Data Protection Enforcement

March 21, 2021

Regulators globally continue enforcement of data protection and privacy laws including issuing fines against organizations that did not meet the requirements of applicable law. In this article, we summarise some of the recent cases of interest:

Posti Group Oyj (Finland): Direct Marketing

According to the Deputy Data Protection Ombudsman, there were complaints alleging that data subjects received direct marketing from the company although they had requested that their postal data be deleted. Investigations also revealed that the data protection information provided by the company was not transparent enough and a fine of €100,000 was issued.

Consumers are more likely to complain about unsolicited marketing and in many countries, electronic communication and data protection laws require consent to be obtained before sending emails or SMS messages to consumers. Further, when a consumer has opted out from receiving marketing, organizations are mandated to heed this request.

Banca Comercială Română SA (Romania): Data Security

The National Supervisory Authority for Personal Data Processing ('ANSPDCP') announced, on 5 May 2020, that it had fined Banca Comercială Română SA RON 24,163.50 (approx. €5,000) for violating its obligation to ensure the security of data processing under Article 32 of the GDPR. In particular, Banca Comercială Română had not implemented adequate technical and organizational measures to ensure an adequate level of security in light of the risk of data processing. In addition, the ANSPDCP found that the collection and transmission to the operator via WhatsApp of copies of customers' identity documents constituted a violation of the internal working

procedure.

Organizations should assess their current technical and organizational measures to ensure it aligns with Article 32 of the GDPR or applicable local laws.

National Government Service Centre (NGSC) (Sweden): Data Breaches

On 29 April 2020, the Swedish data protection authority ('Datainspektionen') announced its decision to fine the NGSC SEK 200,000 (approx. €18,700) for violations of the GDPR, having failed to notify a data breach. The NGSC had taken almost five months for the NGSC to notify the concerned parties and close to three months for the Datainspektionen to receive a data breach notification. Moreover, the NGSC was ordered to introduce internal policies for the documentation of personal data breaches and to ensure compliance with such procedures.

Organizations are required to comply with requirements to comply with data breach notification requirements within the applicable timeframe and in the method specified by applicable law. personal data breach policies and procedures are a must and can fit into the existing framework of data breach response policies.

Unnamed Company (Netherlands): Biometrics

The organization had required its staff to have their fingerprints scanned to record attendance. The Dutch Supervisory Authority (DSA) identified several violations of data protection law, in particular:

i. no evidence that employees explicitly and freely consented to having their fingerprints scanned;

ii. insufficient information provided to employees about how their biometric data would be used;

iii. over-retention of former employees' biometric templates, which were "blocked" in the system but not actually deleted.

The company's use of biometric data was disproportionate to the aim pursued because the security risks were not particularly high in this case. Moreover, less intrusive means could have been used to achieve the company's objectives. Due to the severity of the violation, its "long" duration of ten months, and the "high" number of individuals concerned (337), the DSA decided to impose a significant fine of €725,000. In an effort to reduce the fine, the company asserted that the encryption of the biometric templates and ISO certification of the technology supplier (and its sub-processor) should serve as mitigating factors. The DSA is using its fining model which it announced last year.

Many jurisdictions restrict the use of biometric data by organizations and in some cases may even require approval from your data protection authority. There is no time like the present for you to assess your current or proposed use of biometrics and conduct a privacy impact assessment to identify and mitigate any data protection risks.

Proximus SA (Belgium): DPO

The Belgian Data Protection Authority has issued its decision to fine Proximus SA (Belgium's largest telecommunications operator) €50,000 for appointing its head of compliance, audit, and risk as its Data Protection Officer According to the DPA, this combination of roles creates a conflict of interest and therefore constitutes an infringement of Article 38(6) of the GDPR.

The decision is intended to be dissuasive for other companies when appointing a data protection officer. If you need assistance in determining whether you require a DPO, please reach out to us.

Amazon Turkey Retail Services Limited (Turkey): Direct Marketing, Transfers and Policies

On 7 May 2020, the Personal Data Protection Authority ("KVKK") published its decision to fine Amazon Turkey Retail Services Limited TRY 1,200,000 (approx. €160,000) for violations of consent requirements, among others. In particular, the decision concerns Amazon's failures to obtain explicit consent from users for the sending of commercial messages for advertising, campaigns, or promotional purposes as required by Law No. 6563 of 2014 on the Regulation of Electronic Commerce.

In addition, Amazon failed to obtain the explicit consent of users for transfers of personal data abroad and made such transfers without an approved written approval from the KVKK, as well as against the requirements of Article 9 of the Law on Protection of Personal Data No.6698.

The KVKK has instructed Amazon to update its personal data processing processes and its "Privacy Statement," "Terms of Use and Sales", and "Cookie Notification" pages to bring them into compliance with the Turkish law.

Like the GDPR, the Law on Protection of Personal Data No. 6698 has specific requirements to be met before personal data can be transferred outside of Turkey. Further, organizations are required to implement the requisite legal notices on their customer-facing websites.

Author: Mahmoud Abuwasel
Title: Partner – Disputes
Email: mabuwasel@waselandwasel.com
Profile:
https://waselandwasel.com/about/mahmoud-abuwasel/