Apr 2022

Poland: Challenges and trends on privacy rights

Increasing consumer awareness on privacy rights makes it vital for companies to comply with requirements under privacy regulations and stay up to date with relevant guidance from data protection authorities to adequately respond and facilitate data subject requests. Artur Piechocki and Katarzyna Gorzkowska, from APLAW, share their insights into the Polish landscape with regards to data subject rights and discuss how companies can respond to associated challenges.

ewg3D / Signature collection / istockphoto.com

Recent guidelines published by the UODO

The Polish data protection authority ('UODO') has published several guidelines for specific sectors, and personal data controllers follow the guidelines issued by the UODO. Indeed, in the case of the right of access to medical data, the UODO has indicated that, for example, the performance of the obligation set out in Article

15(3) of the GDPR may therefore be carried out both by making a copy or extract of a document (carrier) containing personal data and other data, and by providing the authorised person with the content of their personal data, disregarding the information contained in the carrier, which is not personal data within the meaning of Article 4(1) of the GDPR. If a patient requests a copy of personal data processed in the medical records, it does not unequivocally mean that they will receive a copy of the medical records. The position of the UODO does not differ from the positions of other bodies and the European Data Protection Board ('EDPB').

The UODO's guidelines on the implementation of the information obligation towards representatives of legal persons have caused confusion in Poland. For many, it is obvious that a person acting as a board member should be aware that their personal data will be processed by the company and contractors. In addition, personal data of members of the management board of companies, including PESEL numbers, is publicly available in the National Court Register and any person can consult it.

In addition, the UODO pays particular attention to the need to protect children's privacy. The UODO has, *inter alia*, questioned the processing of children's biometric data for the purpose of taking meals in the school canteen. With regard to the guidelines on informing a child about a breach of personal data concerning them, it cannot be ignored that children are at different developmental levels depending on their age. For younger children, information should be addressed to their legal guardians. Older children, especially adolescents, are able to understand what personal data is and the consequences of its misuse.

Facilitating data subject rights

Our experience shows that Polish companies are increasingly aware of the challenges of applying the GDPR. How rights are enforced depends on the awareness of the organisation. Data controllers try to enable the enforcement of rights in accordance with the will of data subjects. Above all, this concerns the scope and manner of providing information. Polish companies try to meet the expectations of data subjects, especially when it comes to the enforcement of rights by customers. Data controllers, in case of doubt, try to establish what right the data subject wants to exercise, what information they want to obtain, and how they want to obtain it. Of course, there are companies that flagrantly disregard the obligations indicated in the GDPR, and in such cases, the UODO intervenes.

Data controllers verify the categories of processed personal data on an ongoing basis. In addition, they use the assistance of personal data protection inspectors. The role of the data protection officer ('DPO') has become extremely important. More and more data controllers are beginning to understand that the function of a DPO is a real benefit for the organisation and support.

Additional guidance from the UODO

The existing guidelines issued by the UODO are undoubtedly valuable for many companies. Nevertheless, Polish personal data controllers still expect additional guidance on how to implement the right to privacy.

One of the main problems is the need to identify the entity making the request to the personal data controller. Exercising the right to information (e.g. providing information on what personal data about a particular person is being processed) requires taking steps to establish whether the requesting person is indeed the data subject. Establishing the identity of the subject is not a simple task. In order to identify the person, the personal data controller should obtain from the requester information which will make it probable that the requester is the person whose data the controller is processing. This is a significant problem in the case of online communication. The data subject should be able to enforce their rights quickly and easily. In the digital environment, the most convenient channels are usually email, chat, or other instant messaging. These are means of distance communication. In this situation, the personal data controller or their representative (e.g. an employee) cannot see or hear the applicant. There is no way to verify whether the applicant is male or female, or how old they are. When obtaining information from the applicant, such as, for example, email address or PESEL number, it is never certain whether the applicant is the data subject or another person, who came into possession of the personal data, such as a customer of the personal data controller. Therefore, a situation may occur, including the disclosure of the customer's data to a third party (fraudster).

In such a case, the danger of phishing for the customer's personal data arises. It should be emphasised that due to the position of the UODO, personal data controllers have limited possibilities of requesting additional documents from the applicant. The UODO takes a strict approach to the issue of requesting a copy of an identity document by the controllers. Another problem is the period for keeping such copies and the period for keeping personal data in order to defend against claims. It may happen that the applicant defrauds the personal data. In such a situation, the data subject may have claims and demand compensation from the controller. The UODO takes a strict approach to the possibility of storing information about a person for the purpose of possible defence against claims or potential redress. As a consequence, controllers of personal data are at a disadvantage. The protection of their rights is made more difficult. It is worth emphasising, however, that UODO's position in this respect has recently been challenged by an administrative court.

Obligations on data subject rights

The UODO may not always be right in its application of administrative penalties, but as a general rule, it takes a fair approach to enforcing obligations relating to data subjects' rights. The UODO takes into account whether a data controller's failure to enforce rights is due to wilful misconduct or inadvertent negligence. The issue of enforcement of data subject rights is important, which is why the UODO is not inactive. To date, the UODO has imposed penalties on companies for failing to exercise data subjects' rights. It should be emphasised that these have not only been financial penalties. In many cases, the UODO has given a warning

penalty, and the type of penalty depends on the circumstances of the investigated case. In light of the criteria set out in Article 83(2) of the GDPR, a warning may be sufficient, and at least as 'effective, proportionate and dissuasive' as imposing a financial penalty (vide Article 83(1) GDPR).

Currently, we have not received any information about the commencement of an audit by the UODO on the enforcement of data subjects' rights. Whether the UODO will initiate proceedings in this type of case usually depends on whether the data subject lodges a formal complaint to the UODO. The source of information for the UODO about irregularities is the data subject's complaint.

Exemptions to data subject rights

In our view, the possibility to exclude data subjects' rights is justified in cases where the enforcement of the rights may lead to an infringement of third parties' interests or other important interests. As an example of another important interest, one can point to secrets protected on grounds of public safety.

Artur Piechocki Attorney-at-Law and Founder of APLAW
artur.piechocki@aplaw.pl
Katarzyna Gorzkowska Lawyer
katarzyna.gorzkowska@aplaw.pl
APLAW, Warsaw