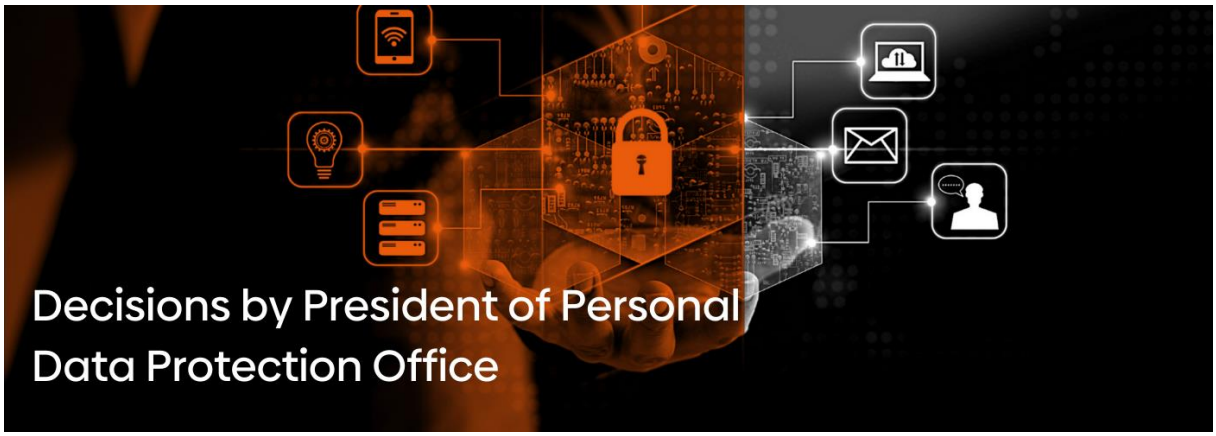

In December and January the President of the Personal Data Protection Office (*Urząd Ochrony Danych Osobowych,* "**UODO**") imposed a number of fines for violating the General Data Protection Regulation ("**GDPR**").

Below we present the imposed fines with our brief comments on what a controller should do in the given circumstances to minimise the consequences of a potential violation of the GDPR provisions.

Virgin Mobile Polska

On 3 December 2020 the President of UODO issued decision No. DKN.5112.1.2020 that imposed on Virgin Mobile Polska seated in Warsaw a fine of **PLN 1,968,524** for a violation of the GDPR by a failure to put in place appropriate technical and organisational measures ensuring safety level adequate to the risk regarding processing of personal data using IT systems for registering personal data of pre-paid services subscribers. The failure to implement necessary measures resulted in an unauthorised access to these data.

Background:

The fined company reported to the President of UODO a data breach consisting of an unauthorised access to personal data of pre-paid services subscribers. In connection with this report, the President of UODO carried out an inspection in the company. As a result of the breach, a vulnerability (gap) of the system for registering subscribers was taken advantage of (an unauthorised person accessed the personal data of pre-paid services subscribers, and obtained personal data including 123,391 first and last names, PESEL numbers, subscriber's document numbers, in various configurations. During the inspection the authority established that the regulations had been violated, and therefore imposed the fine.

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

Conclusions for controllers:

1. Controllers are required to comprehensively and regularly (in a scheduled manner) review and update the technical and organisational measures put in place. It is not sufficient to test the safeguards (including the vulnerability of IT systems) only when a risk arises ("when the need arises, in the case of organisational or legal changes").
2. Material changes regarding data processing, such as legal, organisational or technical changes (e.g. a change of an IT system operator) should entail a reassessment of the effectiveness of the technical and IT solutions implemented.
3. Controllers are required to put in place and follow procedures for regular testing, measuring, and assessing the effectiveness of the technical and organisational measures securing the data processing.

