

ONLINE TRACKING - PROBLEMS AND LEGAL REMEDIES

Academic Training Lecture Regular Programme (CERN)

May 10th, 2023

Stefano ROSSETTI – data protection lawyer at noyb

LINE UP

- I. Presentation of *noyb*
- II. GDPR, and Other Applicable Laws
- III. NGOs and organisations and the GDPR
- IV. Enforcement projects
- V. Other projects

I. PRESENTATION OF *NOYB*

noyb?

= *None Of Your Business*

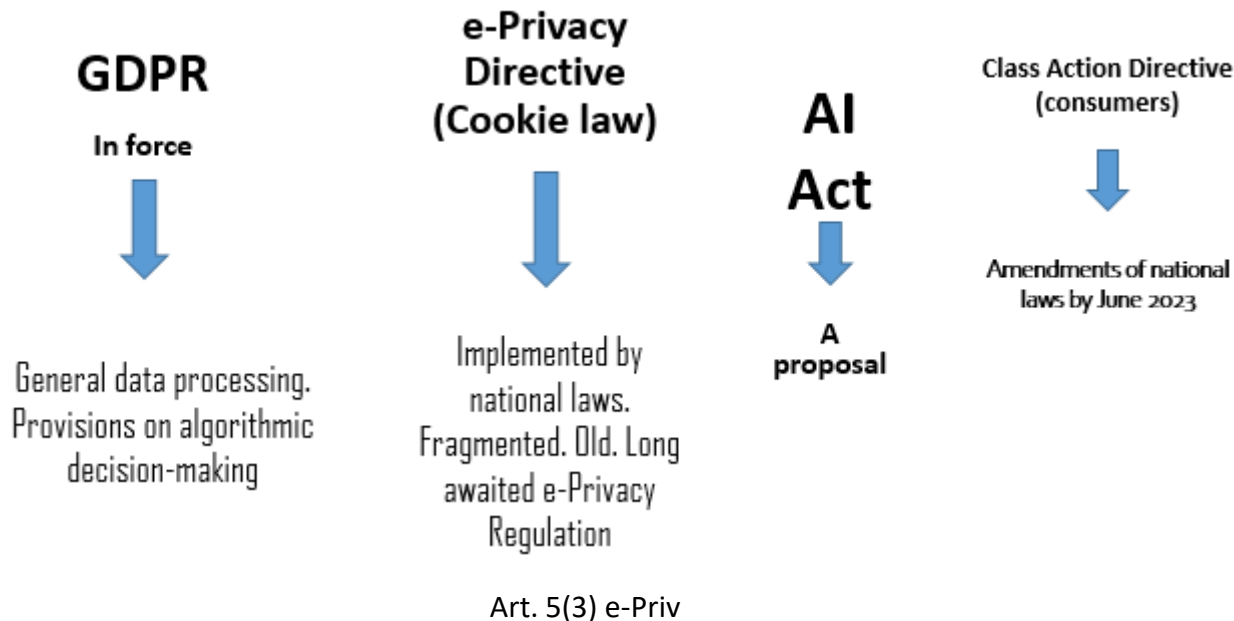
European Center for Digital Rights

- Not-for-profit organisation
- Independent
- Created by Max Schrems
- Founded in May 2017
- Based in Vienna
- 15 people, including 9 data protection lawyers from several jurisdictions
- About 3,300 supporting members at the moment who contribute around 240 000 € per year
- Additional funding comes from institutional members and project funding by public and private institutions (eg EFF). We also receive single donations and sponsorships on a non-regular basis

I. PRESENTATION OF *NOYB*

- fills a structural gap in private sector privacy enforcement
- cooperate with existing NGOs and groups in the fields of privacy, IT security and consumer protection
- support businesses that seek to comply with the law
- not directly involved in issues of government surveillance
- raises public awareness
- provides legal assistance to members

II. GDPR, AND OTHER APPLICABLE LAWS



II. GDPR

- It is a Regulation → direct application;
- GDPR, in General
 - Recital 11: «*Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data*»
- An attempt to strengthen control over personal data processing through controller's **obligations** and individual **rights**
 - **Data processing obligations (on controllers and processors)**
 - **Principles** (Transparency, Lawfulness, Fairness, Proportionality, Security → Article 5 GDPR)
 - **Specific provisions** (Privacy policies, Legal basis, Data Prot By Design, Data Breaches)
 - **Data subjects rights**
 - Access, deletion, rectification, right not to be subject to algorithmic decisions

