SK&S PRIVACY INSIGHT

Quarterly magazine on data protection law

30 YEARS | SK&S SOŁTYSIŃSKI KAWECKI SZLĘZAK

In this issue

WHISTLEBLOWERS VS THE GDPR – THE DRAFT OF THE WHISTLEBLOWER PROTECTION ACT

A FEW COMMENTS ON THE BILL AMENDING CERTAIN ACTS IN CONNECTION WITH THE DEVELOPMENT OF E-GOVERNMENT

FIRST FINE FOR INADEQUATELY PROTECTING WHISTLEBLOWERS' PERSONAL DATA

DECISIONS OF EUROPEAN AUTHORITIES - THE PROCESSOR'S RESPONSIBILITY FOR PROCESSING PERSONAL DATA

POLAND - HEALTH SECTOR CODE OF CONDUCT ON THE PROCESSING OF PERSONAL DATA FOR HEALTH SERVICE PROVIDERS AND PROCESSORS

RECENT CASE LAW - THE MOST IMPORTANT JUDGMENTS AND DECISIONS IN THE AREA OF DATA PROTECTION

JUNE 2022 | NO. 1

Whistleblowers vs the GDPR – the draft of the whistleblower protection act

Sylwia Macura-Targosz
Senior Associate, attorney-at-law
sylwia.macura-targosz@skslegal.pl
+48 694 415 447

When analysing employers' new obligations under the EU Directive on the protection of whistleblowers and the draft of the whistleblower protection act, one cannot forget about the GDPR's provisions and the processing of personal data in connection with whistleblowing. This is because, in this process, the employer is the controller of the data collected throughout the process and the whistleblower and other persons mentioned in the notification are the data subjects.

The (second) draft of the whistleblower protection act published on 12 April this year aims to implement the EU Directive on the protection of whistleblowers.[1] It is worth recalling that Poland was obliged to adopt the above-mentioned act by 17 December 2021. Currently, the draft act is at the stage of renewed inter-ministerial consultations.

What regulations does the current draft act contain? What should we pay attention to? What else would it be worthwhile regulating?

- **The whistleblower's personal data is not only their name and surname** but also *"other information from which the identity of the whistleblower can be directly or indirectly identified"* (e.g. information about the specific time or place where the violation took place, position, specific qualifications).

- **The legal basis to process the personal data of the whistleblower and persons named in the notification will be Article 6(1)(c) of the GDPR**, i.e. the fulfilment of legal obligations incumbent on the controller, and such obligation can be found in Article 8 of the draft act, under which, the entity collects and processes data to the extent necessary to fulfil the act's purposes. Unfortunately, the legislator omits the issues related to the processing of special categories of data or data concerning convictions which may be indicated in the notification by the whistleblower.

- **The lack of the obligation on the controller to provide information about the source of data (i.e. about the whistleblower's identity) – exclusion of the application of Article 14(2)(f) of the GDPR.** However, the legislator decided to neither exclude the obligation to provide information under Article 14 of the GDPR at all nor postpone its implementation in time. One should be aware that, sometimes, mere information about pending proceedings may render further follow-up actions pointless.

- **Providing information about the source of data under Article 15 of the GDPR (right of access to the content of the data) later than it results from the GDPR's provisions**, but no later than within 3 months from the date of completion of the follow-up activities. The legislator decided to postpone the realisation of the obligation to provide information about the source of data only (Article 15(1)(g) of the GDPR). The remaining information the controller is obliged to provide within the deadline results from the GDPR.

- **Access to personal data only for persons who have a written authorisation to process personal data or entities with which the controller has concluded an agreement on entrusting the processing of personal data.** Under the GDPR's provisions, the controller may entrust the processing of personal data only to entities which provide sufficient guarantees to implement appropriate technical and organisational measures.

- **Personal data processed in connection with the notification must be stored for no longer than 15 months from the date of the completion of follow-up activities.** In the first draft of the act, this period was 5 years from the date of acceptance of the notification.

[1] Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law

Please remember the GDPR's general provisions!

The draft act does not contain comprehensive or exhaustive regulations in the area of protecting the personal data of whistleblowers or persons indicated in a notification. Thus, controllers, when designing procedures or systems concerning whistleblowers' notifications in the area of personal data, should largely rely on the GDPR's general provisions. Thus, controllers should not forget, i.a. to update the register of data processing activities by adding a new process, or to carry out a personal data protection impact assessment. The President of the Personal Data Protection Office has directly indicated whistleblowing systems as those that require the performance of a personal data protection impact assessment.

