered joint controllers (Facebook and fanpage users in the first place).

- **Data sharing -** GDPR does not address directly a situation in which one controller shares data with another controller (controller to controller transfer).

GDPR Details

Legality 1

Lawfulness of data processing

Legality 1 - Principles

- data processing principles - 5
- basis for processing - 6
- consent requirements - 7
- minors' protection in Internet - 8
- special categories data (ex sensitive) - 9
- criminal data - 10
- „unidentified" data - 11
- information obligation - 13, 14
- tracking recipients 19.1st

Lawfulness of data processing

Legality 2 - Controller and processor

- risk-based approach and accountability principles - 24
- privacy by design - 25.1
- joint controlling - 26
- EU representative
- data processor - 28
- documented instructions - 29
- register of activities and register of categories - 30
- DPO - 37-39

Lawfulness of data processing

Legality 3 - Transfers of data outside the EU only under additional conditions - 44

- Standard Contractual Clauses + TIA
- Adequacy decision
- Treaty
- Contract performance
- Explicit consent informed of possible risks
- Absolute necessity

Principles of data processing

We should process personal data in accordance with the following principles:

a) Lawfully, fairly and transparently (lawfullnes/legality)

b) For specific purposes only (purpose limitation)

c) Only necessary data (data minimization)

d) Ensure data are correct and up to date (accuracy)

e) No longer than necessary (temporality / storage limitation)

f) Securly (integrity and confidentiality)

very vague and general BUT

The controller […] must be able to **demonstrate compliance ("accountability").**

Fairy = do not hoax

Basis + Conditions = Article 6 + 9

Ordinary/regular data

a) consent
b) performance or conclusion of the contract
c) controller's legal obligation (e.g. AML)
d) someone's vital interests
e) public task, public authority
f) legitimate interest of controller / third party (witnesses, opponents, etc.)

Special categories also

a) express consent
b) employment and social law
c) vital interests + unconsciousness/underage/ incapacitation
d) NGOs...
e) publically disclosed data (Elton John not Hunter Biden. HB is a journalist exception)
f) claims enforcement/defense
g) letter of law
h) health care (occupational medicine, diagnosis, health care ...)
i) public health (abused for sanitarism)
j) archives, statistics, scientific and historical research

Information obligations

Information obligation

GDPR 13 and 14

- Identity, contact details of controller, DPO, representative
- Purposes of processing, legal basis
- Legitimate interests (e.g. marketing) if invoked
- Information about recipients of personal data or categories of recipients, if any (other companies if we want to e.g. sell the data, subcontractors - processors, but not state authorities)
- Where applicable, information on transfers to a third country
- Categories of data obtained, if not from the person concerned
- Information on rights
- Information on obligations (if data must be provided)
- Information about automated decision-making (including related profiling)
- Information about the source of the data, if not from the person concerned

In what situations and when do we inform you about data processing?

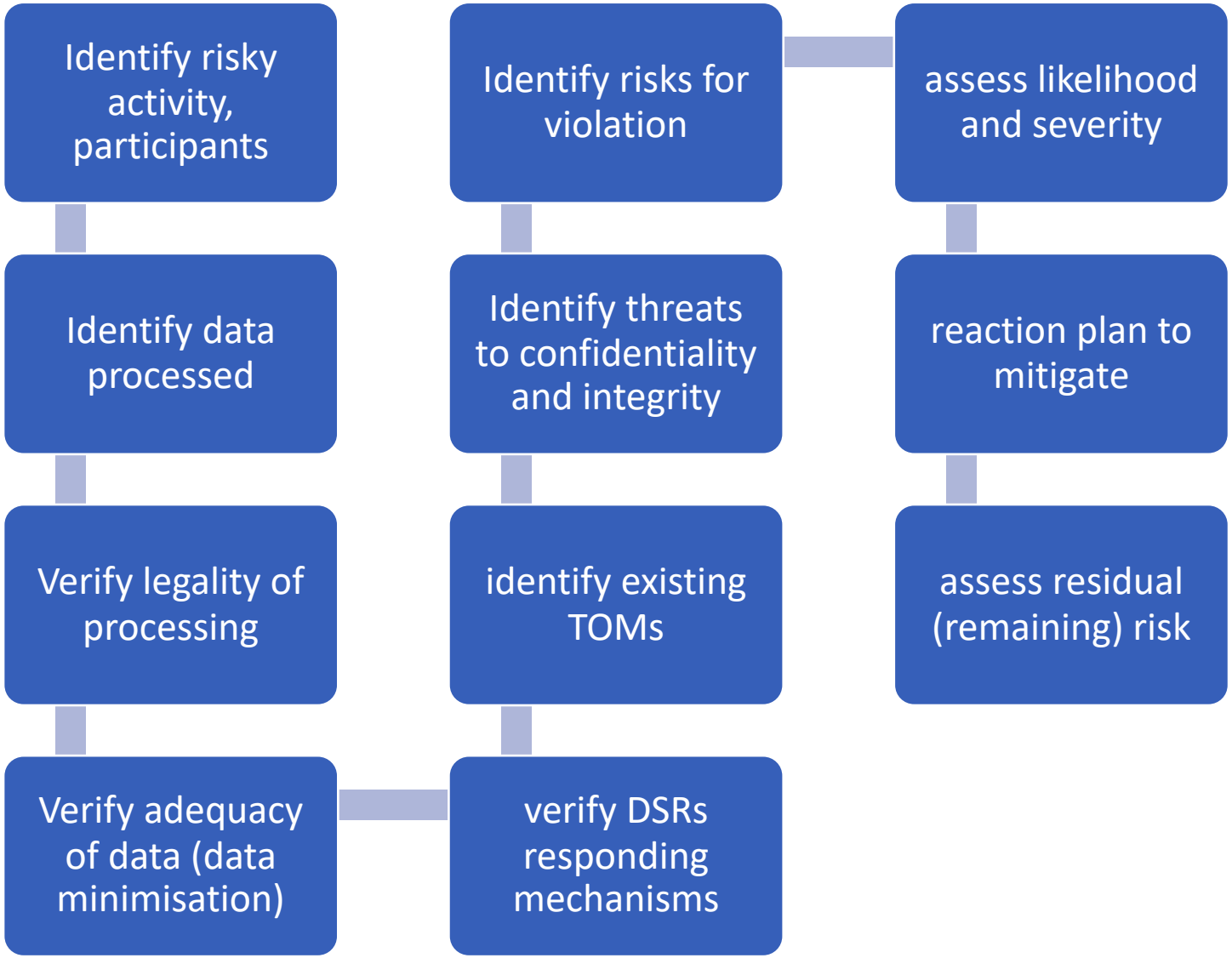
- When we collect data directly from data subjects (GDPR 13) - we inform when we obtain data from a person
- When we obtain data by other means, e.g. from publicly available sources such as LinkedIn (GDPR 14) - we inform within one month. We inform as soon as possible, within a month or at the first contact or at the disclosure of the recipient's data, whichever is sooner.
- When we change the purpose of data processing (GDPR 13(3) and 14(4))
- When we execute a data access request (GDPR 15) - within one month of the request (as a general rule, extendable by 2 months).

Privacy by design – designing privacy

GDPR 25.1

Taking into account the **[1]** state of the art, the **[2]** cost of implementation and the **[3]** nature, scope, context and purposes of processing as well as the **[4] 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**, 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.

DPIA - CNIL



I. Data processing agreement - Article 28 GDPR

II. Joint control - Article 26 GDPR

END OF COMPLIANCE I

NEXT – DATA SUBJECT'S RIGHTS

DATA SUBJECT'S RIGHTS

Individuals' rights

- Metrics (SLA) - 12
- information obligation direct collection - 13
- information obligation indirect collection - 14
- data access, data copy - 15
- rectification - 16
- removal - 17
- data limitation - 18
- notification to and about recipients - 19
- **data portability - 20**
- objection - 21
- automatic processing - 22

Rights of data subjects – yes same slide (almost)

Reactive obligations

- to access data and to a copy of data
- to rectify data
- to erasure
- to restrict processing
- to data portability
- to object to processing due to particular situation
- to object to processing for marketing purposes
- to a human intervention in automated processing

and many more…

Individuals' rights

- **Right to be informed about data collection**
- **Right to access to and copy of data** (15)
- **Right to rectify** (16)
- **The right to erasure /be forgotten** (17)
- **Right to restrict processing** (18)
- **Right to know about recipients** (19.2nd)
- **Right to data portability** (20)
- **Right to exceptional and marketing objection** (21)
- Right to withdraw consent
- **Right of appeal against automatic decision** (22)
- Right to response (prohibition of ignoring)
- The right to "readability"

- Right to facilitate (to guide)
- Right to deadlines
- Right to information about rights
- Right to equally easy consent withdrawal
- Right to information on data recipients
- Option for convenient electronic handling
- **Right to know about a data breach**
- **Right to complain and appeal**
- **Right to court damages**
- Right to an NGO support

Right of access

GDPR 15.1

Right to:

confirmation as to whether data are being processed

access to the data

and to information on: **[a]** purposes, [**b]** categories, **[c]** recipients, [**d]** retention, [**e, f]** rights, [**g]** source, **[h]** automated decision-making, profiling, its rules and consequences - corresponds to the right to information

Right to a copy of the data

GDPR 15.3 The controller shall provide the person with a copy of the data relating to them.

First copy for free. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs.

If the data subject requests a copy by electronic means and unless he or she indicates otherwise, the information shall be provided by commonly used electronic means.

GDPR 15.4 The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

- **Notice & Takedown – i.e. the procedure for objection by others + denial of release due to own rights and secrets**

Right of rectification

GDPR 16

- The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.
- Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

The right to erasure/to be forgotten

GDPR 17

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- withdrawal of consent
- **object** to the processing **and there are no overriding legitimate grounds for** processing (with direct marketing there will be none - GDPR 21.2)
- the data have been unlawfully processed
- personal data must be deleted in order to comply with a legal obligation
- **the personal data was collected in connection with the offering of information society services** (as in direct marketing)

Limitation of processing

a) Data subject questions accuracy of data

b) processing is unlawful and data subject objects to erasure of the data, requesting instead that the use of the data be restricted;

c) the controller does not need the data, but the person needs them to establish, assert or defend a claim;

d) for the duration of the specific objection (whether the controller's grounds override the grounds for objection).

- practical solutions:

  1) no one will come forward with this on their own because they won't understand

  2) we will propose a restriction in lieu of other rights - e.g., for the purpose of storing surveillance data, if we are afraid to disclose the recording directly to the data subject

Obligation to track and notify the recipients

GDPR 19

- The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort.
- The controller shall inform the data subject about those recipients if the data subject requests it.

- recent ECJ ruling - where personal data have been or will be disclosed to recipients, there is an obligation on the part of the controller to provide the data subject, on request, with the actual identity of those recipients. It is only where it is not (yet) possible to identify those recipients that the controller may indicate only the categories of recipient in question.

- Technically it is a part of legality. You need to proactively track recipients to be able to comply with DSR

Right to data portability

GDPR 20

- The data subject shall have the right to **receive** the personal data concerning him or her, which he or she **has provided to a controller** and has the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:
  - the processing is based on consent or contract,
  - the processing is automated
- In exercising his or her right to data portability, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.
- Exceptions: public interest or exercise of official authority entrusted to the controller.
- The right to data portability must not adversely affect the rights and freedoms of others (the issue of data rights and the lawfulness of data - analogy to the grounds for notice & takedown)

Right to object: special situation and direct marketing

GDPR 21

- The data subject shall have the **right to object**, on grounds relating to his or her **particular situation**, at any time to processing of personal data concerning him or her including profiling based on those provisions.
- The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
- Where personal data are processed for the purposes of **direct marketing**, the data subject shall have the **right to object** at any time to processing of personal data concerning him or her for such marketing, including profiling, to the extent that the processing is related to such direct marketing. If the data subject objects to the processing for direct marketing purposes, the personal data shall no longer be processed for such purposes
- At the latest on the occasion of the first communication with the data subject, the data subject shall be expressly informed of the right to object.

