Welcome to our data protection newsletter in which we cover – in our view – the most interesting decisions in the field of compliance (personal data protection and telecommunications law). We also present practical information for businesses that arise from the discussed decisions and judgments.

Judgment of the Regional Administrative Court in Warsaw of 10 February 2021, case no. II SA/Wa 2378/20

The Regional Administrative Court dismissed the appeal against the decision by the President of the Personal Data Protection Office (PDPO) that imposed an administrative fine of **PLN 201,559.50** on the Company for:

- violating the principle of lawfulness of processing,
- violating the principle of fair and transparent processing,
- failure to ensure proper exercise of the right to be forgotten.

Background:

According to the President of the PDPO, the Company did not ensure an easy and effective way to exercise the right to data erasure. In one of the documents provided to data subjects the Company informed that persons to whom a marketing campaign would be addressed would be able to revoke their consent in a simple and easy way, for instance by clicking on a link provided in received emails and SMSs. **However, during an inspection the authority established that after clicking on the "revoke consent" link users were redirected to a website with a question regarding the reason for unsubscribing from email advertisements**. After answering this question, users were redirected to another website where a message was displayed wrongly stating that the consent

JDP DRAPAŁA & PARTNERS Sp. j. / Numer KRS: 0000880140 / Organ rejestrujący: Sąd Rejonowy dla m. st. Warszawy, XII Wydział Gospodarczy Krajowego Rejestru Sądowego / NIP: 7010056483 / REGON: 140887753

had been revoked, together with the information on a data subject's rights, including the right to data erasure.

Conclusions for controllers:

1. A company is required to ensure that consent can be revoked in an as easy way as the way in which the consent was given (e.g. by the same channel) or easier (e.g. by using additional communication channels).
2. A company may not employ solutions that would obstruct revoking consent or would make the consent revocation more difficult than the granting of consent (e.g. to give consent it was sufficient to check a box, whereas to revoke it, it is necessary to exchange formalised correspondence with the controller, including to answer additional questions).
3. Asking the data subject about the reasons for the consent revocation has been considered to be an action obstructing the consent revocation.
4. Controllers are required to act with utmost care to communicate with data subjects in a fully transparent way. Sending contradictory messages to data subjects about the information on the consent revocation and then about information on how to effectively revoke consent has been considered to violate the principle of fair and transparent processing.

The judgment (Polish version) is available at:
https://orzeczenia.nsa.gov.pl/doc/EFE0EE4EE0

Judgment of the Regional Court in Warsaw, XVII Division Court for Competition and Consumer Protection, of 4 February 2021, XVII AmT 81/19

The Regional Court in Warsaw dismissed an appeal against the decision by the President of the Office for Electronic Communications imposing on the Company the following fines:

- **PLN 4,200,000** for failure to fulfil the obligation to obtain consent for using automatic calling systems for direct marketing purposes,

- **PLN 4,900,000** for failure to fulfil the obligation to obtain consent for using automatic calling systems for direct marketing purposes.

JDP DRAPAŁA & PARTNERS Sp. j. / KRS: 0000880140 / Registration Authority: District Court for the Capital City of Warsaw, XII Commercial Division of the National Court Register / NIP: 7010056483 / REGON: 140887753

Background:

Between 1 October 2015 and 29 February 2016 the Company carried out direct marketing by sending direct SMSs to its customers without having obtained their prior consent to receiving marketing information as prescribed in art. 172 of the Telecommunications Law. The Company did not present upon the demand of the President of the Office for Electronic Communications the information regarding the number and the content of the statements of consent of the consumers to whom marketing communication was sent.

Conclusions for controllers:

1. A company is required to possess the required consents at the moment of carrying out marketing activities, and must be able to demonstrate this.
2. Failure to present them, upon request of the President of the Office for Electronic Communications, the content and the scope of consents of certain recipients of marketing communications is considered the acknowledgement that the company does not have such consents.
3. The Regional Court stated that art. 172 of the Telecommunications Law requires prior consent to using automatic calling systems for marketing purposes. An automatic calling system means all technical solutions for providing contents to individual recipients, without any direct human involvement, e.g.:

    - voice systems,
    - fax solutions,
    - electronic mail based solutions,
    - SMS and MMS generators, etc.

