

Digital Legal Update

July 2024

Weinhold Legal

Fines of the Office for unauthorised processing of personal data

Avast Software s.r.o. has been fined CZK 351 million by the Office for Personal Data Protection ("the Office") for unauthorised processing of personal data of users of its antivirus software and its Browser Extensions in 2019.

The Office imposed the fine because Avast improperly transmitted the pseudonymized internet browsing history of approximately 100 million users to Jumpshot, Inc. This company provided data to marketers to track consumers' online behaviour. Although Avast claimed that the data had been anonymised, the Office found that the data transmitted was capable of identifying users, meaning that it was not truly anonymised.

The Office for Personal Data Protection stressed that as a leading expert in cybersecurity, Avast should not transmit data that could reveal users' identities or private information such as interests, residence, assets, etc. As this was a case of cross-border processing of personal data across the EU, the matter was also addressed with other supervisory authorities in the EU under the One Stop Shop mechanism.

Control of consent to the processing of personal data for marketing purposes

[The Office carried out an audit](#) focused on the setting up of consent to the processing of personal data for marketing purposes at a commercial corporation offering mail order services. This company allowed customers to order goods by mail, via order coupons, and by signing the order the customer automatically consented to the processing of

personal data for marketing purposes. It was not possible to place an order without this consent.

The Office found that there was a systemic misconfiguration of the consent to the processing of personal data. In addition, if the customer wanted to exercise his right to rectify his personal data, he had to use the form 'Consent to change address data', which also contained consent to the processing of personal data for marketing purposes. This practice was surprising to data subjects and in breach of the GDPR.

The practice found did not meet the conditions of Articles 4(11) and 7(4) of the GDPR as the consent was not free and therefore not valid. Thus, the company did not have a valid legal title to process personal data for marketing purposes. Moreover, the documents did not contain information about the right to withdraw consent at any time, which was a further breach of the Regulation. The company also failed to inform data subjects of the legal basis for processing their personal data.

EDPB on "pay or OK" models

Following a request from the Dutch, Norwegian and Hamburg Data Protection Authorities, the European Data Protection Board ("EDPB") adopted [Opinion 08/2024](#), which addresses the validity of consent to the processing of personal data for behavioural advertising purposes in the context of "pay or OK" models implemented by large online platforms.

Key points of the opinion:

- ▶ 'Pay or OK' models often force users to either consent to the processing of personal data or to pay a fee, which does not give users a real choice;
- ▶ Offering only a paid alternative to services processing personal data for behavioural advertising is inadequate and controllers should consider providing an 'equivalent

Digital Legal Update

July 2024

Weinhold Legal

alternative' without requiring payment;

- ▶ Large online platforms should ensure that any fee charged does not push users into unwanted consent;
- ▶ Consent must be informed, specific and unambiguous as mandated by the GDPR; users should be fully informed of the consequences of their choice.

The EDPB is now working on more detailed guidance on "pay or OK" models.

European Commission on Meta's "pay or OK" model

The European Commission ("Commission", "EC") has initiated proceedings under Article 8 of the Digital Markets Act ("DMA") and informed Meta of its provisional findings regarding its "pay or OK" advertising model because, according to the Commission, it does not comply with the requirements of the DMA.

The new "pay or OK" model was introduced by Meta in November 2023, when Facebook and Instagram users in the EU had to choose between a paid subscription without ads or free access with personalised (behavioural) ads.

The Commission takes the provisional view that Meta's 'pay or OK' advertising model is not compatible with the DMA because it does not meet the necessary requirements set out in Article 5(2) of the DMA. In particular, Meta's model:

- ▶ does not allow users to choose a service that uses less of their personal data but is otherwise equivalent to a service based on personalised advertising;
- ▶ does not allow users to exercise their right to freely consent to the combination of their personal data between the designated services of the underlying platform and other services.

In the course of its investigation, the Commission coordinated

with the relevant data protection supervisory authorities.