Appeal against automated decision

GDPR 22

The right not to be subject to a decision producing **legal or similarly significant effects** which is based **solely on automated processing**, including profiling, unless

- is necessary for the conclusion or performance of a contract with a person
- lawful
- is based on an explicit consent

In cases (1) and (3), the Controller shall implement appropriate safeguards,at least the rights to **obtain human intervention** by the controller, to express one's point of view and to challenge that decision.

End of DSRs

Next - Security

Security

- *Privacy by default 24.2 (Security)*
- Security and risk analysis - 32 (Security)
- Data Protection Impact Assessment – 35 (Compliance)
- Prior Consultation - 36 (Seppuku)
- Breach notification - 33 (Consequences)
- Breach communication - 34 (Consequences)

Security - GDPR 32

Taking into account the (1) state of the art, (2) the costs of implementation and (3) the nature, (4) scope, (5) context and (6) purposes of processing as well as **(7) the risk of (8) varying likelihood and (9) severity** for the rights and freedoms of natural persons, 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:

- pseudonymisation and encryption of personal data
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services [CYBER SECURITY//BUSINESS CONTINUITY].
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident - DISASTER RECOVERY
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing - TESTING

Data Security Risk Assessment

- GDPR 32.2 risk assessment

  In **assessing the appropriate level** of security account shall be taken in particular of the **risks** that are presented by processing, in particular from accidental or unlawful **[1]** destruction, **[2]** loss, [3] alteration, [4] unauthorised disclosure of, or [5] access to personal data transmitted, stored or otherwise processed.

- GDPR 24.1 and 25.1 and 32.1

How to calculate data protection risk?

so that it’s good

Privacy by default – Minimisation!

GDPR 25.2

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 **[1]** amount of personal data collected, the **[2]** extent of their processing, the **[3]** period of their storage and **[4]** 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

How about this?

Data transfer to a third country

Territoriality

Principle

- Free movement of data within the European Economic Area
- No specific regulation for intra-EEA transfers
- Data transfer = data processing
- Transfers of data outside the EEA- transfer of data to third countries + international organisations.

Transfers of data outside the EEA - a two-step approach

- General obligations + additional obligations provided for in Chapter V of the GDPR

What is data transfer outside the EU?

Transfer of data to third countries = transfer of data outside the European Economic Area

No legal definition of transfers to third countries in the GDPR

Under the proposed definition:

any transfer of personal data that is actively made available to a limited number of parties or identified parties with the knowledge of the transferor or with the intention of providing the recipient with access to the personal data

a transfer of personal data which leads to the **personal data 'crossing' a 'secure' border into the European Economic Area** (EEA)

Basis for transfers to third countries
Article 45 GDPR

Pursuant to a decision of the European Commission
The Commission may decide that certain countries provide adequate protection for personal data:

EC Decisions:

1. Switzerland (2000/518/EC)
2. Canada (2002/2/EC)
3. Argentina (2003/490/EC)
4. Guernsey (2003/821/EC)
5. Isle of Man (2004/411/EC)
6. Jersey (2008/393/EC)
7. Faroe Islands (2010/146/EU)
8. Andorra (2010/625/EU)
9. Israel (2011/61/EU)
10. Uruguay (2012/484/EU)
11. New Zealand (2013/65/EU)
12. ~~USA - Privacy Shield (2016/1250) (self-certification).~~
13. Japan - C(2019) 304
14. Republic of Korea – C(2021) 9316
15. UK – new adequacy decision

Basis for transfers to third countries
Article 46 GDPR

"**subject to appropriate safeguards**", which means:

Based on the following specific legal instruments:

a) a legal instrument between public authorities and bodies (e.g. an administrative agreement between a Member State authority and a non-EU country authority)

b) Binding Corporate Rules (47 GDPR) - internal agreements within a corporate group (group of companies)

c) standard data protection clauses - model contract terms (adopted by the EC, adopted by the national supervisory authority)

d) approved code of conduct

e) approved certification mechanism

f) contract or administrative arrangement approved by the supervisory authority

Additional grounds for transfers to third countries Article 49 GDPR

Specific grounds for data transfer:

a) risk-based consent

b) performance of a contract or for the **conclusion of a contract at the** request of a person

c) concluding or performing a contract, where it is in the interest of the data subject, who is not party to the contract

d) public interest

e) redress

f) to protect someone's vital interests where the data subject is incapable of giving consent: (i) physically, (ii) legally

g) transfer from the public register under normal access conditions

Transmission really specific Article 49(2) GDPR

The transfer of data may take place on the basis of specific grounds which are: the **compelling legitimate interests of the controller:**

To benefit from the export of data under Article 49(2) requires that:

a) the transfer was not repetitive

b) concerned a limited number of people

c) was necessary for the legitimate interests of the controller (en. *compelling*, i.e. "compelling", fr. *imperieux*, i.e. "vital" interests of the controller)

d) the interests, rights and freedoms of the data subject are not overridden,

e) the Controller made a comprehensive assessment of the situation and consequently

f) ensure adequate safeguards for the protection of personal data,

g) informed the supervisory authority,

h) informed the data subject.

Transfers of data to third countries outside the EEA

What should I do?

- identify situations **where we transfer data outside the EEA,**
- **verify contacts with counterparties outside the EEA**, transfer of data to the parent company,
- **review the manner of communication** (monitoring of shadow IT) and use of public cloud services by our organization as well as processors (subcontractors).

Transfers of data to third countries - executive summary

- The most practical basis for transferring data outside the Union is the **standard data protection clauses**
- Consent is an inconvenient basis for data export because it can be revoked at any time
- The duty of information of data subjects to whom we transfer data outside the EEA exists and when transferring on the basis of:
  - standard data protection clauses
  - decisions on data protection adequacy

Judgment Schrems II

Maximilian Schrems, initiator of the ruling overturning the Safe Harbour (2015) and Privacy Shield (2020) program decisions

Judgment of the CJEU C-311/18 of 16.07.2020 so called Schrems II[1]

- **CJEU invalidates Privacy Shield** (lack of procedural safeguards for non-US persons subjected to mass electronic surveillance)
- **CJEU leaves in place SCC** .... but it is not necessarily legal to transfer data on the basis of SCC[2] - no more mechanical signing of SCC , because of risk of eavesdropping by NSA
- **SCCs to U.S. are now "suspect"**

and then what happened?

[1]link: http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=PL&mode=lst&dir=&occ=first&part=1&cid=9890094).

[2] For more on the verdict : https://gppartners.pl/pl/co-z-uslugami-chmurowymi-po-wczorajszym-wyroku-tsue-uniewazniajacym-transfery-do-usa/

EDPB guidelines or 4 steps to where?

1. **map** data **transfers**
2. **Establish a legal** transfer **tool** (SCC, ad hoc clauses, BCRs, consent, Article 49 GDPR exception).
3. **evaluate the law of the** target country - does it undermine the effectiveness of the transfer tool?
4. **apply additional** protective **measures** (examples in the Annex to the Guidelines)
5. document
6. repeat regularly

"if you still wish to proceed with the transfer, you should look into other relevant and objective factors, and not rely on subjective factors such as the likelihood of public authorities' access to your data in a manner not in line with EU standards."

FACEPALM - and why so? because they figured out that the CJEU logic doesn't pass the probability test according to the disclosure statistics published by the giants?

G+P EDPB - Recommendations for Basic Guarantees

Evaluate whether the law of the destination country undermines the effectiveness of the transfer tool

a) Are the data access rules clear

b) Is the necessity and appropriateness for legitimate access purposes ensured

c) Is there an independent access control mechanism

d) Do people have effective legal tools

Poland would not pass this test.

Consequences of Schrems II - What to do?

Assess the risks to rights and freedoms, including in particular:

- try not transfer content to the US 😂
- Evaluate the potential for interest in our clients or others whose data we send to the U.S. by U.S. services (**NOTE:** EDPB doesn't like that approach);
- assess whether the NSA's eavesdropping on our telemetry or so-called user data poses a real risk to those individuals (it **doesn't**, unless we know we're working with intelligence, counterintelligence, international crime, or states, in which case maybe it does 🤪)
- delegate to a client - inform them of the risks? "If you're a terrorist or you're contracting assassinations in addition to drug trafficking, we advise against using our services because we transfer data to the U.S."
- to see if/how our CP "handled" Schrems II.

Data export disaster

~~Safe Harbor~~ -> Schrems I

Schrems* I -> Privacy Shield

~~Privacy Shield~~ -> Schrems II

Schrems II -> Privacy Shield 2.0 ?

*We're not asking where Mr Schrems gets his funding from

On the way to restore the order


BRIEFING ROOM

Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities

OCTOBER 07, 2022 • PRESIDENTIAL ACTIONS


Press release | 13 December 2022 | Brussels

Data protection: Commission starts process to adopt adequacy decision for safe data flows with the US

https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/

https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7631

GDPR and compliance

Responsibility

Division of roles in the organization

Liability for non-compliance with GDPR

A. **PERSONAL**

- General **criminal**
- **Criminal** obstruction
- **Employee**
- **Disciplinary**

B. **Controller RESPONSIBILITY**

- **Reputational**
- **Business** (contractors)
- **Financial**
- **Civil**: GDPR, tort, contractual
- **Administrative**

Liability in GDPR

Who can be sanctioned? Controller, Joint Controller, Processor, Sub-Processor, Certifier (42, 43 GDPR), Code Monitor (Article 41(4) GDPR) = Organization = Board of Directors

What is he responsible for?

- special care, utmost care, risk principle

How do you protect yourself? - on the following slides

<u>Who will hold us accountable?</u>

- Individual customers
- Former employees
- Competition
- GDPR Law Offices and District Courts
- Large institutional customers
- Important processors (service providers such as call centres)
- Niebezpiecznik.pl, ZaufanaTrzeciaStrona
- Newspapers
- Prosecution
- The President of the Data Protection Authority

When is the threat of penalities real?

If we implement GDPR well, are we safe? **NOT EXACTLY**

- when we're on the front page of the newspaper
- when our personal data leaks (do we fall victim to a hacking attack?)
- ...when someone reports us. Who? Customers, employees, unions. Why? Why not?
- when we process data without a legal basis (e.g. after withdrawal of consent)
- when we fail to handle individual rights (higher penalty)
- when the assistant sends "send to all" instead of "bcc"
- when we unlawfully use a non-EU cloud... (higher penalty).