The draft act can be found here

A few comments on the bill amending certain acts in connection with the development of e-government

Jakub Derulski
Associate, attorney-at-law
jakub.derulski@skslegal.pl
+48 880 780 275

The bill on amending certain acts regarding the development of e-government was published on 21 April this year and is currently at the early stage of public consultations before being sent to Parliament (details on the bill and legislative work can be found ***here)***. The project's main goal is to remove systemic barriers to the development of e-government, e.g. by creating a framework for a document repository accessible to all public authorities and removing barriers related to the development of digital services.

Changes in the functioning of the GOV.pl portal and the EZD system

The project introduces provisions governing the administration of the GOV.pl portal and the Electronic Document Management (EZD RP). According to the project creators, the portal GOV.pl is to give citizens full access to the collection of information and online services the public administration provides. EZD RP will make it possible to perform clerical activities, document the process of handling and resolving issues, and collect and create documentation in an electronic form. The effect of the changes will be the creation of a powerful and integrated database, allowing for the effective use of the data potential. While the changes themselves are to be assessed very positively, the already prepared data protection impact assessment is not (more about threats in the assessment section).

On the other hand, the precise indication of the Minister of Administration as the data controller contained in the GOV.pl portal is a very good solution which will save the time of citizens whose data is processed, e.g. by directing the request for data changes to one addressee and not to several relevant offices.

Changes in the Act on Identity Cards

A number of far-reaching changes also concern the Act on identity cards. The changes aim to increase the effectiveness and security of processes related to establishing the identity of natural persons. A tool to realise the goals is, i.a. to add a 2-step procedure consisting of verifying the data contained on the identity card with verifying based on a facial image which will be stored in the Register of Identity Cards. In the case of a positive verification, it is planned to generate a report on data compliance. The solution itself will facilitate the activity of entities, especially in the financial sector.

Catalogue of entities authorised to verify databases

The directory of entities that may use the register has been limited to entities for which, in performing their duties, it is necessary to verify customers. In our opinion, to carry out this process in a precise manner, it will be necessary to extend the catalogue which should additionally include domestic banks, branches of foreign banks, credit institutions, and branches of credit institutions, as well as cooperative savings and credit unions which do not operate as payment service providers.

Further changes are envisaged in the law on the Population Register consisting of, i.a. making certain data from the PESEL register available to entities listed in Article 2 of the Banking Law, and cooperative savings and credit unions. In our opinion, the reference to Art. 2 of the above-mentioned act is incorrect because it refers to a catalogue of banking activities and not to a catalogue of entities - this which raise interpretative doubts.

Is everyone ready for change?

The possibility for businesses conducting regulated activities to freely verify data should be assessed very positively. However, the lack of a limit on the purposes and scopes of data processing may, in the long term, raise interpretative doubts both on the part of citizens, other market participants, and supervisory authorities. This conclusion seems to be confirmed by the position of the President of the Office for the Protection of Personal Data presented, respectively, in the communication of 24 July 2019 titled "The ban on replicas of public documents", "Banning replicas of public documents will reduce identity theft", and in a letter to the President of the Polish Bank Association in August 2019. In view of the above, a statutory restriction on the scope of the use of data available in the above-mentioned registers seems to be a good solution.

It is also worth noting the change in law on the national archival resource and archives which is to change the word "may be" to the word "are". The seemingly minor and cosmetic change aims to oblige public entities to carry out tasks related to electronic document management. It might seem that such an initiative should only be viewed positively, considering the nuisance of paper documents; however, the reality may be different. As it stands, these changes may make it impossible for state bodies, state organisational units, and other obligated entities to properly record, store, and protect from damage documents prepared or received in a paper form. If tasks are always to be realised within the EZD RP, this may mean excluding the possibility to keep documentation in a form other than electronic. Such a solution may be a revolution for which not everybody is prepared for at the moment.

Summary of the prepared Data Protection Impact Assessment and beyond, and practical concerns

Although the initiative should be evaluated very positively as a part of the worldwide trend of the computerisation of administration, there are some project provisions that are problematic from the perspective of personal data protection. Below is a brief summary of the improvements and risks associated with the project in terms of personal data.