The decision is available at:
https://www.uodo.gov.pl/decyzje/DKN.5112.1.2020

Smart Cities

On 9 December 2020 the President of UODO issued decision No. DKE.561.13.2020 that imposed on Smart Cities sp. z o.o. seated in Warsaw a fine of **PLN 12,838.20** for a violation of the GDPR consisting of a failure to cooperate with the President of UODO, and to ensure access to personal data and other information necessary for the President of UODO to fulfil its duties.

Background:

UODO received a complaint regarding irregularities in the processing of the complaining person's personal data by Smart Cities. The President of UODO requested Smart Cities to reply to the complaint, and to answer detailed questions regarding this matter. However, the controller provided incomplete information, and did not collect any further correspondence. The President of UODO requested the company several times to present clarifications without success, and therefore instituted a procedure to impose a fine, and issued a decision in this respect.

Conclusions for controllers:

1. A lack of cooperation with the President of UODO constitutes an independent ground for issuing a decision on imposing a fine in a procedure different

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

than the procedure in which UODO requested the controller to provide clarifications.

2. A violation consisting of a lack of cooperation with the President of UODO by not replying to UODO's request is classified by UODO as intentional, grave, and reprehensible conduct.
3. Where a controller is grossly negligent in the area of personal data protection, and providing clarifications could result in UODO identifying such material negligence (about which UODO does not know) that would justify a heavy fine, a lack of cooperation with UODO could be used instrumentally as a tool to mitigate a fine, regardless of the effectiveness of this tool.

The decision is available at:
https://www.uodo.gov.pl/decyzje/DKE.561.13.2020%20

TUiR Warta

On 9 December 2020 the President of UODO issued decision No. DKN.5131.5.2020 that imposed on TUiR Warta seated in Warsaw a fine of **PLN 85,588** for a failure to report a data breach to the President of UODO, and to notify the data subjects about the breach without undue delay.

Background:

The supervisory authority was notified about the data breach by an unauthorised recipient that came into possession of documents containing personal data that were not addressed to that person. The breach consisted of **sending once by email an insurance policy containing personal data of two persons**, by an insurance agent (P.U.J.K. seated in O.) that processed personal data for TUiR WARTA S.A. seated in W., **to an unauthorised recipient**, as a result of which the confidentiality of the personal data including first and last names, residence or correspondence addresses, PESEL numbers, phone numbers, email addresses, information regarding the insured thing (passenger car), insurance coverage, payments, assignment, and additional provisions of a contract, had been breached.

Importantly, Warta had sent the policy to an email address indicated by the insured person. The insured person themselves mistakenly indicated a wrong email address, and consequently a third person came into possession of the policy.

Conclusions for controllers:

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

1. Even a breach that affects only individual persons may be a reason for imposing a substantial fine.
2. A controller using emails in its operations should put a verification system in place to detect customers' mistakes in indicating their email addresses (e.g. working verification of email addresses) or a system preventing unauthorised access to personal data (e.g. emails encryption). If such system is not in place, and a customer indicates a wrong email address, and as a result personal data are sent by a controller to some other person, a data breach occurs for which a controller is responsible.
3. Even if a controller receives declarations from the persons that mistakenly received the data that they have deleted the received data, the controller cannot consider these persons as trusted persons because it does not have a business relationship with them, and therefore cannot conclude that the risk of violating rights and freedoms of the data subjects is lower because of such declarations.
4. Each unauthorised disclosure of data categories mentioned above should be treated as notifiable to UODO and the data subjects. An exception may be only an unauthorised disclosure to trusted recipients.

