Bird & Bird

Inspection activities of the Czech Data Protection Authority in 2021 – what are the key findings?

November 2021

The Czech Data Protection Authority ("**DPA**") has recently published an overview of its inspection activities for the first half of 2021. Although a significant part of the inspections this year concerned the public administration and the non-profit sector, the DPA's conclusions from some of these inspections may also be useful for controllers and processors in the private and commercial spheres. In addition, the DPA also carried out a number of inspections regarding the sending of commercial (marketing) communications, where it again drew attention to non-compliance with what are often very basic rules. We have therefore prepared a short summary of the key take-aways from the published inspections.

Unsolicited commercial communications

The highest published fines imposed by the DPA in connection with unsolicited commercial communications amounted to CZK 250,000 (approx. EUR 9,750) and CZK 200,000 (approx. EUR 7,800).

What was the violation/subject of the inspection?	What to look out for?
In the first case, commercial communications were sent to persons who were not customers of the audited company (as a result of mixing newly obtained contact details with the original contacts), nor did they give their consent to receiving commercial communications. The extent of the fine of CZK 250,000 reflects, *i.a.*, the fact that this was a continuous and long-standing systemic error of the audited company. Moreover, the commercial communications did not contain any information on how to opt out.	*Separate customer databases* Adequate control mechanisms should be in place to ensure that commercial communications are actually sent only to persons: (a) who have consented to them or (b) who are customers of the company in question (and at the same time other conditions of the so-called opt-out exemption under the Act on Certain Information Society Services are met). *Opt-out option* The recipient of the sent commercial communications must have the possibility to unsubscribe in a simple way from receiving commercial communications, *e.g.*, via an opt-out link in the e-mail. In the case of text messages, it may be indicated that if the recipient does not wish to receive commercial communications, they may reply to the respective telephone number, *e.g.*, "stop".
The second case, where a fine of CZK 200,000 was imposed, occurred when the sent commercial communications did not contain information about the sender on whose behalf the communication was being conducted, and in some cases even inaccurately referred to another third party as the sender.	*Marking of commercial messages* The DPA repeatedly draws attention to the need to correctly label commercial communications. In addition to indicating that it is a commercial communication (*e.g.*, a "newsletter" in the subject line), the sender and the company whose products or services are being promoted (if different from the sender) must be clearly identified. The identification should include the company name,

	name with additions and, where appropriate, a corporate ID number or another identifier. It is interesting that in one of the inspections concerning commercial communications sent via a text message (SMS), the DPA acknowledged that the indication of the website of the audited company was sufficient as an identification of the sender considering the short format of the text message (while on its website the DPA states that such indication is generally not sufficient). *Liability for the dissemination of commercial communications* Both the actual sender of the commercial communications and the company for whose benefit the commercial communications are disseminated are liable for the dissemination of commercial communications.

However, it is also worth mentioning other inspections in which the DPA, for example, evaluated what should be considered a commercial communication.

What was the violation/subject of the inspection?	What to look out for?
Based on the complaints about unsolicited commercial communications (sent by e-mail and text message), the DPA found that, in addition to communications containing specific offers of electronic goods and furniture and offers of discounts, together with a link to the audited company's website, communications containing information from visits to individual stores must also be regarded as commercial communications. These communications clearly indicated potential purchases of goods and also referred to the company's website.	*Promotion of the company* Commercial communication is any form of communication, including advertising and encouragement to visit websites, intended to directly or indirectly promote the goods or services or the image of the business. This includes messages containing birthday wishes, messages containing various user reviews, purchase ratings, or even messages requesting consent to receive commercial communications.

Copies of ID cards

In two inspections, the DPA dealt with making copies of identity cards, whilst in one of the cases, it was for the purpose of identifying the client in accordance with the statutory AML (anti-money laundering) requirements. In this context, the DPA recently issued an opinion on the interpretation of the AML Act, as a response to the opinion of the Czech Financial Analytical Office which oversees AML compliance.