Administrative responsibility in GDPR

Greater Punishment

Violation of processing principles:

1) **Article 5 principles**
2) **legal grounds for processing under article 6 and 9 GDPR**
3) conditions for consent in Article 7 of the GDPR
4) **the rights of the** data subjects, as referred to in Articles 12-22 of the GDPR (so also the SLA: transparent information, timing, facilitation…)
5) data transfer (export) (Articles 44-49 GDPR)
6) infringement of Member State law obligations under Chapter IX of the GDPR - national data protection rules in employment law - Article 88 GDPR),
7) inobedience of regulators (Article 58(2) GDPR, Article 58(1) GDPR

Smaller Punishment

A lesser fine for violation of other obligations, including

1) **security**
2) records
3) DPO
4) Children's data processing
5) unidentified data
6) **privacy by design, privacy by default**
7) minor breaches not amounting to a breach of the processing rules, and
8) the obligations of the certifier referred to in 42 and 43 GDPR, the obligations of the monitor referred to in 41(4) GDPR

Administrative penalties GDPR

gdps Good Data Protection Standard

- GP Partners

	Controller	Sector	Country	Fine [€]
1	Amazon Europe Core S.à.r.l.	Industry and Commerce	LUXEMBOURG	746,000,000
2	Meta Platforms, Inc.	Media, Telecoms and Broadcasting	IRELAND	405,000,000
3	WhatsApp Ireland Ltd.	Media, Telecoms and Broadcasting	IRELAND	225,000,000
4	Google LLC	Media, Telecoms and Broadcasting	FRANCE	90,000,000
5	Facebook Ireland Ltd.	Media, Telecoms and Broadcasting	FRANCE	60,000,000
6	Google Ireland Ltd.	Media, Telecoms and Broadcasting	FRANCE	60,000,000
7	Google LLC	Media, Telecoms and Broadcasting	FRANCE	50,000,000
8	H&M Hennes & Mauritz Online Shop A.B. & Co. KG	Employment	GERMANY	35,258,708
9	TIM (telecommunications operator)	Media, Telecoms and Broadcasting	ITALY	27,800,000
10	Enel Energia S.p.A	Transportation and Energy	ITALY	26,500,000

Compensation - GDPR 82

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered. - **PRINCIPLE**

2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller. - **PROCESSOR**

3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage. - **PRINCIPLE**

4. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject – **JOINT LIABILITY**

5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2 - **COOPERATION**

Responsibility of Processor and Sub-Processor

Responsibility for:

- Adequate standard of data protection (32 GDPR) - Processor is accountable to the supervisory authority as well as to the data subjects whose data it processes on behalf of the Controller
- Legality of the Controller's instructions
- Documenting the Controller's instructions
- Data misappropriation = „marching” into the Controller's sphere of authority

The GDPR does not differentiate between a „direct procesor” and the "sub-processor" - 28.2 and 28.4 talk about "other processor" = **liability along the entire processing chain**

GDPR reputational liability

Article 34 GDPR

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

The communication to the data subject shall describe in clear and plain language the nature of the personal data breach

If the communication to a data subject would involve disproportionate effort, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

Financial liability - GDPR

- **Cost of incident investigation** - e.g., the cost of an outside law firm conducting an audit of the incident
- **Cost of incident notification**
- Cost of notifying those whose data has been breached

Liability for non-compliance with GDPR

A. **PERSONAL**

- General **criminal**
- **Criminal** obstruction
- **Staff,** including
- **Disciplinary**

B. **Controller RESPONSIBILITY**

- **Reputational**
- **Business** (contractors)
- **Financial**
- **Civil**: GDPR, tort, contractual
- **Administrative**

Division of roles in the organization

Role and responsibility of the DPO

DPO and compliance

When should there be a DPO?

37(1) GDPR

a) public authority or body ...the courts too

b) main activity = processing operations requiring systematic monitoring on a large scale

c) main activity = processing of special categories of data and criminal data on a large scale

What if you don't need a DPO?

Document your analysis of the lack of obligation to appoint a DPO. ...Accountability / WP29 Guidelines

Who can be DPO?

Article 37(6) GDPR

- staff (employee, personal service provider)
- company (outsourcing)

Criteria for selecting the DPO

- professional qualifications, expertise, ability to carry out the tasks referred to in Article 39
- in-depth knowledge of GDPR, knowledge of local and EU data protection legislation
- sectoral knowledge, knowledge of organisations
- IT knowledge
- cybersecurity expertise
- ability to promote a data protection culture in the organization
- regular training

Who cannot - conflict of interest

Article 38.6 GDPR

- management and other substantive positions (decision-making on objectives or means) - WP 29
- organisational conflict (cross-subordination)
- substantive conflict (crossing of duties)
- time conflict (cross availability)
- DPO vs head of compliance or internal audit in a large company? Better not (substantive conflict + time conflict)

Independence

Art. 38 par. 3 sentence 1 GDPR

"The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. (...)"

- The DPO is not bound by instructions from the Controller, including indications of, for example, the interpretation of the provisions of the GDPR;
- Controller partner/advisor relationship.

Status of DPO - prohibition of sanction and dismissal

- Prohibition on the dismissal and sanctioning of DPOs

In accordance with Article 38(3), second sentence, of the GDPR the DPO

"(...) shall not be dismissed or penalised by the controller or the processor for performing his tasks. (...)"

- The prohibition also includes revocation and punishment when refusing to comply with an order of the controller.

Punishment

WP 29 :

- Lack of or delay in promotion (how to promote a DPO?!), impediment to professional development (denial of training), restrictions on access to benefits offered to other employees (discrimination).
- It means DPOs can't be temporarily delegated to other tasks, such as manning the printer in the hallway, much less assurance duties ;-)

Cancellation

- A cancellation should be understood as a termination of an employment contract or a service contract - outsourcing!
- WP 29 only gives reasons for discipline

  e.g. theft, physical and mental harassment, sexual harassment, gross misconduct

How do you normally fire a DPO?

- Demonstrate that one is ignorant, lacks emotional intelligence (antagonistic personality), lacks training
- You can't revoke the DPO because the organization got a penalty
- Better to hire for a definite period

Ultimate subordination

- Direct reporting to the Board.

In accordance with Article 38(3) sentence 3 of the GDPR:

"(...) The data protection officer shall directly report to the highest management level of the controller or the processor.".

- It gives you the opportunity to directly report violations, information about non-compliance with the DPO's recommendations, submit your opinions and reports.
- The DPO is to be assured of being heard.

Tasks of the DPO - Article 39(1) GDPR

- information, education, sensitization, training
- knowledge audits
- monitoring and compliance audits
- recommendations and monitoring of the DPIA
- cooperation with supervisory authority

Responsibilities of the DPO

- The DPO is not responsible for the organization's data protection compliance
- The responsibility still lies with the management
- So, let the management should appoint another person responsible for data protection other than the DPO

DPO and compliance

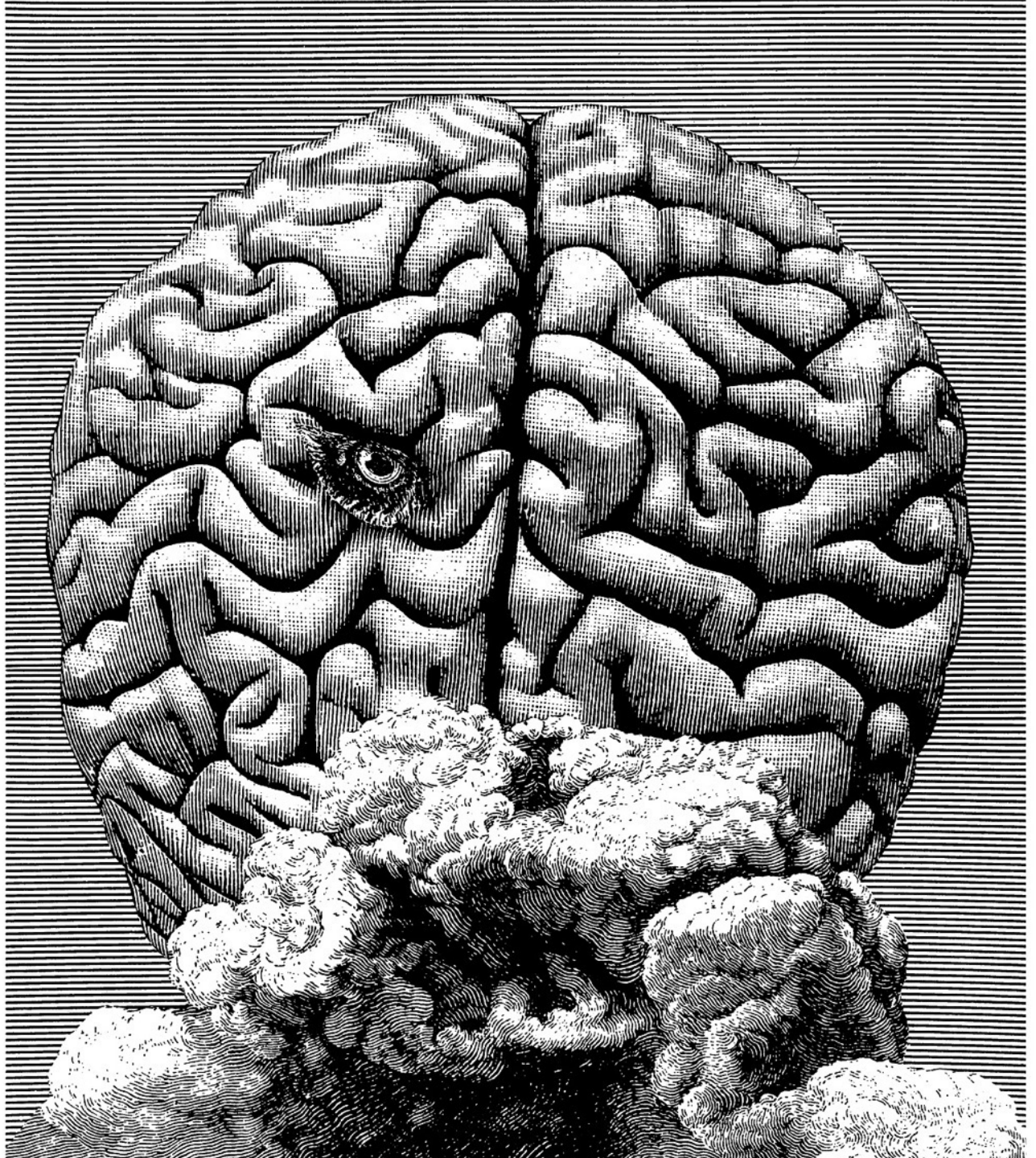
- The DPO should not act as a compliance officer
- DPOs and compliance are supposed to work together
- The DPO is part of the organization's compliance but does not report to the compliance officer and reports to management
- Compliance cannot control the DPO in the performance of the DPO function - independence of the DPO
- Compliance can verify "GDPR compliance" and assess risks

Thank you.

GP Partners

info@gppartners.pl
al. Jana Pawła II 12, 00-124 Warsaw, Poland

maciej.gawronski@gppartners.pl



Training of Lawyers on European Data Protection Law 2 (TRADATA 2)

How to manage the GDPR easier?

Mikołaj Otmianowski

Warsaw, 17 February 2023

The project is co-financed with the support of the European Union's Justice programme

How to manage the GDPR easier?