Changes for the better:

- It is positive that the Data Protection Impact Assessment is carried out for the project itself. Despite the manner in which it was carried out, it is common practice for many laws with data protection implications to omit the legally required Data Protection Impact Assessment. Here, it has been carried out. Unfortunately, there are caveats to the manner in which the assessment was conducted, as indicated below.

- Changes towards the integration of internal systems used by administration (portal.gov and EZD RP) are a milestone in developing modern administration and the modern state. Effectively verifying identity and other information by offices and market participants in central databases is a foundation in the development of a modern state.

- The Act has introduced minor changes resulting in the elimination of minor legal obstacles making life difficult for ordinary citizens. For example, the provisions of the Family and Guardianship Code and the Law on Identity Cards have been amended to allow citizens to change their surname online.

Project Risks:

- The speed and manner of introducing changes generates the risk of the non-compliance of changes with current regulations and ineffectively implementing changes. The introduction of detailed technical conditions, which are crucial for the project's functioning, in the form of a communication of a competent minister and not in the form of a regulation, is incomprehensible from the perspective of the requirements of the Regulation of the Prime Minister on the Principles of Legislative Techniques. And the introduction of the short deadline of 14 days to implement these conditions from the moment of their publication may be a serious challenge hindering the effective implementation of the changes.

- In our opinion, the way the risk assessment of personal data processing is carried out (Assessment) does not meet the requirements described in GDPR and the requirements set out by PUODO in this respect. For example, the Assessment attached to the draft does not include all processing operations resulting from the statutory changes, and the assessment of the described processes, e.g. in terms of risks generated by the creation of an image database, is questionable.

In summary, the bill appears to be a good step forward but it appears that further work on the details of the bill is needed to achieve the legislature's intended goals.

INTERESTING FACTS

First fine for inadequately protecting whistleblowers' personal data

In connection with the growing interest in "whistleblowers issues" and the work on the Polish act regulating the institution of the whistleblower, it is worth drawing attention to the fact that the issue of ensuring whistleblowers' confidentiality and protection of personal data is extremely important if we really want whistleblowers to provide significant information. This fact was also pointed out by the Italian data protection authority GPDP (*Garante Per La Protezione Dei Date Personali*) which, on 10 June 2021, imposed a fine of EUR 40,000.00 on Aeroporto Guglielmo Marconi di Bologna S.p.a., the company managing Bologna Airport. The reason for the fine was the inadequate protection of the whistleblowers' personal data. The Italian controller, implementing a whistleblower protection system, decided to use the "WB Confidential" application provided by the company aiComply S.r.l. In the GPDP's opinion, the personal data processed in the application was improperly secured because access to the application was via an unsecured http protocol which does not guarantee the integrity or confidentiality of data. In consequence, in the GPDP's opinion, the controller did not take appropriate technical or organisational measures to secure the data. The audit also found that the controller did not carry out the "Privacy by design" or "Privacy by default" procedures to evaluate the implemented process which, according to the authority, should have been carried out. The Italian data protection authority referred to the legal basis for processing the personal data of whistleblowers, indicating that such legal basis should be found in Article 6(1)(c), Article 9(2)(b), and Article 10 of the GDPR. In Poland, this issue is still undecided.

ITALY
EUR 40,000.00 EUR

The GPDP decision is available here

Decisions of European authorities - the processor's responsibility for processing personal data

The French supervisory authority (CNIL) issued a decision imposing an administrative financial penalty of EUR 1.5 million on the processor (the Dedalus Biologie company). The financial penalty was imposed on the processor for violating the obligations to: (1) ensure adequate security measures to protect personal data (Article 32 of the GDPR); (2) comply with the controller's instructions (Article 29 of the GDPR); and (3) formalise the entrustment relationship with controllers (customers of the processor).

The processor's breaches led to the disclosure of personal data of more than 500,000 individuals, and the scope of personal data disclosed included health data (information on diseases, e.g. HIV, cancer, genetic diseases or pregnancy, drug therapies, genetic data).

In the case, CNIL pointed out, i.a. that the obligation to enter into a data processing agreement is incumbent upon both the controller and the processor. However, in the case, it was the processor being the service provider that provided commercial documentation that did not include provisions on the entrustment of the processing of personal data or that contained incorrect provisions. Consequently, CNIL held that the processor breached Article 28(3) of the GDPR. Another significant ruling by CNIL is that the processor exceeded the controller's instructions. This occurred by acquiring more data than was required as part of a migration from software to another tool performed (performed at the controllers' request).

