



# Web data analytics under scrutiny of domestic EEA regulators

---

## Enforcement of the Schrems II judgment

On January 13 and February 10, 2022, the Austrian and French Data Protection Authorities, respectively, published their decisions targeting EU-based domains which utilized Google Analytics, declaring data transfers to Google Analytics unlawful. The decisions follow 101 complaints filed by noyb.eu to the EEA data protection authorities, seeking to enforce the Schrems II judgement.

### The most important consequences of the recent decisions:

- use of the US-hosted web services, such as Google Analytics, by EEA-based websites poses increased risk of regulatory scrutiny;
- data transfers to 'non-adequate' countries outside the EEA should be verified regarding their reliance on the appropriate safeguards or well-justified legal exemptions.

Concluding, having regard to the most recent regulatory activity, each organization transferring data to countries outside the EEA should verify the currently used transfer mechanisms in terms of legal, technical and data security safeguards.

### What necessary actions must exporters take?

1. Identify utilized web services which result in data transfers outside the EEA.
  2. Assess the factual elements of the data transfers: what data is transferred, whether any data transferred can be deemed personal data (even in the pseudonymous sense), and whether personal data encryption effectively anonymizes data.
  3. Analyse, in legal and technical terms, whether existing additional measures address country-specific circumstances, such as information request from the public authorities and existing practice/technical capabilities of intelligence agencies.
  4. In light of regulatory decisions and Schrems II judgement, analyse whether transferred personal data can be lawfully accessed by the 'other person' in accordance with the GDPR (i.e., intelligence agencies), assessing the likeliness of such occurrence.
  5. Document the above-mentioned analyses in the event of an inspection by a supervisory authority.
-

## DWF's support

Due to the combination of knowledge and extensive experience in the fields of data protection, risk management, compliance and technology, DWF's Legal's Data Protection team has developed a **unique methodology** supported by a **dedicated IT solution** that allows you to perform **inventory, assess and manage transfers** of personal data in organizations. In addition to the methodology and the IT solution our support may also consist of:

- **assistance in inventory** and assessment of transfers and **recommending measures** to mitigate both legal, technical and organizational risks thanks to the support of specialized DWF's Cybersecurity teams;
- ongoing support, thanks to the DWF global legal business, consisting of **monitoring legislation** in the field of personal data protection all over the world.

## Who we work with

Our clients range from FTSE100, Fortune 500, multi-national and household names, from the public and private sector.

Clients are at the heart of what we do. They lead our business expansion and guide our evolving approach to delivering integrated business services.

We listen and act on client feedback to ensure we meet their needs for improved transparency, greater flexibility and cost certainty.

## Our team



### Gerard Karp

Partner, Head of Data Protection  
Cyber Security & Technology Compliance

**M** +48 502 184 707

**E** gerard.karp@dwf.law

---



### Paweł Dudojc

Counsel

**M** +48 571 244 781

**E** pawel.dudojc@dwf.law



### Marian Giersz

Counsel

**M** +48 791 211 803

**E** marian.giersz@dwf.law



### Agnieszka Sagan-Jeżowska

Of Counsel

**T** +48 22 653 4200

**E** agnieszka.sagan-jezowska@dwf.law