3 November 2022

GDPR Enforcement – It's Not All About The 4% Fines

Rohan Massey
Ropes & Gray

Rosemary Kuperberg
Demandbase

Colin Rooney
Arthur Cox

Cian O'Brien
Irish Data Protection Commission

Privacy+ Security Forum

GDPR Enforcement – It's Not All About The 4% Fines

Privacy+ Security Forum

Financial penalties against organizations pursuant to the GDPR are often highly publicized and provide a useful reminder of the GDPR's coercive force. However, attention must also be paid to the non-financial sanctions in European DPAs' arsenals.

This panel will discuss the various non-financial penalties that European DPAs are capable of enforcing and their impacts on businesses.

The panel will also provide potential solutions as to how organizations can engage with regulators before and during a personal data breach incident.

GDPR Sanctions – Current Landscape

Privacy+ Security Forum

- GDPR enforcement is often focused on the financial penalties: non-compliant organizations face fines of up to the higher of €20 million or 4% worldwide annual turnover.
- Non-financial penalties received less publicity but can be just as significant:

1. Reprimands and warnings issued by the DPA:
    i. UK Home Office was reprimanded in October 2022 by the ICO for losing sensitive documents relating to terrorism in a public location. The personal data in the documents included a foreign visa applicant's details and details of two Metropolitan Police officers.
2. Temporary or permanent ban on data processing:
    i. In July 2022, the Danish municipality of Helsingør was ordered to temporarily stop processing data via Google Analytics after a Danish decision ruled that Google Analytics' transfers of personal data could not be afforded GDPR-like protections.
3. Order of rectification, restriction or erasure of personal data:
    i. Tends to be enforced by individuals exercising their rights under Articles 16, 17 and/or 18 GDPR.
4. Suspension of transfers of personal data to third countries:
    i. In April 2021, Portuguese National Institute for Statistics' transfers of personal data to Cloudfare, Inc. in the US were based on the SCCs. Portuguese DPO ordered the National Institute for Statistics to stop processing the data and suspend the transfers.
    ii. Even if SCCs are in place, there may still be no guarantee that the personal data transferred will be adequately protected in the third country.

Key Trends between Fines and Other Sanctions

Privacy+ Security Forum

- Frequency of fines: up to March 2022, an additional 505 GDPR fines were issued as compared to the previous year.
- Average quantum of fines during the period 2018-2022 was €1,533,910 across the EU. Note that this is distorted due to large fines against global technology companies, including:
    1. Amazon, which was fined €746 million by the Luxembourg DPA;
    2. WhatsApp Ireland, which was fined €225 million by the Irish DPA; and
    3. Google, which was fined €150 million by the French DPA.
- What about the frequency of non-financial penalties?
    1. UK ICO issued 24 reprimands during the period April 2021 – March 2022, compared with 4 fines with an aggregate value of £740,800 during the same period.
    2. French CNIL carried out 18 enforcement actions in 2021, only two of which resulted in solely non-financial penalties.
- Irish DPA often mixes financial penalties with non-financial penalties:
    1. WhatsApp Ireland decision resulted in a reprimand (as well as a fine) against WhatsApp for its low standards of processing personal data.
    2. In December 2021, Limerick City and County Council installed CCTV cameras for traffic monitoring purposes. The Irish DPA held that this was an unlawful basis for processing. The Council was issued with a €110,000 fine, a reprimand, and an order to stop processing the data collected via the CCTV cameras.

Business Impacts of Non-Financial Penalties

Privacy+ Security Forum

- Priority of the DPA is to ensure individuals are protected from poor data protection practices.

- Businesses should consider the following:

1. Engagement of senior management to ensure data protection remains a priority
2. Cost of third-party advisors to bring their data protection compliance program up to the GDPR's standards.
3. Conduct diligence into third-party partners' GDPR compliance, especially in the supply chain.
4. Consider certifications such as ISO, SOC and CMMI?
5. Operational cost of reviewing IT systems and implementing a new, GDPR-compliant, data processing infrastructure in the business.
6. Time frame for assessing and implementing any required changes.
7. Reputational damage for the business if issued with a public reprimand and order to stop processing.

How to Prepare and Engage with Regulators

Privacy+ Security Forum

- **Practical steps to be taken:**
  1. **Maintain and update records of processing.**
  2. **Regularly undertake DPIAs before processing data.**
  3. **Designation of a data protection officer / point of contact.**
  4. **Active engagement with regulator is criteria in mitigation.**

- **Timing for action**
  1. **As early as possible once issues are clear.**
  2. **Early contingency planning is critical as remediation timeframe may be short.**
  3. **Compliance with the requirements of the GDPR should not be an afterthought.**

Questions & Contacts

Privacy+ Security Forum

Rohan Massey

Partner
Ropes & Gray

Rosemary Kuperberg

Assistant General Counsel, Privacy
DemandBase

Cian O'Brien

Deputy Commissioner
Irish Data Protection Commission

Colin Rooney

Partner
Arthur Cox