The case is interesting because, unlike most cases that attribute liability under the entrustment of processing to the controller, in this case, CNIL attributed such liability only to the processor. Furthermore, CNIL did not address the assessment of whether the controller would incur liability for the data breach in the present case.

The CNIL decision is available here

Poland - Health sector code of conduct on the processing of personal data for health service providers and Processors

Adrianna Gnatowska
Associate, attorney-at-law
adrianna.gnatowska@skslegal.pl
+48 538 628 072

The code of conduct for the health sector is in the final stage of proceedings. The code indicates solutions for personal data protection within the activities of the health sector, including the obligations arising from the GDPR for healthcare entities and the proposed legal basis for processing. The solutions presented in the document will help controllers choose the correct solutions when processing personal data and will contribute to the unification of the approach to these issues on the market. Although the code will not constitute binding legal regulations, acting in accordance with it will increase the controller's level of legal security. Once it is approved by the DPO, the code may become a tool to confirm the entity's compliance with the GDPR and, as a consequence, influence the mitigation of penalties related to the breach of personal data protection provisions. Moreover, the introduction and application of the code ensures an increased level of data protection for data subjects. Under the Act of 23 August 2007 on counteracting unfair market practices, non-compliance with a code of good practices to which the entrepreneur has voluntarily joined may be deemed a misleading action if the entrepreneur states that it is bound by such code within the framework of market practice.

The document is available here

The codes approved by UODO will be found here

JUDGMENTS & DECISIONS

Agata Szeliga
Partner, attorney-at-law
agata.szeliga@skslegal.pl
+48 698 660 648

Katarzyna Klonecka
Associate
katarzyna.klonecka@skslegal.pl
+48 602 151 178

Recent case law - the most important judgments and decisions in the area of data protection

The year 2022 started with the issuance of several significant decisions by the President of the Personal Data Protection Office ("**PUODO**"). In addition to those, there have been some interesting recent court judgments in this area. Below is a summary of the most important conclusions to be drawn from these judgments and decisions:

1 Data protection breach risk assessment guidelines - Santander Bank Polska S.A. (imposed penalty - over PLN 545,000, along with the obligation to notify individuals of the breach; decision available ***here***). Failing to notify individuals of a breach of confidentiality of their data due to a former employee's further access to employees' data on a social security electronic platform.

CONCLUSIONS

- **when assessing the risk connected to a breach, controllers should take into account both the number of persons and the amount of data affected by the breach and the relevant categories of data - breaches that involve special categories of data or a larger set of personal data should always be assessed with more caution.** The large number of people affected by the breach and the extent of the data breached (including information on sick leave which is classified as health data) led PUODO to conclude that the breach posed a high risk of infringing the rights or freedoms of individuals, and so a breach notification was necessary.

- **the actual unjustified use of data is not a necessary factor to assess the obligation to notify the data subjects about the breach. The sole possibility of such a risk is enough.**

- **a former employee does not constitute a 'trusted recipient'** (i.e. a person towards whom data sharing can be considered less risky). Controllers should be more cautious when reacting to breaches involving former employees, regardless of other factors (e.g. training of that employee on data protection while they were still employed) and notwithstanding the fact that an employee who is still working for an controller generally has the status of a trusted recipient (until their employment is terminated). **Suspicious behaviour by the individual, e.g. logging on to the system despite their employment being terminated or a lack of authorisation, should also contribute to a lack of trust.**

- **controllers should implement or review measures to be used if an employment relationship has been terminated with a person who has access to personal data.** Among other things, the controller should terminate such persons' access to any databases.

- **when notifying of breaches, controllers should provide specific information about the breach that meets the requirements under Article 34(1) of the GDPR.** A controller can fulfil this obligation not only by sending a direct message to employees but also through publicly available communication (e.g. on the intranet). It is important that the communication reaches all persons at risk because of the breach and that it clearly indicates that it concerns a specific breach.

2 **It is the controller (and not the employee) who is responsible for implementing data protection measures in the organisation - judgment of the Voivodeship Administrative Court in Warsaw of 15 February 2022 (ref. II SA/Wa 3309/21) upholding PUODO's decision to impose an administrative fine (PLN 10,000) on the President of the District Court in Zgierz.** Aprobation officer lost an unencrypted pen drive containing personal data.