II. GDPR (LAWFULNESS)




- Principle: Personal data shall be: (a) processed lawfully [...] (Art. 5)
- Application: Legal grounds, or consent, contract, legitimate interests, legal obligation, and a few others (Art. 6)
- Consent, must be freely given, specific, informed and unambiguous (cookie banners)
- Contract, processing must be necessary for the performance of the contract (hotel reservation, e-commerce purchases)
- Legitimate interests, balancing exercise, key word: overweight

II. GDPR (TRANSPARENCY)






















































































- Principle: Personal data shall be processed: (a) in a **transparent** manner[...] (Art. 5)
- Application: The controller shall take appropriate measures to provide any information referred to in **Articles 13** and 14 and any communication under **Articles 15 to 22** and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child (Art. 12)
- Application: so called, “privacy policies”, documents providing general information on the processing, for instance, the legal grounds, purposes, categories of data required, recipients, sources (Art. 13)

II. GDPR (TRANSPARENCY) - ELEMENTS IN A PRIVACY POLICY

Overview of some of the information requirements of Article 13 GDPR

Legend:  means generally satisfactory.  means only partially satisfactory.  means not satisfactory.

Netflix & Chill – What streaming services do while you’re on the couch

Elements according to Article 13 GDPR	Amazon Prime (Amazon)	Apple Music (Apple)	DAZN	Flimmit	Netflix	SoundCloud	Spotify	YouTube (Google)
Name and contact details of the controller								
Contact details of the data protection officer			Not applicable	Not applicable				
Purposes of the processing								
Legal basis of the processing								
If legitimate interests: What is the interest?	Not applicable							
Link between purposes, legal basis, and categories of personal data								
Recipients of personal data								
Transfer of personal data outside the EU/EEA								
Retention period								
Information about GDPR rights								
Existence of automated decision making incl. profiling								

II. GDPR (USERS RIGHTS)

Underlying idea: **control over our personal data**

- Right to access (Article 15 GDPR)
 - **Keystone** of entire European data protection framework. Two main elements: **Information**, clear, easy-to-understand, tailored to the specific case, among the others, on Purposes, Categories, Recipients, Retention period, Logic involved in the Algorithms + **Copy** of All Data Undergoing processing (cookies, usage data, online actions, video and audio recordings, biometric data, performance data and all profiles controllers can create based on the above)
- Right to rectification (Article 16 GDPR)
- Right to erasure and right to be “forgotten” (Article 17 GDPR)
- Right to object to the processing (Article 21 GDPR)
- Right not to be subject to automated decision making (Article 22 GDPR)

II. GDPR (USERS RIGHTS)

- **In practice**, Request by the data subject (facilitated – Article 12(2) GDPR) → Response by the controller (clear, concise, tailored, in other words, *transparent*) **BUT** controllers are generally **reluctant to comply**
- **Example: AdTech**
 - As we move around on the internet and in the real world, we are being continually tracked and profiled for the purpose of showing targeted advertising. In this report, we demonstrate how every time we use our phones, a large number of shadowy entities that are virtually unknown to consumers are receiving personal data about our interests, habits, and behaviour.
 - Many actors in the adtech industry collect information about us from a variety of places, including web browsing, connected devices, and social media. When combined, this data provides a detailed picture of individuals, revealing our daily lives, our secret desires, and our most vulnerable moments.
 - Exercising GDPR rights and more generally controlling personal data in this field is rather **difficult**, plenty of reasons: controllers deviate from user's consent (forcing them to accept contracts, for instance); or make it look like users are consenting while in fact they are not; trackers are buried in software and OOSS, oftentimes neither authorized nor announced; data is used in the context of complex, obscure algorithmic decisions, over which very little transparency is provided;
- **Problem → Information and control asymmetry**
- **Solution (or part of it) → not only legal, but also organizational...**

III. ORGANISATIONS AND THE GDPR

Underlying idea: **structural problems need structural solutions**

Article 80.1 GDPR explained

Who can act ?

- not-for-profit body, organisation or association
- properly constituted in accordance with the law of a Member State
- statutory objectives which are in the public interest
- active in the field of the protection of data subjects' rights and freedoms

What can they do ?