The decision is available at:
https://uodo.gov.pl/decyzje/DKN.5131.5.2020

ID Finance Poland (MoneyMan.pl)

On 17 December 2020 the President of UODO issued decision No. DKN.5130.1354.2020 that imposed on ID Finance Poland Sp. z o.o. in liquidation seated in Warsaw a fine of **PLN 1,069,850** for a violation of the GDPR provisions by a **failure of ID Finance Poland Sp. z o.o. in liquidation to put in place, both at the stage of designing the process of personal data processing and at the stage of data processing, appropriate technical and organisational measures adequate to the risk to the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems, and ensuring the ability to effectively and quickly detect a personal data breach, and ensuring the regular assessment of the effectiveness of these measures, which resulted in an unauthorised access to the personal data.**

Background:

The fined company reported a data breach involving problems with the server operation, and then made a supplementary report. As a result of the reported

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

breach, **an unknown person gained access to a database including 140,699 customers** with such data as first and last name, education, email address, employment details, email address to a person to whom a customer wants to recommend a loan, salary details, marital status, (landline, mobile, previously used) phone number, PESEL number, nationality, NIP number, password, place of birth, correspondence address, registered address, work phone number, and bank account number. These data were used to blackmail the company and to demand a ransom.

During the investigation it was established that **ID Finance Poland did not adequately respond to an email written in English from an independent researcher about gaps in the security system**. The gap occurred by starting a firewall improperly by ID Finance Poland's subcontractor during restarting a server, and as a result one of the ports remained open. Additionally, user passwords were stored as a clear text, without encryption/hashing. An unauthorised access took place due to a late (after 10 days) reaction of the controller to the email about the security gap.

Conclusions for controllers:

1. Each information that a controller receives with respect to improper operation of the data processing system should be treated seriously, and should be analysed within a time that allows for reporting a breach to UODO within 72 hours, and notifying the data subjects.
2. In the case of any doubts, having regard in particular to the nature and the scope of the processed data, and the risk of their accidental disclosure, a controller should report a breach to the supervisory authority even if such prudence could turn out excessive.
4. A controller should put in place and follow procedures allowing to smoothly handle reports, taking into account contact with subcontractors and procedures for regular testing, measuring, and assessing the effectiveness of the implemented technical and organisational measures ensuring data security.
3. Storing user passwords as a **clear text, which if there are no other technical and organisational measures for securing data processing in place, also constitutes a data breach.**

The decision is available at:
https://uodo.gov.pl/decyzje/DKN.5130.1354.2020

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

Medical University of Silesia in Katowice

On 5 January 2021 the President of UODO issued decision No. DKN.5131.6.2020 that imposed on the Medical University of Silesia in Katowice a fine of **PLN 25,000** for a failure to report to the President of UODO a data breach, and to notify the data subjects about the breach without undue delay. Additionally, the President of UODO required the University to inform its students about the breach.

Background:

UODO received several notifications about a personal data breach. In an investigation it was established that the breach consisted of **uploading on an e-learning platform videos from practical exams in paediatrics with participation of students**. These videos had been made available to each person having a link, without logging in, however, the links had been provided only to other students and lecturers. **The videos contained details from the students' ID and student cards (including PESEL numbers)**.

Conclusions for controllers:

1. When it comes to reporting a data breach to UODO it is irrelevant whether an unauthorised person actually read or came into possession of personal data, in a situation where as a result of a controller's behaviour this person was given such opportunity. Making a controller's reaction dependent on the materialisation of suspected risks is contrary to the GDPR.
2. Publishing videos with images and voices as well as PESEL and ID card numbers, in the context of other data such as year of study, student group, etc, means that there is a high risk of a breach of rights and freedoms, and such breach must be reported to UODO, and the data subjects must be notified.
3. In this case, the mere fact that the data had been made available only to persons being in a relation with the controller (students, lecturers) is not a reason for considering them "trusted recipients" because there is no guarantee as to these persons' intentions. Therefore the risk of violating rights and freedoms cannot be considered to be lower.

The decision is available at:
https://uodo.gov.pl/decyzje/DKN.5131.6.2020

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

Contact :

If you have any further questions, please do not hesitate to contact our experts.

Anna Matusiak-Wekiera
Radca prawny (Attorney-at-law)
Head of Data Protection/
Compliance Practice
anna.matusiak-wekiera@jdp-law.pl

Krzysztof Bąk

Radca Prawny (Attorney-at-law)
Associate
krzysztof.bak@jdp-law.pl

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