The judgment (Polish version) is available at:
http://orzeczenia.ms.gov.pl/content/$N/154505000005127_XVII_AmT_000081_2019_Uz_2021-02-23_001

Judgment of the Supreme Administrative Court of 20 April 2021, III OSK 161/21

The Supreme Administrative Court in Warsaw dismissed an appeal against a decision by the Inspector General for the Protection of Personal Data finding that provisions on consents to data processing had been violated.

JDP DRAPAŁA & PARTNERS Sp. j. / KRS: 0000880140 / Registration Authority: District Court for the Capital City of Warsaw, XII Commercial Division of the National Court Register / NIP: 7010056483 / REGON: 140887753

Background:

The Company used to obtain one consent from data subjects for three different processing purposes, that is:

- processing personal data for the purposes of the marketing of the **Company** products and services,
- processing personal data for the purposes of the marketing of products and services of **entities from the Company group**,
- using **telecommunications terminal equipment and automatic calling systems for direct marketing purposes**.

Conclusions for controllers:

1. A company must ensure that the consent to data processing is given freely and voluntarily. In particular, where data are processed for various purposes (concerns various issues), separate consent is required for each such purpose.
2. Combining several consents in one statement makes it impossible to choose the consent that the person wants to give. This means that the data subject is not entirely free in giving their consent to processing personal data for certain purposes (e.g. the Company's marketing only), in particular in a way which ensures that the consent is not forced by the need to make other declarations of will (e.g. consent to marketing of entities other than the Company).
3. Including purposes of marketing of products and services of the Company and of other unspecified entities in one consent clause (one check box), and using telecommunications terminal equipment and automatic calling systems to conduct this marketing is unlawful.

The judgment (Polish version) is available at:
https://orzeczenia.nsa.gov.pl/doc/524FC93261

U.S.A.

On 11 January 2021 the President of the PDPO issued decision no. DKN.5130.2815.2020 in which it **admonished** the Company for breaching data protection regulations i.a. by:

- choosing ineffective security measures for an IT system,
- lack of appropriate testing, measuring, and assessing the effectiveness of technical and organisational measures.

JDP DRAPAŁA & PARTNERS Sp. j. / KRS: 0000880140 / Registration Authority: District Court for the Capital City of Warsaw, XII Commercial Division of the National Court Register / NIP: 7010056483 / REGON: 140887753

Background:

An inspection showed that the data breach was associated with breaking the security of the Company's IT system, and encrypting the data processed in this system. As a result, the Company could not access the system and the personal data gathered there. The Company stated that the breach concerned around 80,000 records regarding employees, customers and patients, including: forename and surname, parents' names, date of birth, bank account number, residential address, PESEL number, email address, ID card series and number, phone number, and health data.

Conclusions for controllers:

1. Controllers are required to take measures ensuring a required level of data security by putting appropriate technical and organisational measures in place, for instance by:
    - using software with the manufacturer's current technical support for data processing,
    - taking measures to ensure optimal configuration of the operating systems used,
    - measuring and assessing the effectiveness of technical and organisational measures regularly in the form of security tests of IT infrastructure and applications.
2. Lack of the manufacturer's technical support poses a great risk of reduced software resistance against, for instance, maleware.
3. Controllers are required to verify both the **adequacy and the security level** of the technical measures put in place at each stage of the processing.

The decision (Polish version) is available at:
https://uodo.gov.pl/decyzje/DKN.5130.2815.2020

The National School of Judiciary and Public Prosecution

On 11 February 2021 the President of the PDPO issued decision no. DKN.5130.2024.2020 imposing on the National School of Judiciary and Public Prosecution seated in Cracow a fine of **PLN 100,000** for:

- failure to put appropriate technical and organisational measures in place,
- failure to test and assess the effectiveness of technical and organisational measures ensuring security of personal data placed on the learning platform of the National School of Judiciary and Public Prosecution,
- entrusting data processing without obliging the processor in an agreement to process personal data only upon the controller's documented request,

JDP DRAPAŁA & PARTNERS Sp. j. / KRS: 0000880140 / Registration Authority: District Court for the Capital City of Warsaw, XII Commercial Division of the National Court Register / NIP: 7010056483 / REGON: 140887753

- and without specifying in the data processing agreement the categories of persons and without specifying the type of personal data by indicating their categories.