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

RED INTO GREEN
GDPR compliance trial by DAPR
DAPR

About Mikolaj

Training of Lawyers on EU Law relating to Data Protection 2

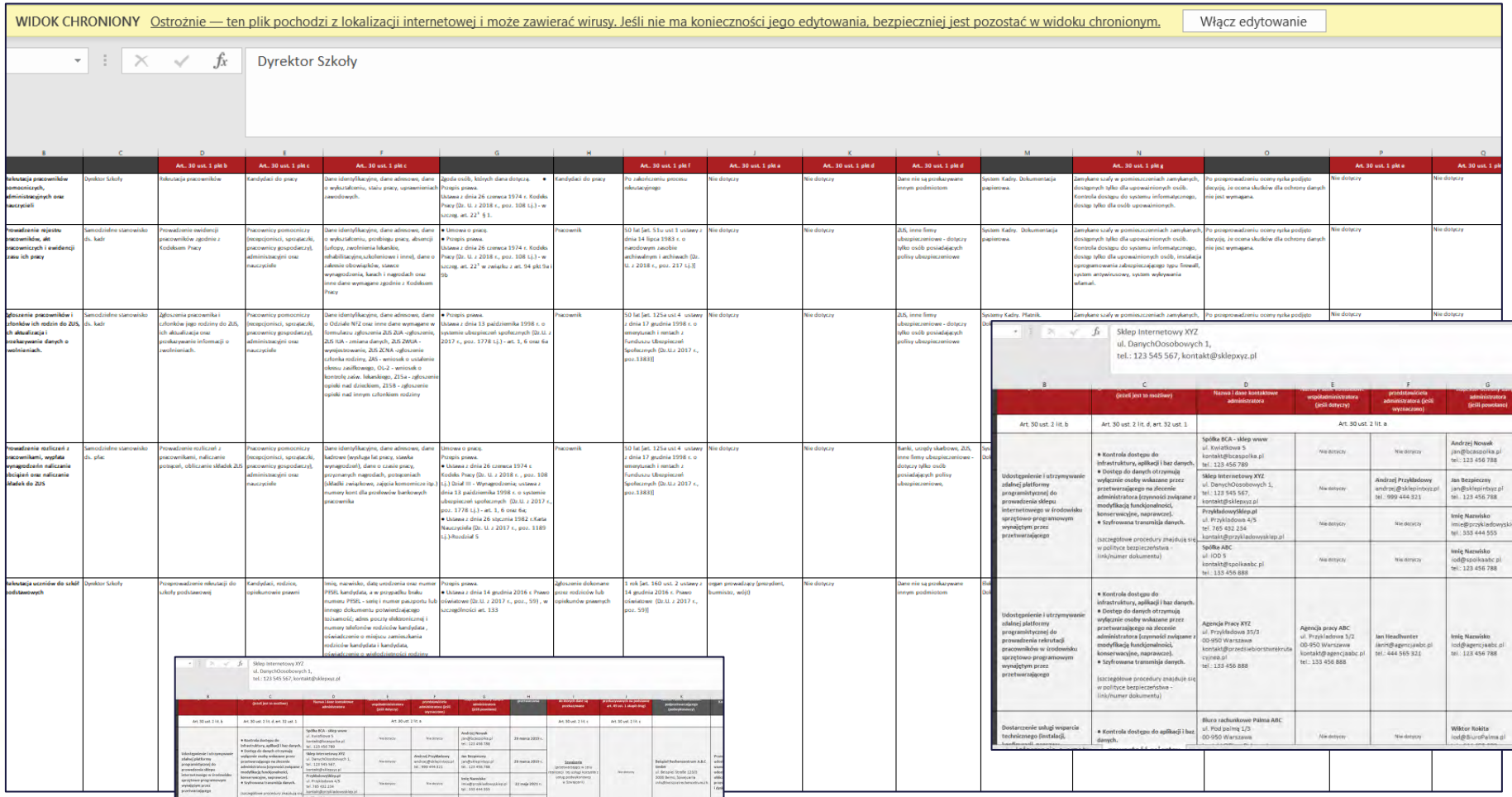
#TRADATA2

I help privacy teams to simplify their life and save time

ROPA and risk assessment in Excel

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

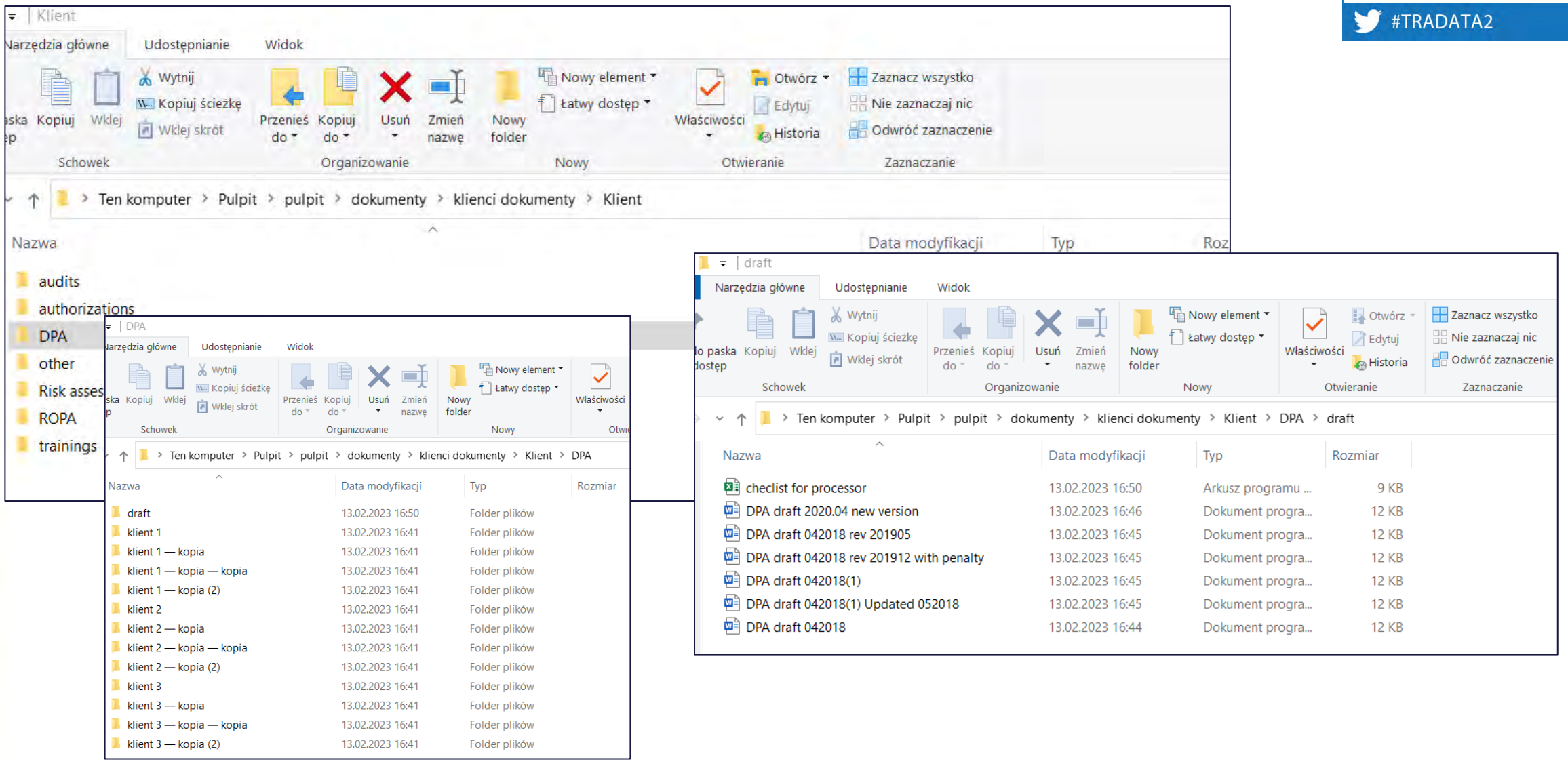


RED INTO GREEN GDPR compliance Trail by DAPR

Archive in Windows

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2



Poland AD 2018

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

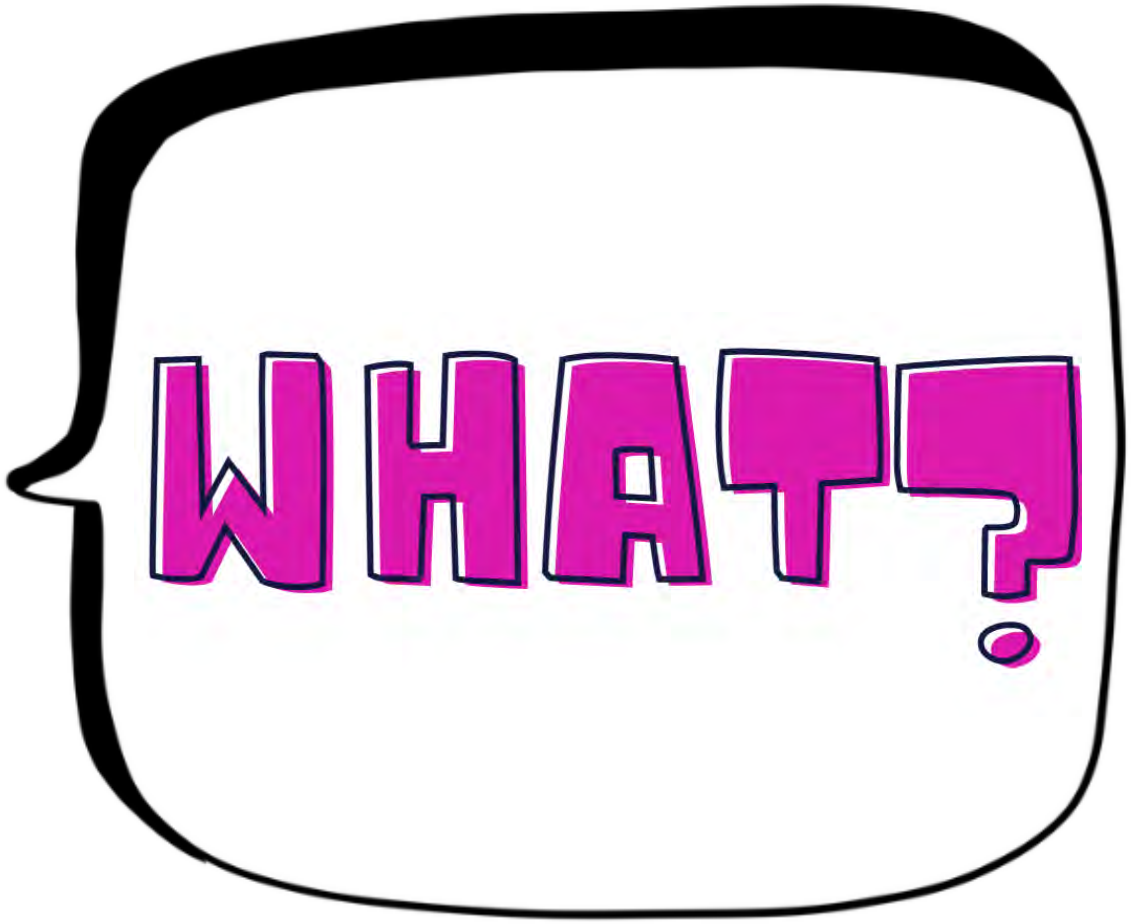
- Fear of penalty
- Pure understanding of the GDPR
- Chaos
- Hardly any comments from DPA
- Common belief „we are excempt to have ROPA”
- DPA everywhere, just in case

A standard „WHAT”?

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

- Risk analysis
- PDCA (Plan, Do, Check, Act)
- Data protection team
- Independent DPO role



RED INTO GREEN GDPR compliance trial by DAPR

DAPR

„Yes, we have implemented the GDPR”

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

- Long, unclear obligation information
- Consent as a main ground on everything
- DPA everywhere
- General trainings
- No process
- No audit
- Trust to subcontractors based on their statement
- Long not verified questionnaire

RED INTO GREEN GDPR compliance trial by DAPR

DAPR

Polish speciality

Warszawa, 13.02.2023
(city and date)

Authorisation No. 1/2023

Under Article 29 of the Regulation (EU) 2016/679 of the European Parliamen
and of the Council of 27 April 2016 on the protection of natural persons wit
regard to the processing of personal data and on the free movement of suc
data, and repealing Directive 95/46/EC (General Data Protection Regulation)
I hereby authorise

Mikołaj Otmianowski
(authorised person's name and surname)

employed as:

DPO
(authorised person's position)

- Współpraca na podstawie umowy zlecenia
- Współpraca z mediami
- Wybór dostawców i zawarcie umowy
- Zakładowy Fundusz Świadczeń Socjalnych
- Zarządzanie flotą samochodową
- Zatrudnienie pracowników tymczasowych - outsourcing
- Zgłoszenie pracowników i członków ich rodzin do ZUS

authorisation is valid from: 03.10.2022
authorisation is valid until: until further notice or until the employment relationship or cooperation relationship expires

Authorisation includes the processing of special categories of data and data relating to criminal convictions and offences.

Authorisation expires upon termination of cooperation between the authorised person and the Controller. Regardless of the above, the Controller may revoke the authorisation at any time.