Meta now has the opportunity to exercise its rights of defence and to comment on the Commission's provisional findings. The Commission plans to conclude its investigation within 12 months of the opening of the proceedings, i.e. by the end of March 2025. If it maintains its provisional findings and the non-compliance decision itself, it may impose a fine of up to 10% of Meta's total worldwide turnover, which could amount to approximately 315 billion crowns.

The Commission also has the power to adopt other remedies, such as an obligation to sell the business or parts of it.

EDPS investigation into the use of Microsoft 365 by the European Commission

In May 2021, the European Data Protection Supervisor ("EDPS") launched an investigation into the European Commission's use of Microsoft 365 following the Schrems II judgment. The aim was to check whether the EC is complying with the EDPS recommendations on the use of Microsoft products and services by EU authorities.

The EDPS concluded that the EC had breached several provisions of EU Regulation 2018/1725 on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, by failing to provide adequate safeguards to protect personal data transferred outside the EU/EEA, contrary to the requirements for an adequate level of protection. Furthermore, the EC's contracts with Microsoft did not sufficiently specify what data would be collected and for what purposes. The EDPS therefore ordered the Commission to

Digital Legal Update

July 2024

Weinhold Legal

- ▶ suspend all data flows resulting from the use of Microsoft 365 to Microsoft and its affiliates and sub-processors located in non-EU/EEA countries not covered by the adequacy decision; and
- ▶ brought processing operations resulting from the use of Microsoft 365 into compliance with EU Regulation 2018/1725.

The Commission must demonstrate compliance with both conditions by 9 December 2024.

The European Commission brought an action against the EDPS decision before the Court of Justice of the European Union ('CJEU') on 17 May (Case T-262/24), as did Microsoft on 21 May 2024 (Case T-265/24).

Draft law on cyber security

The Legislative Council of the Government (LCG) has recommended to the Government for approval the draft law on cyber security, which implements the Network and Information Security Directive (NIS2) into the Czech legal system. This step follows the modifications that the National Cyber and Information Security Agency (NCISA) has incorporated on the basis of previous suggestions of the LCG.

For a better orientation of the modifications incorporated, the NCISA has prepared an overview of the main changes made. The aim of this document is to simplify the orientation of the public and future addressees of the emerging law in the current version of the document.

The government is now discussing the draft law, taking into account the comments from the inter-ministerial comment procedure. Once approved by the Government, the draft will be submitted to the Chamber of Deputies of the Parliament of the Czech Republic. The transposition deadline according

to the NIS2 directive requires the new law to come into force on 18 October 2024. Depending on the course of the legislative process, the law is expected to come into force at the end of 2024 or even in 2025. The deadlines for the implementation of other obligations will then depend on the final date of the law's entry into force.

Regulation on artificial intelligence published in the Official Journal of the EU

On 12 July 2024, Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (the "AI Regulation", the "AI Act") was published in the Official Journal of the EU. This Regulation brings major changes to the regulation of AI. The AI Act sets out clear rules for the use of AI in order to maximise its benefits and minimise its adverse impacts on society. Companies must now adapt to the new rules and start putting them into practice.

Key points of the AI Act:

- ▶ Classification: AI systems are classified according to their riskiness, with some being banned outright for unacceptable risk;
- ▶ Rules for the use of AI: sets out uniform rules for the development, marketing, commissioning and use of AI systems in line with EU rules on safety, the fundamental rights of EU citizens and ethical principles;
- ▶ Safety, reliability and transparency: introduces strict requirements for AI systems, including accuracy, risk mitigation and the obligation to inform users that they are interacting with an AI system;
- ▶ Innovation: supports AI research and development through safe and regulated practices.

Digital Legal Update

July 2024

Weinhold Legal

The AI Regulation is binding and directly applicable in all EU Member States. Obligations vary according to the risk of each AI system and also apply to non-EU entities if the output of the AI system is used in the EU.