CONCLUSIONS

- **it is the data controller who is responsible for applying appropriate data security measures and the controller cannot transfer the burden of this responsibility to employees.** In the case at hand, the employee received an unsecured pen drive and was obliged to implement security measures themselves. The employee failed to implement safeguards and, as a result, the loss of the medium allowed unauthorised persons to access the personal data contained on the medium (i.e. the data of persons subject to probation supervision and covered by a community interview).
- **the controller should be aware of the safeguards in place in the organisation and their effectiveness.** Making employees responsible for implementing security measures deprives the controller of such information.
- **the controller cannot limit themselves to merely training employees on data protection.** The controller should implement further technical and organisational measures to meet data security requirements.

3 **The right to be forgotten is applicable to press activities - judgment of the Voivodeship Administrative Court in Warsaw of 21 January 2022 (ref. II SA/Wa 1055/21) overturning PUODO's decision on the discontinuance of proceedings concerning the demand to remove personal data from a press article.**

CONCLUSIONS

- Article 2(1) of the Data Protection Act of 10 May 2018 excludes the application of some of the GDPR's provisions to journalistic activities. However, Article 17(1) of the GDPR, i.e. the "right to be forgotten", is not among the excluded provisions. Thus, the **"right to be forgotten" can be applied to press articles.**
- The above ruling changes existing precedent which stated that PUODO is not competent to examine the necessity of erasure of data due to the lack of a legal basis.

4 **Both the controller and the processor are liable for insufficient security measures - Fortum Marketing and Sales S.A. - controller (penalty of over PLN 4.9 million) and PIKA sp. z o.o. - processor (penalty of PLN 250,000); decision available *here*.**

The controller and the processor did not implement appropriate technical or organisational measures to ensure the security of personal data. The controller also did not verify the technical or organisational measures the processor applied before entering into the data processing agreement and during the entrustment.

CONCLUSIONS

- long-term cooperation between the controller and the processor, not supported by audits or inspections, does not guarantee that the processor correctly performs the tasks required by law or by the data processing agreement, and does not exempt the controller from fulfilling its obligations under the GDPR.
- consequently:
  - the controller is obliged, prior to concluding the data processing agreement, to verify that the processor provides sufficient guarantees to implement appropriate technical and organisational measures (implementing Article 28(1) of the GDPR).
  - the controller is obliged to carry out regular audits or inspections of the processor to verify that the processor is complying with its obligations (implementing Article 28(3)(h) of the GDPR). Relying on checklists attached to the agreement or sent prior to the conclusion of the agreement is not sufficient.
- the controller's liability for a data breach does not exclude the processor's liability if the processor directly causes the breach by its action/omission.

MOST IMPORTANTLY

5 **It is possible to use information from the security cameras of a building to check whether a postman placed a letter in a mailbox? Judgment of the Supreme Administrative Court of 15 March 2022 (ref. II GZ 50/22).**

In its ruling, the court stated that, to clarify the discrepancies regarding the correctness of the delivery of registered mail, it would be necessary to ask the manager of the building for information whether the video surveillance recordings show that the postman made an attempt to deliver any correspondence to the addressee. In the case, other presented evidence did not allow this situation to be assessed because the postal operator found it impossible to establish the circumstances regarding the delivery of the mail. Only after obtaining information about what was seen in the camera footage would it be possible to assess whether the correspondence was effectively delivered.

6 **Who can be informed of discontinuing employment? Judgment of the Voivodeship Administrative Court in Warsaw of 29 September 2021 (ref. II SA/Wa 1724/21).**

The employer sent information about the departure of one of its employees to other employees and to one person outside of the organisation. According to PUODO's position, confirmed by the court, the employer may send this information to other employees, nevertheless a non-employee should not receive such information - for the latter, the employer received a warning.

- according to the court's position, providing an employee's personal data while informing others about an employee leaving the company to a person who is not an employee has no legal basis in the GDPR and constitutes a violation of the principle of data minimisation.
- nevertheless, sharing personal data, i.e. information about an employee's departure with their former colleagues, is in line with the GDPR - this sharing can be based on the controller's legitimate interest in the need to reorganise the workforce.
- apart from the issue of personal data protection, the message of the employee's employment termination should also contain content that does not violate the employee's personal rights (i.e., judgments or opinions that violate personal rights should be avoided).

www.skslegal.pl