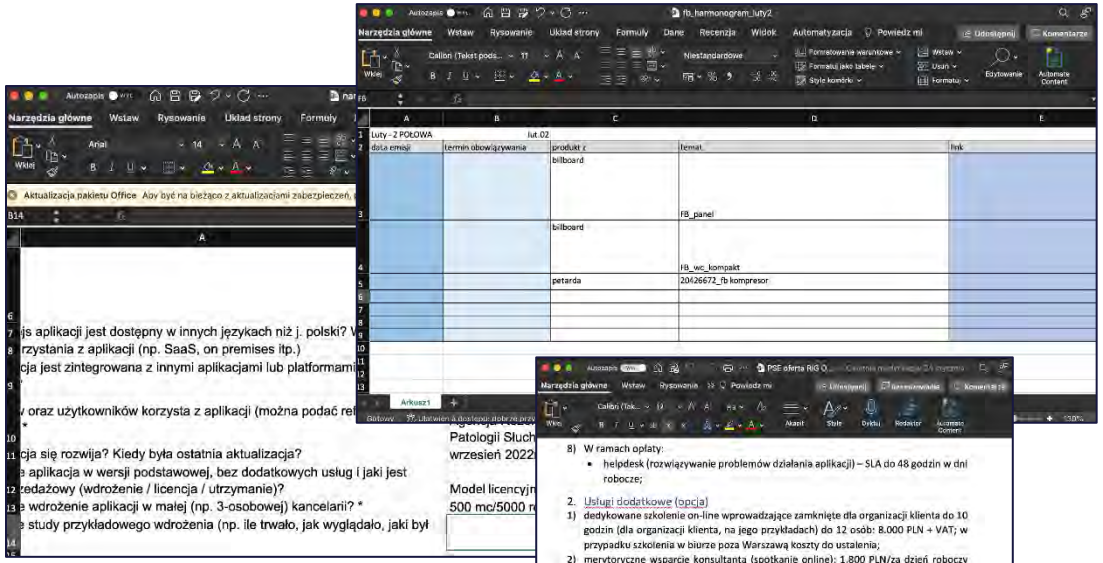
.....
(authorising person's signature with date)

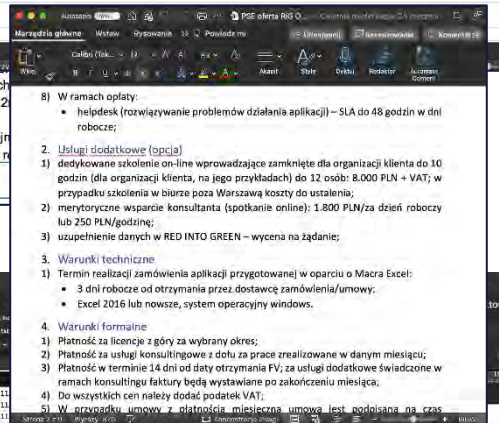
.....
(authorised person's signature with date)

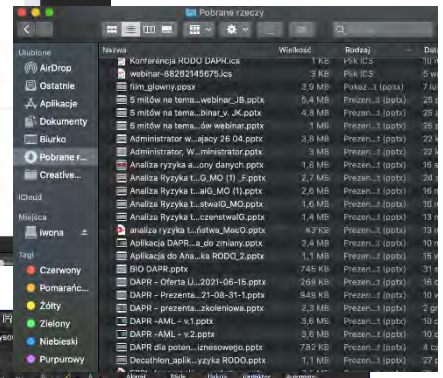
No conclusion, no comparison

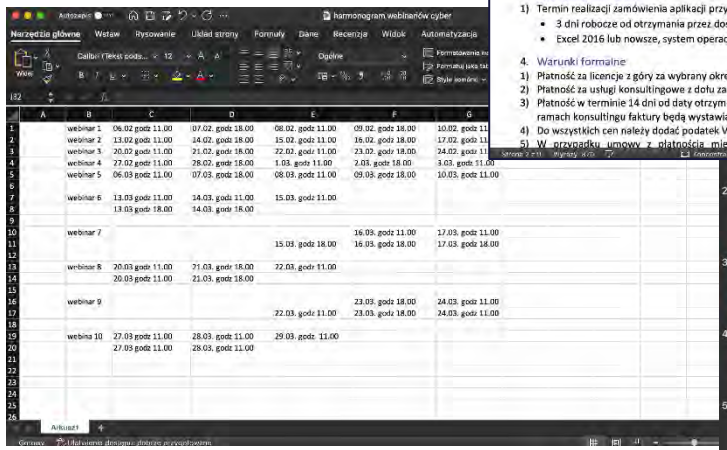
Training of Lawyers on EU Law relating to Data Protection 2

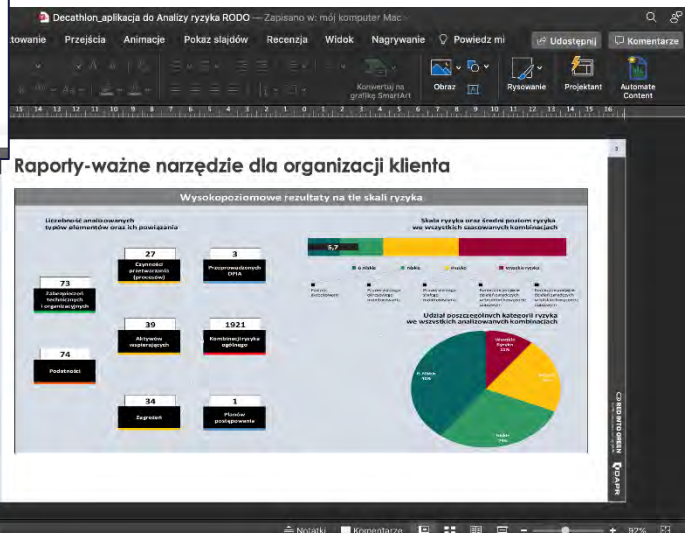
#TRADATA2

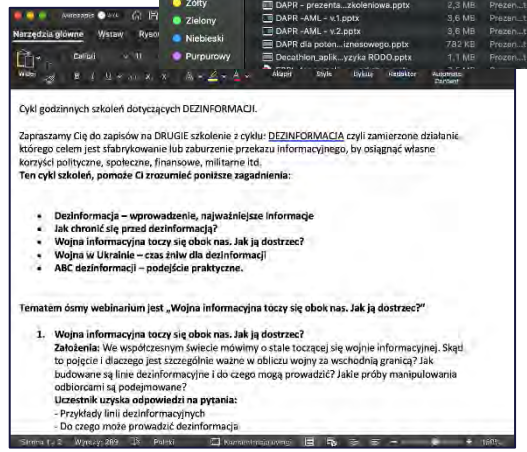








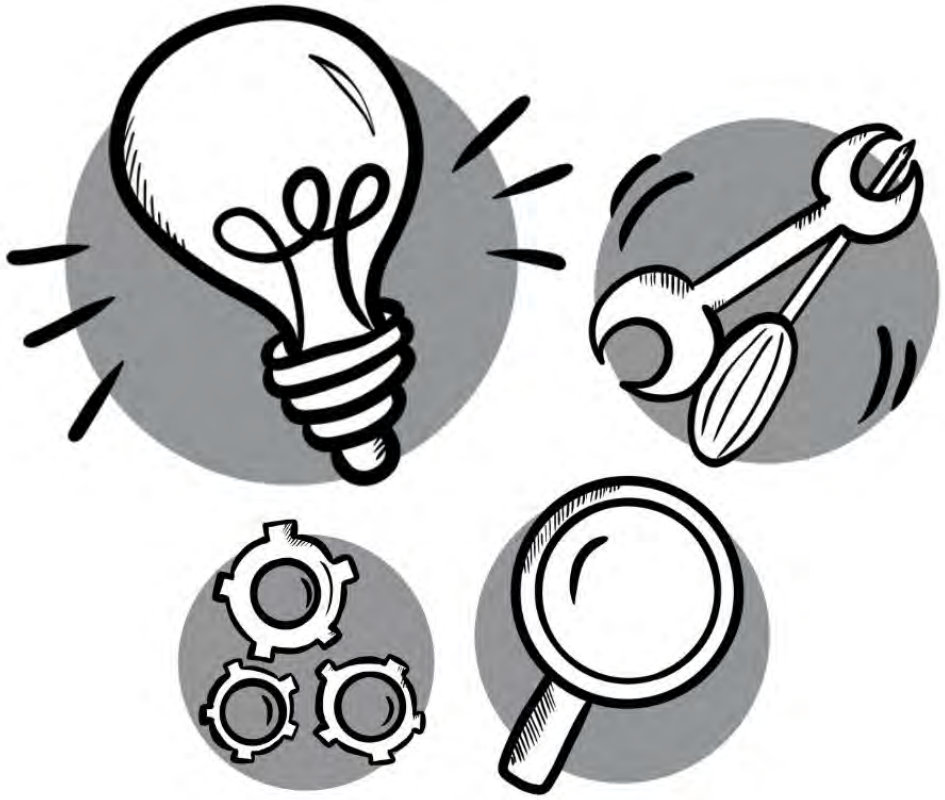




(5 years later) – implications

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2



- The Excel is hard to open, use or update
- Documents become unreadable
- Lack of transparency and order
- No reports or analysis
- Lack or low budget on the GDPR
- One DPO is enough for organization
- Tons of outdated authorisations, DPA and other.

Fear of accounting for the performance of the function for 5 years

Time for software - NOW

- Everybody searches for software
- Many people have the belief that there is nothing

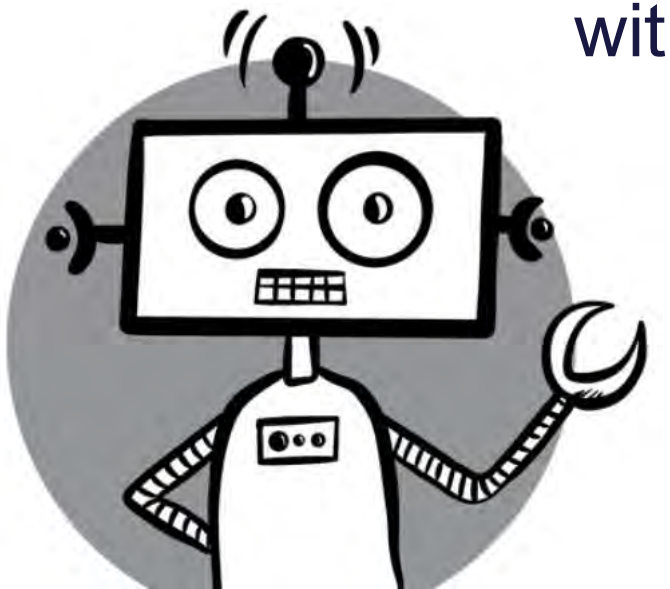
– „I need to clean my desk”

- Fear of the end of cooperation – „I have nothing to give!”

How to make the GDPR management easier?

