Welcome to our data protection newsletter where we discuss decisions issued by the President of the Personal Data Protection Office, which are a source of important information for data controllers regarding i.a. technical and organisational measures in terms of data processing and risk analysis. In its decisions, the President describes in detail what risk analysis involves with respect to putting in place adequate technical and organisational measures – to ensure that data processing complies with the GDPR – and reporting data breaches. In the newsletter we also present the circumstances of imposing the highest-ever fine, interestingly, on not only the controller but also the processor. Enjoy the reading!

Personal data lost as a result of a burglary

In its decision no. DKN.5131.11.2020 dated 30 June 2021 the President of the Personal Data Protection Office (PDPO) fined Lex Nostra Foundation for the Promotion of Mediation and Legal Education **PLN 13,644** for its failure to:

- report a data breach to the President of the PDPO, and
- notify data subjects of the same.

Background:

The President of the PDPO opened proceedings regarding the Foundation after being notified of a suspected violation of data protection regulations consisting in a theft of files with data of 96 beneficiaries of the Foundation, including forenames and surnames, correspondence addresses, phone numbers and most probably PESELs. The files were stolen despite many safety procedures and safeguards being in place. As a result, the President of the PDPO found that the regulations on the obligation to notify a data breach to the authority and data subjects had been violated due to a high risk to the rights and freedoms of individuals.

Conclusions for controllers:

1. If there is a high risk for individuals affected by a breach, a controller is obliged to **immediately inform** these persons about their personal data having been breached. A controller's failure to do so may prevent these persons from counteracting potential damage.
2. The risk should be assessed based on an objective and material analysis (from the perspective of the affected person). **Using available risk assessment calculators may be helpful, however should not be the only basis for assessing risks.**
3. In terms of risk assessment it may be relevant that the controller is unable to precisely indicate the categories of personal data contained in the lost documentation, which could result in inaccurate assessment of the risk of a breach (understated assessment).
4. Employing security procedures and safeguards in business offices does not preclude liability for a data breach. Similarly, reporting a criminal case involving a burglary that resulted in a data loss **does not release from the obligation to report a data breach to a data protection supervisory authority.**

The decision (Polish version) is available at:
https://uodo.gov.pl/decyzje/DKN.5131.11.2020

Loss of data stored on an unsecured data storage device

In its decision no. DKN.5131.22.2021 dated 13 July 2021, the President of the PDPO fined the President of the District Court in Zgierz **PLN 10,000** for failure to put in place appropriate technical and organisational measures ensuring security of the personal data. As a result, personal data protection was breached as the personal data contained on a lost storage device were lost.

Background:

The President of the District Court in Zgierz reported to the PDPO a data breach consisting of a loss of personal data of 400 people being under curator's supervision, including their forenames and surnames, birth dates, residence or stay addresses, PESELs, data regarding salaries and/or property owned, series and number of ID cards, phone numbers, health data and data regarding convictions. **The breach was caused by a loss of a storage device with the data by the curator.**

Conclusions for controllers:

1. A controller may not defend itself by claiming that appropriate security rules operating at the controller were not complied with by the person who caused a data breach, **because it is for a controller to put in place and employ safeguards ensuring security of the personal data processing**.

2. The President of the PDPO held that the data confidentiality and integrity had been breached already when the controller provided curators with **an unsecured storage medium for business use and obliged them to put in place security measures on their own**.
3. A data controller is required not only to implement and apply appropriate safeguards, **but also to verify their effectiveness**.
4. Organising training sessions for employees is not an organisational measure that minimises or eliminates the risk of data loss. Moreover, a training session cannot substitute technical measures.
5. It is required to **periodically verify** the entire system of data protection **in terms of the accuracy and efficiency** of the technical and organisational measures implemented. As stated in the PDPO's decision, **ad-hoc controls are insufficient**, and control measures should be taken in a prescheduled manner.

The decision (Polish version) is available at:
https://www.uodo.gov.pl/decyzje/DKN.5131.22.2021

Liability for a lost parcel

In its decision no. DKN.5131.16.2021 dated 14 October 2021 the President of the PDPO imposed a fine of **PLN 363,822** on Bank Millennium S.A. for failure to:

- report a data breach within 72h after becoming aware of a breach, and
- notify data subjects about a breach.

Background:

The complaint underlying an investigation was filed after data had been lost during opening an account in the Bank. During the investigation it was established that data of two persons containing their forenames and surnames, PESELs, permanent residence addresses, bank account numbers, CIF numbers (identifiers assigned to the Bank clients) had been lost when being transported by a courier from one Bank branch to another. The controller assessed the risk caused by this breach as medium (ENISA methodology), therefore it did not notify the data subjects or the President of the PDPO about it.

Conclusions for controllers:

1. A controller is not required to notify the supervisory authority about a breach if after an investigation it turns out that **the risk to the rights and freedoms of individuals is unlikely to materialise. The supervisory authority may request a controller to justify its decision to not report a breach.**
2. A thorough risk assessment enables the supervisory authority to react appropriately, increasing thereby the chances for avoiding a breach's negative consequences for individuals. A breach should be assessed

by a controller in terms of the risk to the rights or freedoms of a specific person affected by this breach.