- to lodge the complaint on his or her behalf
- to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf,
- to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.

***noyb* uses this possibility to address some of the issues mentioned before**

IV. ENFORCEMENT PROJECTS

#1 Using contract instead of consent to process data for profiling purposes

- Complaints against Meta: Whatsapp, Google, Facebook and Instagram
- No lawfulness and very little transparency;
- Confusion between consent and contract;
- Filed in Austria, moved to Dublin → OSS mechanism
- DPC was very slow, very → first draft, ridiculously low fine → other DPAs disagreed → EDPB overturned entire decision, imposing much harder approach → DPC reluctant but in the end...
- Fine against Meta (Instagram, Facebook, WhatsApp)
- Still too low, not dissuasive, not proportionate

IV. ENFORCEMENT PROJECTS

#2 Giving the user the impression of consenting (Cookie Banners / Dark Patterns)

- AdTech ecosystem – user online tracking
- Trackers are essential → the Industry needs Cookies, desperately but Article 5(3) e-Privacy directive requires consent, right?
- (their) « **Solution** »: Cookie Banners, shaped and presented in ways that people just give their consent without thinking. Examples: No Reject All; Different Colours; Scroll down to «accept»;
- Is this **real** consent? Freely given, specific, informed, unambiguous?
- Hardly so... noyb decided to take action:
 - (1) Developed Ispettore, our software that scan CMPs settings; Outcome → LOTS of websites used settings pointing to dark patterns approach;
 - (2) Violators list (most visited websites in Europe) → Cease and desist letter (Ispettore assisted) → if violation not fixed, filed complaints (500 circa)
 - (3) EDPB task force recently clarified what constitute dark patterns; Companies generally fix their issues or get fined; + Spill over effect.

IV. ENFORCEMENT PROJECTS

#3 Mobile Advertising Identifiers

- Reminder: trackers are **key** to the system → not only cookies but **also Mobile Identifiers** generated by the operating system or the software we are using;
- **Automatically installed**, oftentimes not announced in the privacy policy, accessed by both OS/software developers and third parties (music streaming apps, dating, language exchange, gaming)
- Just like a cookie it is used in the AdTech to profile and store information about users
- Looks like a cookie, smells like a cookie, works like a cookie: **probably it is a cookie!**
- Art. 5(3) e-Privacy is **technologically neutral**, so applies to Mobile IDs as well!
- Filed complaints against different companies in Germany, France and Spain. Waiting for results but difficult due to ePrivacy inconsistent transposition

IV. ENFORCEMENT PROJECTS

#4 authentication issues (cookie-based authentication)

- Normal case, in order to exercise a GDPR right (access, erasure, objection), a data subject has to authenticate with the controller (example: landlord in case of change of surname → ID card)
- But, in the AdTech, this is hardly possible. DS identity is the cookie, mobile ID, or other unique value. In such cases, the most important, the matter becomes much more problematic.
- Practical experience in the sector shows that controllers, who, as we have seen, are perfectly capable of identifying us for more or less announced and/or unlawful purposes, put **considerable obstacles** in the way of exercising the GDPR right.
 - Examples: communicating additional details (such as residential addresses), filling out forms with a signed signature (biometric data), and presenting copies of identity documents (biometric and, in some cases, sensitive data).
- Such a practice is openly **discouraged** by the EDPB and majority jurisprudence → **Litigation/complaints**: violation of Art. 12 (facilitation)/15 (access) /25 (bdbd)

IV. ENFORCEMENT PROJECTS

#5 Workplace Surveillance

- Amazon and platform workers subject to reckless surveillance;
- Suspect of entirely automated decision-making
- Very little transparency on data processing
- UniGlobal contacts noyb and asks if GDPR can help;
- Official reports show, physical harm, pace too high; Surveys and consultation w/workers: depression; inability to cope; fear of being dismissed if performance expectation is not met; fear of algorithms;
- Strategy: Access Request, with a view to obtain clearer information and rule out ADM → Art. 22 GDPR (right not to be subject to ADM)
- Response insufficient, workers may go to court