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2



- Software support
- Engage more business owners
- Connect the GDPR

with cyber security

RED INTO GREEN GDPR compliance trial by DAPR

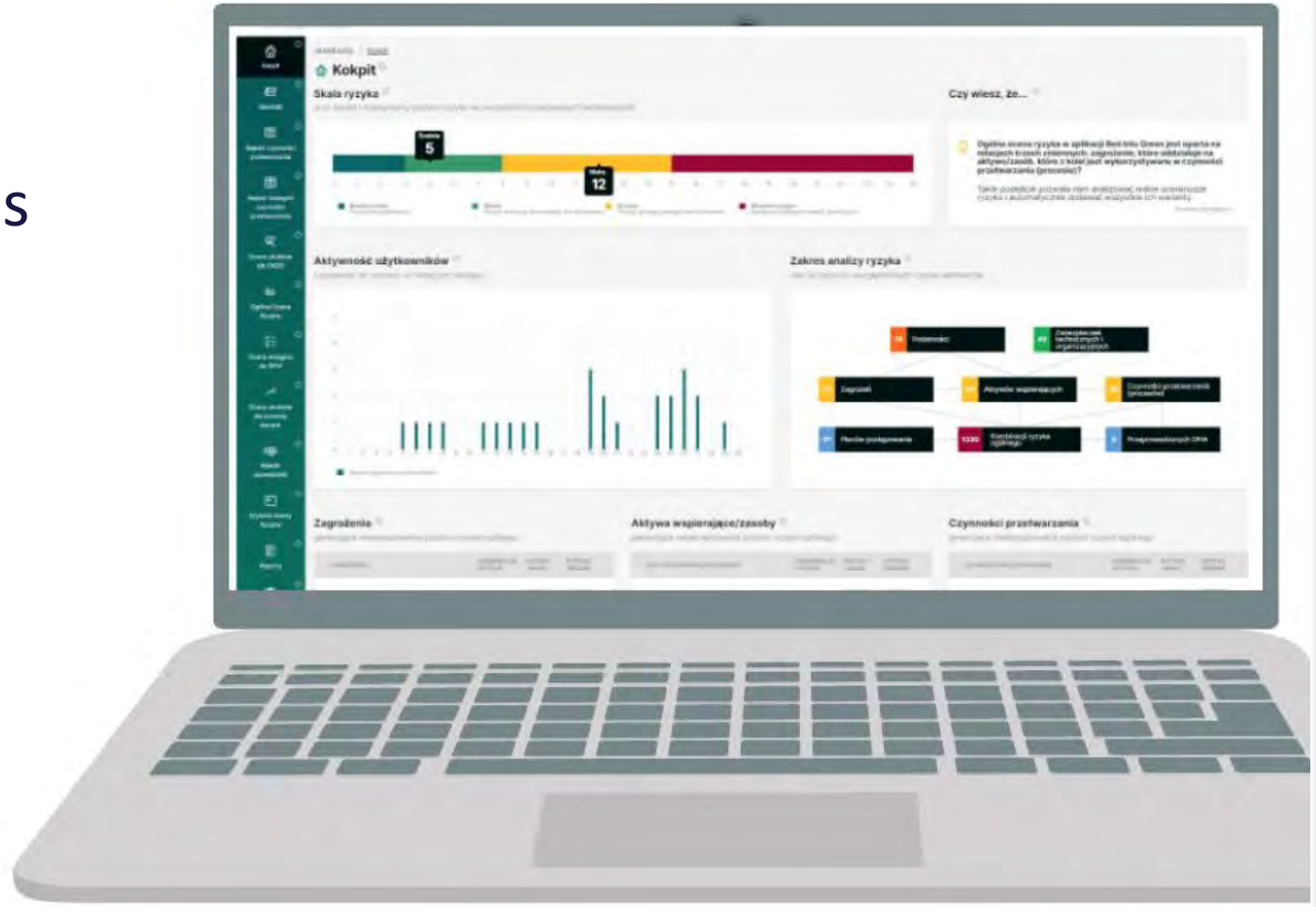
DAPR

What the GDPR software should provide

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

- registry management module
- module to manage risk analysis and DPIA
- audit management module
- training modules
- breach assessment
- reports
- check list and plans



RED INTO GREEN GDPR compliance trial by DAPR

DAPR

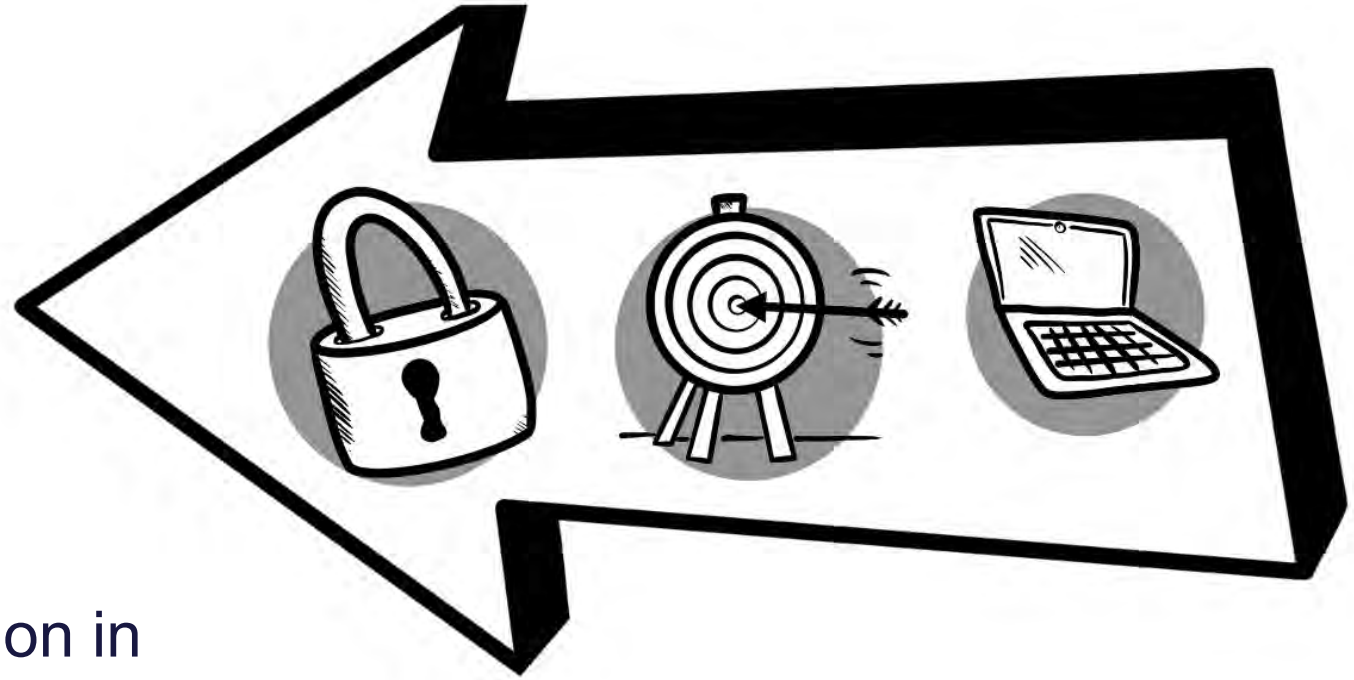
Polish application market for GDPR

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

At least 13 Polish companies produce the software to support the GDPR. Scope is different.

- RED INTO GREEN
- GDPR RISK TRACKER
- PwC
- One trust



- GDPStandard (English version in progres)

RED INTO GREEN

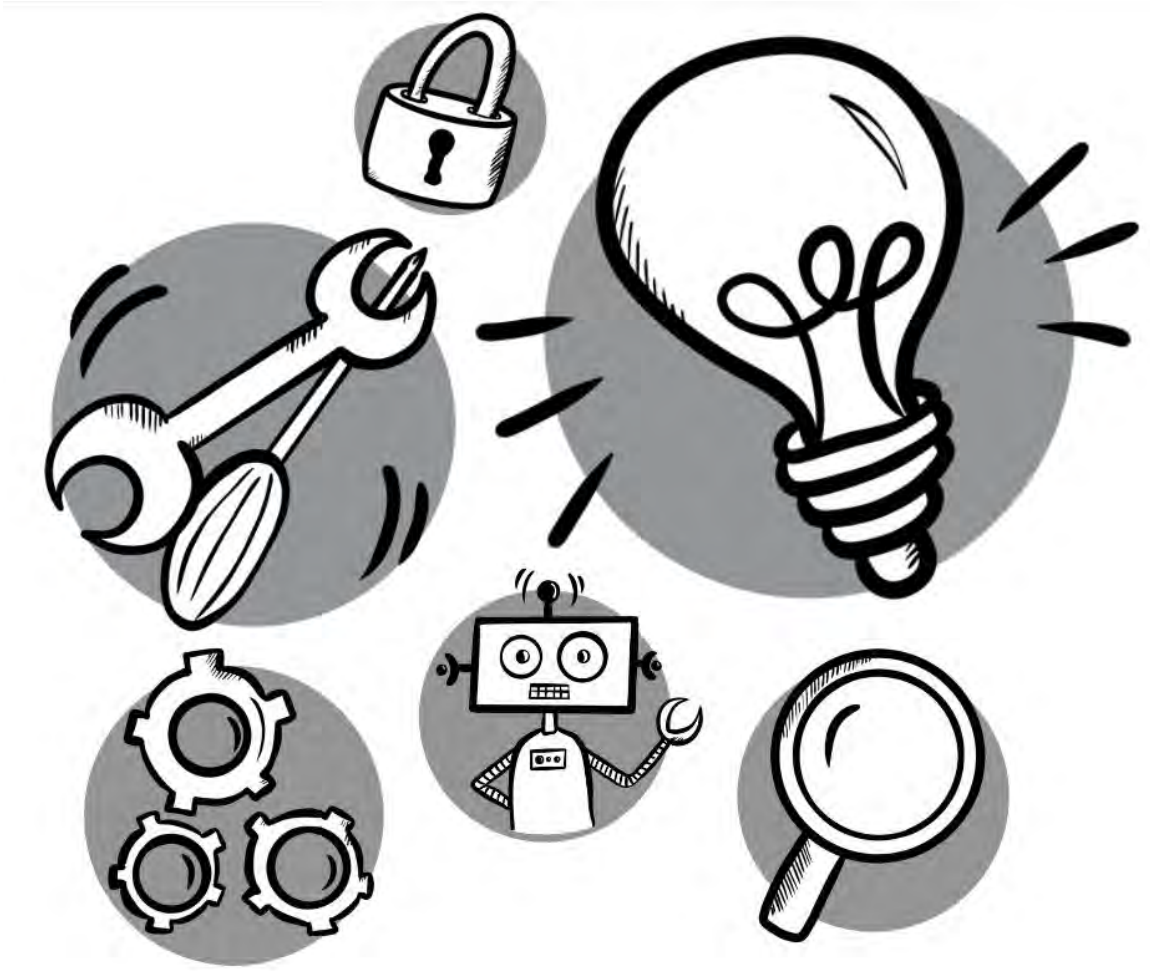
- Methodology based on UODO, ICO, CNIL, DPA, AEPD
- Standard ROPA and complex risk assessment
- Support, drafts of documents
- Key advantage is universal risk assessment methodology ready to use
- One secure place on all the documents and reports
- Report always ready to print
- Update

At the end

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

- All the GDPR issues are in one place
- ROPA is a map of the processes and the GDPR
- Clarity, transparency, linkage of information
- We can combine work done for the GDPR with cyber
- One team working together: IT, DPO and Legal Dept.
- The GDPR is a part of protection of the company
- The whole picture is security and processes, GDPR is a part of security