What was the violation/subject of the inspection?	What to look out for?
In the first case, the inspection concerned the financial services and insurance sector, where the audited company was a so-called obliged entity under the AML Act. The copying of ID cards occurred in two cases and the DPA found no misconduct: 1 identification of the client in the case of concluding a contract exclusively by means of distance communication – the client is obliged to provide a copy of their ID card and the legal basis	*Legal basis for obtaining a copy of the ID card under AML* Firstly, it is necessary to determine under which statutory provision the client is identified and accordingly choose the appropriate legal basis for processing under Article 6 GDPR – compliance with a legal obligation or consent. However, the consent must be entirely voluntary, and the conclusion of the contract must not be conditional on consent.

for the processing is the compliance with a legal obligation, and

2 identification of the client in the case of concluding a contract that is not concluded exclusively by means of distance communication – a copy of the ID card is made only with the prior (voluntary) consent of the client.

In the second case, the audited company took scans of ID cards and other identification documents when concluding accommodation contracts, allegedly on the basis of the data subjects' consent. However, the company was not able to prove these consents. The company had no legal basis for processing the personal data contained in the scans of its clients' ID cards, and thus violated Article 6(1) of the GDPR. In this inspection, the DPA also found a breach of the obligation to keep records of processing activities, where some of the purposes of processing were missing from the audited company's records.

Legal basis for making a copy of the ID card in general situations and data minimisation

The general rule is that making a copy of an ID card (but also, *e.g.*, a passport) is only possible with the holder's consent (to which there are, of course, certain legal exceptions). Such consent must be voluntary and cannot be used as a condition for the performance of the contract. In addition, processing a copy of the ID card may potentially lead to a breach of the data minimisation principle. The ID card contains certain data which may not even be needed for the purpose of the processing. Therefore, it is generally preferable to check only the necessary data from the submitted ID card and not to make a copy of the entire card.

Cookies

What was the violation/subject of the inspection?	What to look out for?
The inspection was focused on compliance with the obligations set out in the GDPR in relation to the use of cookies on the website of an online store. The DPA found a violation of Article 6(1) of the GDPR as the requirement for informed consent was not met for an unspecified period of time. The company committed the infringement by the fact that if the user decided to obtain more information about the processing of personal data before giving consent and clicked on the "Personal Data" link, they simultaneously gave uninformed consent to the processing of personal data through cookies.	*Cookies and consent* Under current legislation, cookies can only be used if they are not rejected (the so-called opt-out regime). Thus, it is not entirely clear from the inspection carried out under which circumstances the DPA evaluated whether consent was validly granted in this context. However, the conclusions of the inspection are particularly relevant for the future. This is because as of 1 January 2022, most cookies can only be used with the user's consent and this consent must fully comply with the requirements of the GDPR. We have prepared a clear guide on how consent should look like under the new cookies legislation in a separate document. *Cookies and information obligation* The information obligation under the GDPR must also be fulfilled in relation to the processing of cookies, including indicating the period for which individual cookies are stored and the possible recipients of the cookies. The failure to comply with the information obligation, specifically by not providing this information, was noted by the DPA in one of the inspections carried out.

CCTV systems

What was the violation/subject of the inspection?	What to look out for?
The DPA found that the kindergarten, by placing and operating video surveillance cameras (CCTV) in the changing rooms used to change the children's clothes, violated the data controller's obligation to process personal data on the basis of lawful grounds under Article 6(1)(a) to (f) of the GDPR.	*CCTV systems and the violation of privacy* Video surveillance systems are usually operated on the basis of the legitimate interest of the controller, which may in particular be protection of the controller's property or third parties or the protection of health. However, it is always necessary to evaluate the degree of interference with the privacy of the persons monitored, the necessity of the processing, and to set up the video surveillance systems to ensure that they do not unduly interfere with the privacy of any persons. This applies, of course, also in the workplace, where, in addition, the specific regulation of employee monitoring under the Czech Labour Code must be taken into account.

We are happy to answer all your questions

Vojtěch Chloupek
Partner

Tel: +420226030518
vojtech.chloupek@twobirds.com

Roman Norek
Associate

Tel: +420226030524
roman.norek@twobirds.com