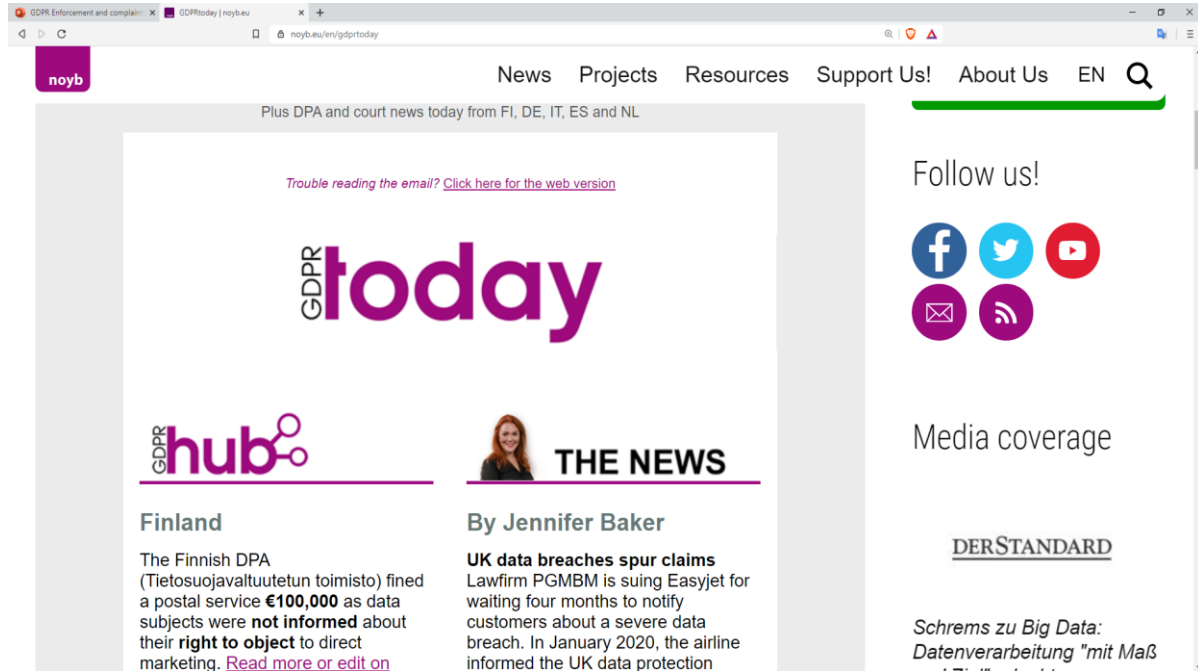
IV. ENFORCEMENT PROJECTS

#6 when the system fails: DPA's inertia and court actions

- Violation → Investigation
- In theory, matters should be handled quickly, especially if they are not complex (ex, a simple Access Request)
- In practice, it often takes forever for certain DPAs to decide. Examples: streaming complaints filed in Jan 2019.
- Why?
 - Few Procedural Rules in the GDPR, so many crucial elements left to the Member States legislative Autonomy
 - No clear deadlines, especially in case of cooperation;
 - Data subject's Rights in case of inertia are not clear;
 - Procedural rights, FOIA, Access to Documents often limited by company interests;
- Solutions, noyb «recipe»:
 - Strategic litigation vs. inertia → Swedish case, Luxembourg, Netherlands
 - New procedural rules to fill the gap

V. OTHER PROJECTS

- *GDPRtoday*



V. OTHER PROJECTS



SecuredropboxDropBox

GDPR Enforcement and complain... x SecureDrop | noyb.eu

noyb.eu/en/securedrop

noyb

News Projects Resources Support Us! About Us EN Q

HOME > SECUREDROP

SecureDrop

SecureDrop is an anonymity tool for journalists, lawyers and whistleblowers. As a source, you can use our SecureDrop installation to anonymously submit documents to our organization. Our lawyers use SecureDrop to receive source materials and securely communicate with anonymous contacts.

SecureDrop

What is SecureDrop?

SecureDrop is an anonymity tool for journalists and whistleblowers. As a source, you can use our SecureDrop installation to anonymously submit documents to our organization. Our lawyers use SecureDrop to receive source materials and securely communicate with anonymous contacts.

When should you use SecureDrop?

It usually takes us some effort and time to retrieve documents from the SecureDrop system.

Support us!

noyb funding goal

79 %

BECOME A MEMBER!

Follow us!

QUESTIONS ?

www.noyb.eu

Twitter – Facebook - LinkedIn

Stefano Rossetti

sr@noyb.eu