DPO

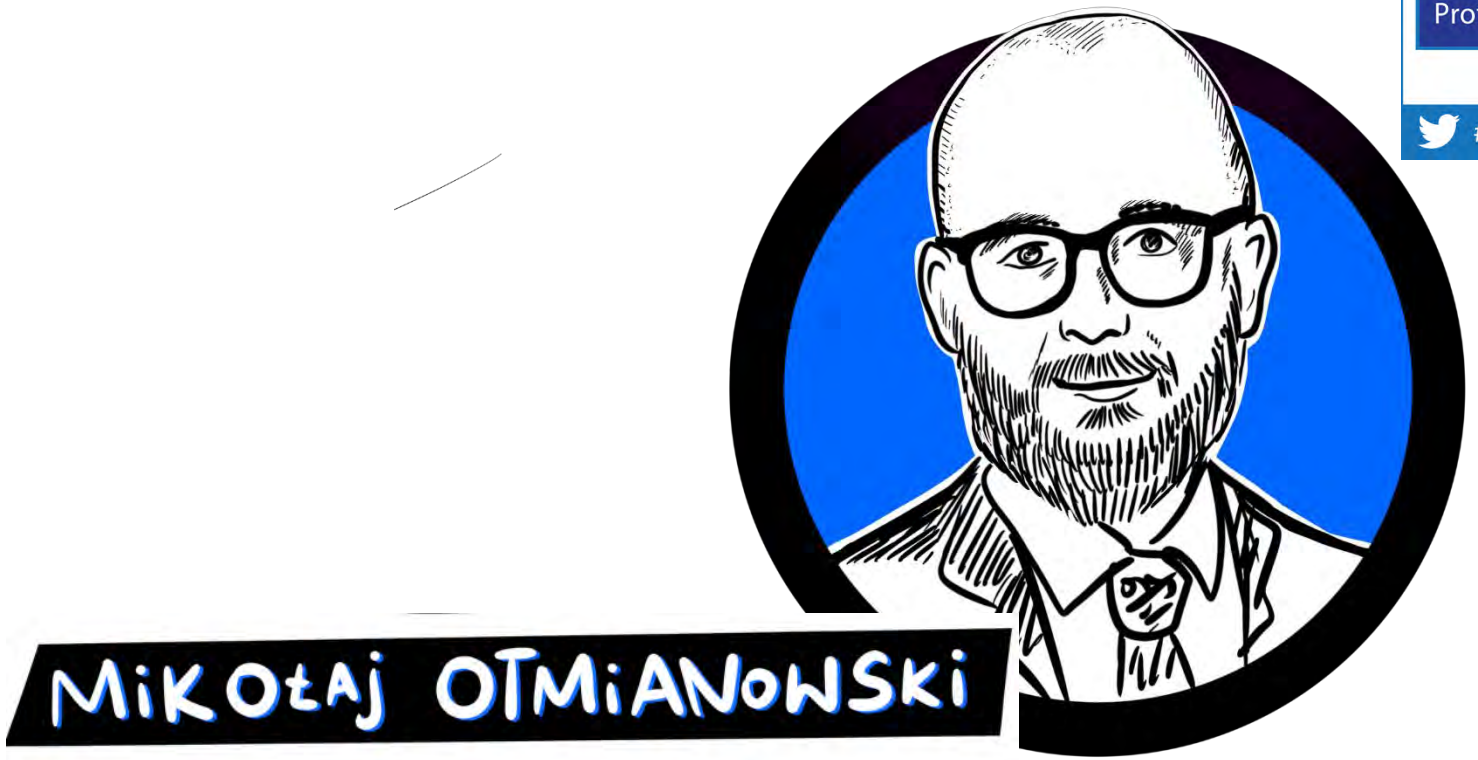
1. see a whole picture
2. role is important as combine with cyber
3. teamwork
4. software support
5. easier to update data and compare it

List of Polish applications for GDPR

1. https://store.pwc.pl/pl/produkty/program-do-rodo
2. https://redintogreen.dapr.pl/
3. https://gdprrisktracker.pl/
4. https://gdpstandard.com/pl/
5. https://odo24.pl/dr-rodo#cennik
6. https://inspektor365.pl/
7. https://rodo-online.eu/
8. https://kryptos72.com/
9. https://rodoprotektor.pl/
10. https://iodinspektor.pl/
11. http://dlaiod.pl/program-rodo/
12. https://ioda.legal/
13. https://sodo.com.pl

Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2



DAPR
Data Protection

RED INTO GREEN
GDPR compliance tool by DAPR

Thank you for your attention

Training of Lawyers on European Data Protection Law 2 (TRADATA 2)

The Intersection of Competition Law and Data Privacy

Natalia Cieloch

Warsaw, 17 February 2023

The project is co-financed with the support of the European Union's Justice programme

Agenda

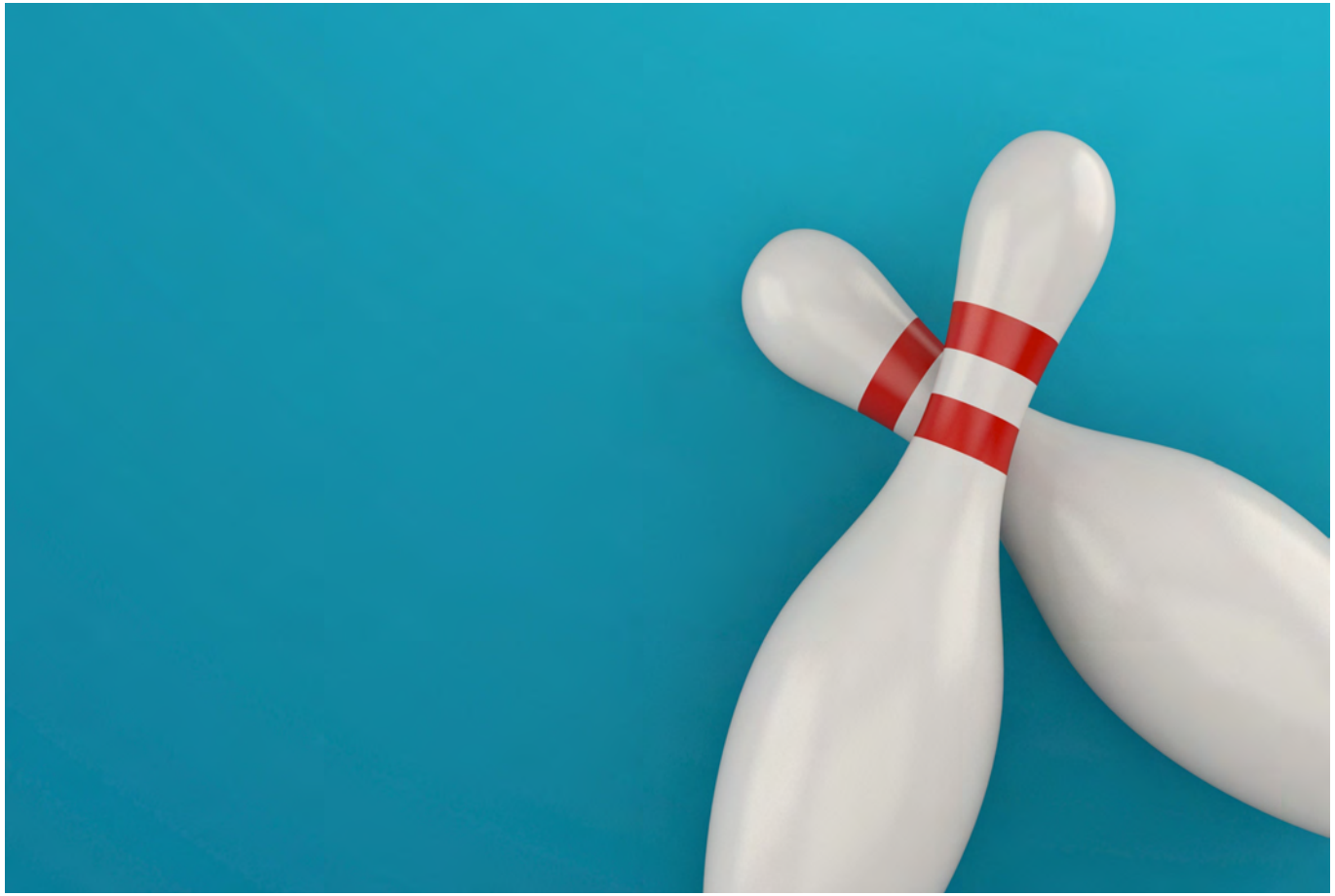
Training of Lawyers on EU Law relating to Data Protection 2

#TRADATA2

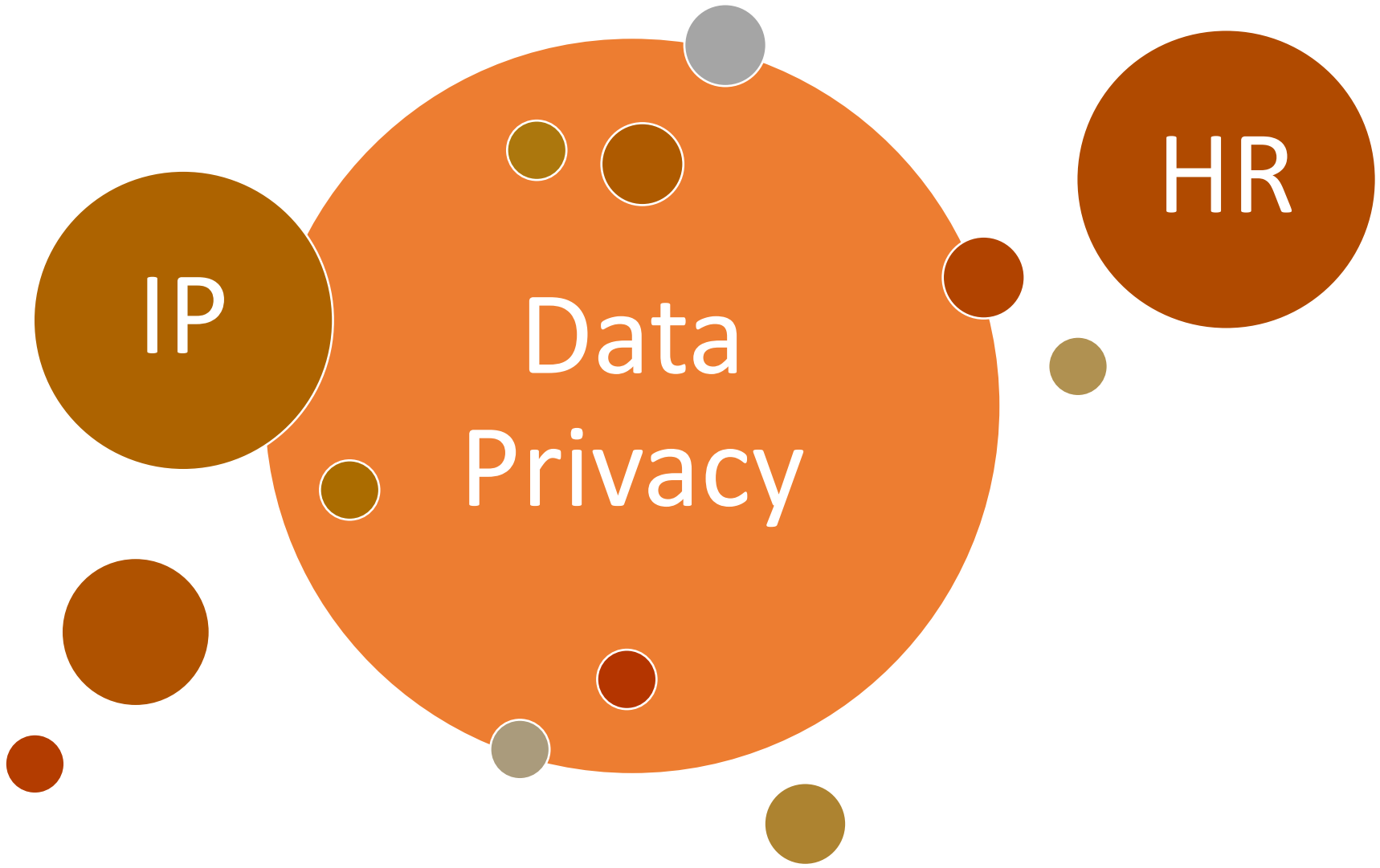
- Competition law – basic concepts
- Intersection with other areas of law
- Recent actions taken by the EC and EU NCAs
- Bundeskartellamt and German FB case (C-252/21)

Pillars of Competition law

Not only about competition law...