3. When it comes to the obligation to notify an individual about a data breach, it is irrelevant whether this person suffers any negative consequences of the breach; important is the mere likelihood of such risk.
4. **When assessing risks in order to determine a controller's obligations related to a data breach, it is irrelevant whether an unauthorised person actually came into possession and read the content of personal data of other persons, but the mere risk of it**, and hence potentially a risk to the rights and freedoms of data subjects which due to the data scope should be assessed as high.
5. A postal operator is only an intermediary for the actions taken by a controller, **therefore it does not release a controller from its liability for a loss of personal data**.

The decision (Polish version) is available at:
https://www.uodo.gov.pl/decyzje/DKN.5131.16.2021

Warsaw University of Technology

In its decision no. DKN.5130.2559.2020 dated 9 December 2021 the President of the PDPO fined the Warsaw University of Technology **PLN 45,000** for a breach consisting in particular of its failure to:

- take appropriate technical and organisational measures to ensure confidentiality of data processing in an IT system,
- take into account a risk associated with the processing of user passwords in an app.

Background:

The Warsaw University of Technology, being a controller of personal data of students, lecturers and candidates placed in an IT system of the university, breached personal data of 5013 people, including forenames and surnames, parents' forenames, birth dates, residence or stay addresses, PESELs, email addresses, usernames and/or passwords, mother's birth names, series and numbers of ID cards, and phone numbers. Having become aware of a high risk to the rights and freedoms of individuals, the controller notified relevant law enforcement authorities and secured the affected IT resources. The personal data were lost due to operation of malware (backdoor file) that enabled an unauthorised person to get access to the personal data. During an investigation it was established that the technical measures being in place were insufficient to secure the personal data.

Conclusions for controllers:

1. In each individual case technical measures should be taken **after carrying out a risk assessment** in terms of data processing. Otherwise, it is highly questionable whether the measures implemented are effective and adequate.
2. Using a hash function for passwords stored in ICT systems **is one of the most common measures ensuring password confidentiality and enabling only the password user to know it**. Negative consequences of a potential risk of unauthorised use are thereby limited.

The decision (Polish version) is available at:
https://www.uodo.gov.pl/decyzje/DKN.5130.2559.2020%20

Santander Bank Polska S.A.

On 19 January 2022 the President of the PDPO issued a decision no. DKN.5131.33.2021 whereby it imposed a fine of **PLN 545,748** on Santander Bank Polska S.A. seated in Warsaw for its failure to notify, without undue delay, the data subjects about a data breach.

Background:

One of the Bank's employees, after the end of the employment with the Bank, still had access to the PUE ZUS platform containing personal data of the Bank's employees, such as PESELs, forenames and surnames, residence or stay addresses, and information on sick leaves, i.e. health data. During an investigation it was established that the former employee not only had access to the data but also used the database several times, also after the employment termination.

Conclusions for controllers:

1. As the President of the PDPO stated, **trusted recipients include entities that operate within a given organisation or are e.g. a supplier whose services a controller uses permanently. There is an actual link, often a legal relationship, between the entities that allows to assess the level of trust**. In case of such recipient, a controller can presume that he or she is familiar with applicable data protection procedures and will behave appropriately.
2. It cannot be assumed that a former employee will behave appropriately in given circumstances, therefore he or she cannot be considered a trusted person.
3. A controller cannot refrain from notifying data subjects about a data breach claiming that there is no specific group of data subjects affected, as in this situation a controller may, for instance, issue a public announcement in this regard.

The decision (Polish version) is available at:
https://uodo.gov.pl/decyzje/DKN.5131.33.2021

Highest-ever fine for improper control over data processing

In its decision no. DKN.5130.2215.2020 dated 19 January 2022, the President of the PDPO imposed the following fines:

- **PLN 4,911,732** on the data controller Fortum Marketing and Sales Polska S.A. seated in Gdańsk for its failure to take appropriate technical and organisational measures ensuring security of the personal data, and to verify the processor in terms of ensuring implementation of appropriate technical and organisational measures in line with the GDPR,
- **PLN 250,135** on the data processor PIKA Sp. z o.o. seated in Gdańsk for its failure to take appropriate technical and organisational measures to ensure security of the personal data.

Background:

The processor made changes to an ICT system, as a result of which an additional customer database was created. As it turned out later, the server where the database was stored was not properly secured, and consequently the database was copied by unauthorised people. It is worth mentioning that the controller learned about it from internet users who found out that they could access the database without authorisation. The personal data of over 120,000 were disclosed.

Conclusions for controllers:

1. A controller is required to **demand** a processor to **analyse the risks and to present concepts of changes to functional and technical projects and alternative solutions** if a processor takes measures improving the efficiency of its services.
2. Despite security procedures implemented by a controller, a controller is also required to **supervise the process of implementing changes to the applicable standards**.
3. Implementing security measures by a controller is not a single procedure. Instead, it is a continuous process in which a controller should verify and update the employed solutions.
4. Stipulation of processor periodic **audits** in a data processing agreement should be **practical**, which means that a controller cannot rely only on contractual provisions but must also be able to prove that the required controls are carried out.

The decision (Polish version) is available at:
https://www.uodo.gov.pl/decyzje/DKN.5130.2215.2020

Contact:

If you have any questions, please contact our experts directly.

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