Key terms and responsibilities:

- ▶ 2 February 2025: the general provisions of the AI Regulation (Articles 1-5) will come into force and the prohibitions for unacceptable AI risk (prohibited AI) will apply. We recommend that companies start preparing now to comply with the new obligations, for example in the area of employee training.
- ▶ 2 May 2025: Codes of Practice should already be in place so that providers can demonstrate compliance in a timely manner. Codes of Practice should be the central tool for proper compliance with the obligations set out in this Regulation for providers of generic AI models, and their development is ensured by the AI Office.
- ▶ 2 August 2025: Member States must establish notifying authorities and designate market surveillance authorities. Obligations for providers of generic AI models will start to apply. Penalty provisions will already be applicable.
- ▶ 2 August 2026: the AI Act enters into full force (except for Article 6(1) which enters into force on 2 August 2027).

Annual Report of the Office for the Protection of Human Rights and Fundamental Freedoms 2023

The Office submitted to the Senate of the Parliament of the Czech Republic the Annual Report for 2023, which presents a comprehensive overview and summary of the most important

results of the Office's supervisory activities in the field of personal data processing. Its key points are:

▶ Cookies

In 2023, the Office significantly increased the number of decisions concerning the processing of personal data through cookies. This is because some controllers did not respond sufficiently to the reprimand letters sent by the Office. The Office will continue to focus intensively on this issue as the processing of personal data through cookies can be very dangerous for internet users.

▶ European proposal for a procedural regulation complementing the GDPR

In July 2023, the European Commission presented a proposal for a Regulation laying down further procedural rules for the enforcement of Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR) and the proposal is now progressing through the legislative process and is being discussed by the European Parliament. The proposal responds to the experience with the application of the GDPR in cross-border cases (e.g. where the data subject resides in a different country than the controller) and aims to improve cooperation between national supervisory authorities in the enforcement of the GDPR.

▶ Digital Economy Bill

The Ministry of Industry and Trade has started intensive preparation of the adaptation of the Digital Services Act (DSA) and the Digital Governance Act (DGA) into the Czech legal system in the form of the draft Digital Economy Act and on amendments to some related laws.

The Digital Economy Act aims to ensure the proper functioning of the internal market in the digital and data economy by creating a clear and predictable legal

Digital Legal Update

July 2024

Weinhold Legal

framework for the enforcement of obligations arising from related EU legislation. This includes, on the one hand, the designation of the competent authorities responsible for the enforcement of the Data Governance Regulation and the Digital Services Regulation. The main supervisory authority will be the Czech Telecommunications Office; the Office will cooperate in particular on the supervision of electronic advertising.

The proposal also sets out rules on penalties for breaches of the DSA and DGA.

► Final fine for the Quarantine app

The Office has issued the first final fine for a violation of regulations governing the protection of personal data under the so-called criminal law directive, specifically for the unauthorised processing of personal data of persons ordered to be isolated by the Police of the Czech Republic under the Karanténa database.

The information contained in this bulletin is presented to the best of our knowledge and belief at the time of going to press. However, specific information related to the topics covered in this bulletin should be consulted before any decision is made. The information contained in this bulletin should not be construed as an exhaustive description of the relevant issues and any possible consequences, and should not be fully relied on in any decision-making processes or treated as a substitute for specific legal advice, which would be relevant to particular circumstances. Neither Weinhold Legal, s.r.o. advokátní kancelář nor any individual lawyer listed as an author of the information accepts any responsibility for any detriment which may arise from reliance on information published here. Furthermore, it should be noted that there may be various legal opinions on some of the issues raised in this bulletin due to the ambiguity of the relevant provisions and an interpretation other than the one we give us may prevail in the future.

For further information, please contact the partner / manager you are usually connected to.



Martin Lukáš
Partner
Martin.Lukas@weinholdlegal.com



Tereza Hošková
Managing Attorney
Tereza.Hoskova@weinholdlegal.com



Daša Aradská
Attorney
Dasa.Aradska@weinholdlegal.com