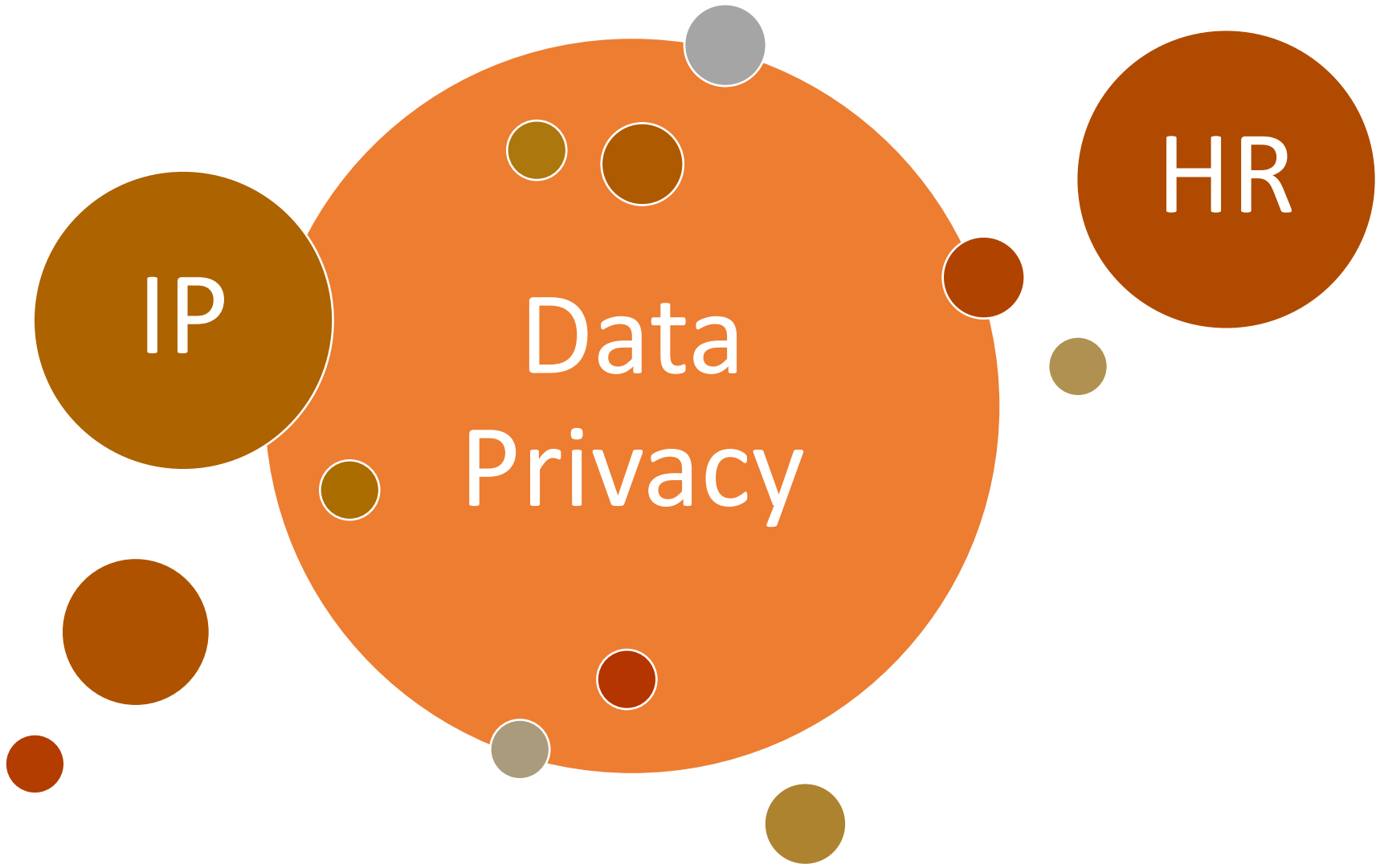


Competition law intersects with...



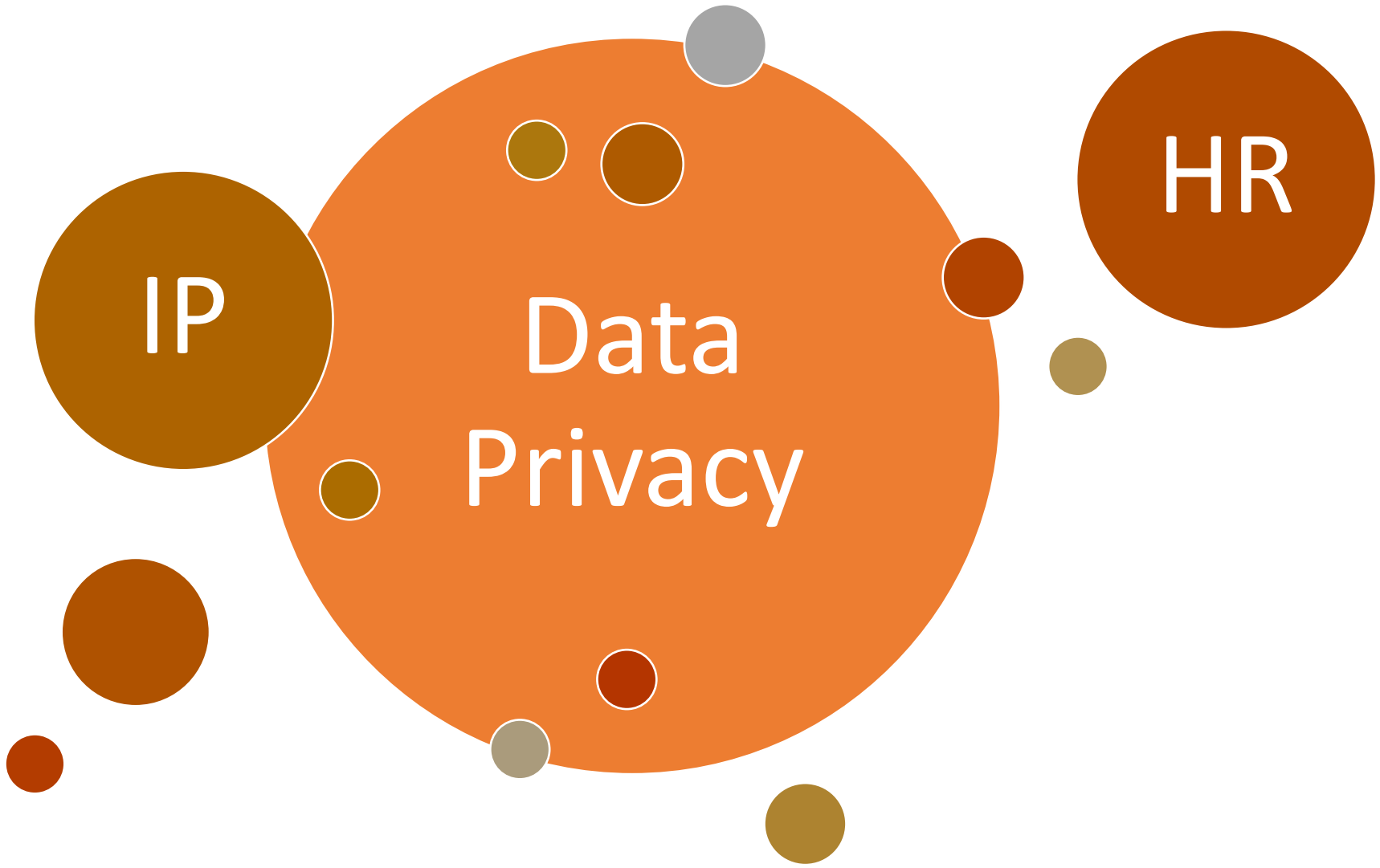
Competition law intersects with...

2008-09
2019



Competition law intersects with...

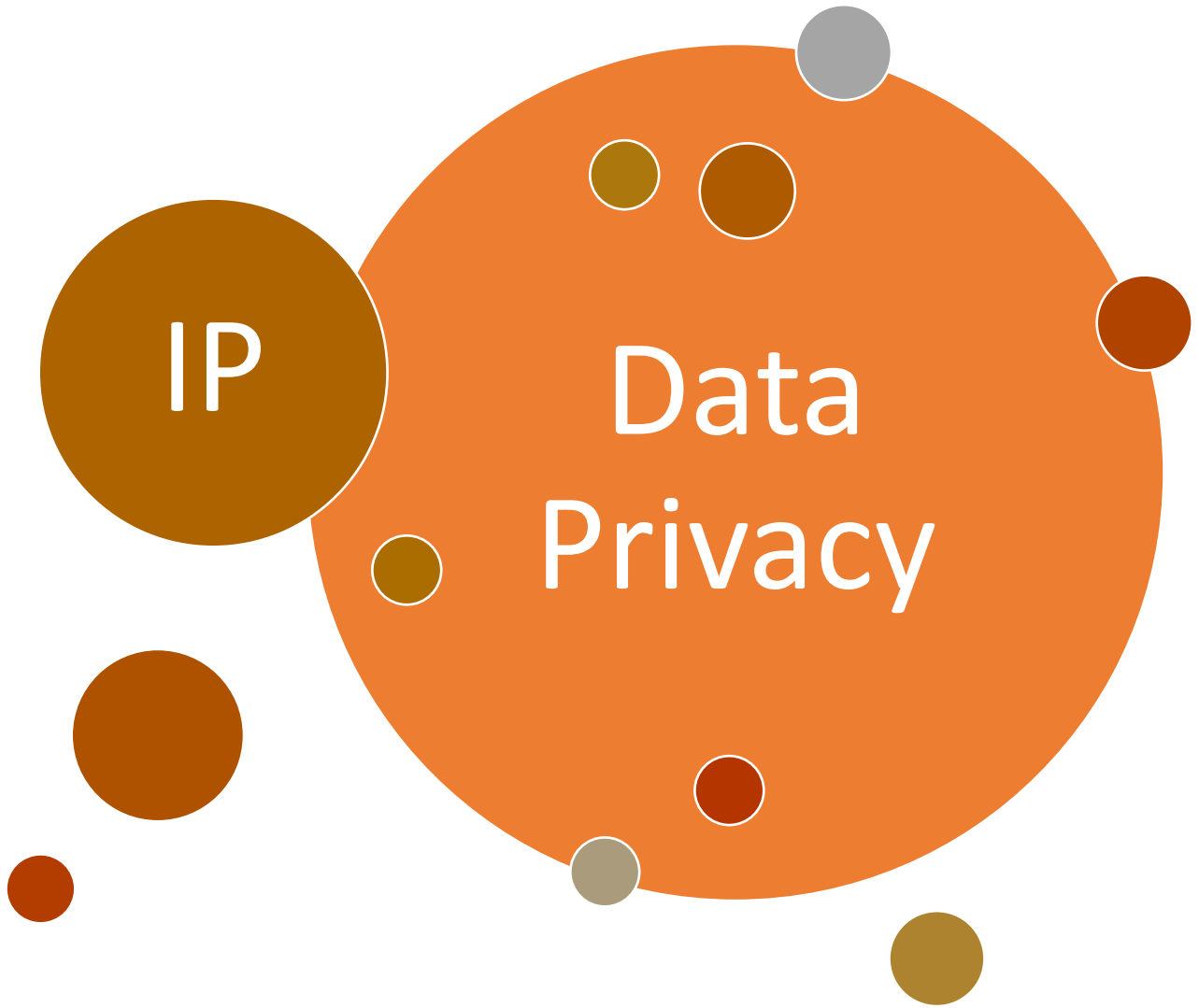
2008-09
2019



2016
2017

Competition law intersects with...

2008-09
2019



2016
2017

2021: EC - Google
2021: UOKiK – Apple
BKA: Apple; German
FB case (C-252/21)

1# How privacy is relevant for competition law?

Separatist view:
Asnef-Equifax case

Competition law
& privacy:
complementary not overlapping

Main concern:
confusion

2# How privacy is relevant for competition law?

Integrationist approach: *German facebook case*

Competition law & privacy: **could be integrated**

Main concern:

BKA vs. German FB/META case (C-252/21)

FB’s violation of GDPR constituted an abuse of dominance

META: NCA can’t enforce GDPR

Advocate General's Opinion

(20th September 2022)

*„(…) while the competition authorities **do not have** direct jurisdiction regarding the endorsement of the GDPR, the EU's data privacy regulation,* ***they may still consider them in exercising their powers."***

Q&A

All comments expressed in this presentation are the author's personal opinions

Contact: natalia.ewa.cieloch@gmail.com