Background:

The controller obtained information from the Central Police Headquarters about publishing personal data relating to kssip.gov.pl domain on the Internet. Afterwards the controller established that a data breach occurred. According to the controller's findings the data came from the data basis from the website szkolenia.kssip.gov.pl, created during the test migration to a new learning platform ekssip.kssip.gov.pl. The breach concerned personal data of 50,283 persons. The categories of data that the breach concerned include: forename and surname, email address, user name, phone number, unit, department, unit address, city, technical data such as IP address, date of the first and last log-in, password (in a non-public form) and PESEL number.

Conclusions for controllers:

1. When describing data processing, a data processing agreement should **refer to data categories**, if they can be specified.
2. A data processing agreement should **contain at least a general** provision obliging the processor **to act only on the controller's documented request**.
3. If parties to the agreement designate contact persons for the purposes of the agreement performance and communication channels, these persons should be informed beforehand about the scope of services and the parties' obligations to make them aware what their role as contact persons is, which may minimise the risk of a data breach.

The decision (Polish version) is available at:
https://uodo.gov.pl/decyzje/DKN.5130.2024.2020

Cyfrowy Polsat

On 22 April 2021 the President of the PDPO issued decision no. DKN.5130.3114.2020 imposing a fine of **PLN 1,136,975** on Cyfrowy Polsat S.A. seated in Warsaw for breaching the GDPR provisions by failure to put appropriate technical and organisational measures in place to ensure security of personal data processed in cooperation with an entity providing courier services by quickly identifying data breaches. For this reason, the following data breaches took place regularly at the Company:

JDP DRAPAŁA & PARTNERS Sp. j. / KRS: 0000880140 / Registration Authority: District Court for the Capital City of Warsaw, XII Commercial Division of the National Court Register / NIP: 7010056483 / REGON: 140887753

- handing parcels to an unauthorised person,
- losing documents by the courier company,
- theft of a parcel with equipment.

Background:

The Company regularly reported data breaches regarding the data of the Company's customers, including i.a. loss of documents containing customers' personal data or delivering documents to a wrong person. A thorough analysis of the reports by the authority showed that a substantial part of the breaches was not identified right away but within 7–14 days, 14–30 days or even more than 60 days from the breach.

Conclusions for controllers:

1. Delivering a parcel to an authorised third person who is recognised as a trusted recipient, i.e. a household member, may in certain circumstances reduce the probability of the risk for individuals.
2. Controllers are required not only to put appropriate policies and procedures in place, **but also develop appropriate mechanisms to control the fulfilment of the obligations specified there**; here it was important to implement mechanisms to verify whether the processor performs its obligations properly.
3. Lack of the processor's quick reaction to a data breach does not release the controller from the responsibility for prompt breach identification,.
4. The time limit for reporting a data breach is counted from the breach identification. The breach identification should be understood as a situation where **a controller becomes aware of facts that could be classified as a data breach. The moment when the controller makes such assessment is irrelevant.**

The decision (Polish version) is available at:
https://uodo.gov.pl/decyzje/DKN.5130.3114.2020

JDP DRAPAŁA & PARTNERS Sp. j. / KRS: 0000880140 / Registration Authority: District Court for the Capital City of Warsaw, XII Commercial Division of the National Court Register / NIP: 7010056483 / REGON: 140887753

Contact:

If you have any questions, please feel free to contact our experts.

Anna Matusiak-Wekiera
Attorney-at-law
Head of Data Protection/
Compliance Practice

anna.matusiak-wekiera@jdp-law.pl

Krzysztof Bąk
Attorney-at-law
Associate

krzysztof.bak@jdp-law.pl

JDP DRAPAŁA & PARTNERS Sp. j. / KRS: 0000880140 / Registration Authority: District Court for the Capital City of Warsaw, XII Commercial Division of the National Court Register / NIP: 7010056483 / REGON: 140887753