SK&S PRIVACY INSIGHT

Quarterly magazine on data protection law

SOŁTYSIŃSKI KAWECKI SZLĘZAK

In this issue

JUNE 2023 | NO. 4

Update on the principles for processing personal data in the course of a clinical trial

Katarzyna Wnuk
Associate, attorney-at-law
katarzyna.wnuk@skslegal.pl
+48 602 151 178

In mid-April, the act on clinical trials of medicinal products for human use (hereinafter: the "Act") came into force. For more information on the Act in terms of regulatory requirements, see the summary by J. Myszko and M. Jakubiak available here.

Do data subjects' requests have to be met in the course of clinical trials?

Pursuant to the GDPR, data subjects may exercise specific rights concerning their personal data. However, it results from Article 8 Sec. 1-3 of the Act, that in the course of clinical trials constituting scientific research, it is permissible to restrict the designated rights of data subjects if it is likely that these rights will prevent or seriously impede the achievement of the objectives of such a clinical trial and if the restriction of the rights is necessary to achieve these objectives. An example of such a situation is indicated in the explanatory memorandum to the Act: *possible changes in the personal data of a clinical trial participant that could adversely affect the outcome of the clinical trial, its credibility or the impossibility of publishing the results of the clinical trial should be highlighted. As a consequence, medicinal products developed as part of a clinical trial, whose efficacy has been proven as part of that trial, will not be able to be referred for further activities which may result in their availability for widespread use to the general population. Consequently, the right of others to effective treatment may be adversely affected.*

In addition, it should be emphasized that changes to the personal data of a clinical trial participant resulting in the aforementioned inability to conduct a clinical trial that is a scientific study will adversely affect the rights of other trial participants.

The rights that may be restricted are:

- the right of access (Article 15 of the GDPR) - the restriction may be applied until the clinical trial is completed
- the right to rectification (Article 16 of the GDPR) - the application of this right can be limited during and after the clinical trial
- the right to restrict processing (Article 18 of the GDPR) - the principles of restriction of the right are the same as for the right of rectification
- the right to object to processing (Article 21 of the GDPR) - as above, the principles for limiting the right are the same as for the right of rectification.

The limitations of rights described above do not apply to the following data (what means that the aforementioned rights of access, rectification, restriction of processing, objection can be exercised in relation to them):

- name
- PESEL number (national identification number) or, if no such number has been assigned, the type and number of the identity document and date of birth
- mailing address
- telephone number or e-mail address.

Thus, when receiving a data subject under the GDPR from a clinical trial subject, the entity conducting the clinical trial should bear in mind that it does not have to fully respond to each and every request and comply with its demands; however:

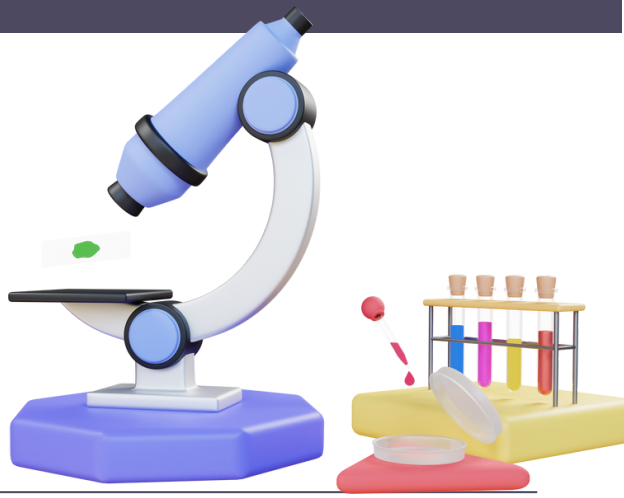
- The law introduces a LIMITATION, not an EXCLUSION, of rights;
- The data controller should be able to PROVIDE EVIDENCE THAT THE LIMITATION REQUIREMENTS under the Act have been met (i.e. it is likely that the fulfillment of requests will prevent/seriously impede the achievement of the objectives of the clinical trial as described at the beginning of this section); bearing in mind that the GDPR requires accountability of actions, the assessment and should be DOCUMENTED
- Please note that the LIMITATIONS DO NOT APPLY TO ALL RIGHTS THAT THE GDPR GRANTS TO DATA SUBJECTS (e.g. it is not possible to limit the right to be forgotten, i.e. the right to erasure under Article 17 GDPR)
- Despite the limitation, the provisions on the exercise of data subjects' rights as laid down in Chapter III of the GDPR apply. (e.g., there is still a time limit of one month in which to respond to a request and, in the event that a request is refused, an explanation of why the request will not be met must be provided within one month).

Data security

Article 8 Sec. 4 of the Act emphasises that, in the course of processing personal data obtained for the purposes of and during a clinical trial, the controller shall implement appropriate technical and organisational safeguards referred to in Article 32 Sec. 1 of the GDPR, having regard in particular to the nature of the personal data processed in the clinical trial and the risk of violation of the rights or freedoms of data subjects processed in connection with the conduct of the clinical trial.

This provision highlights how important it is to properly secure personal data processed in the course of a clinical trial. It may be argued that the requirements indicated therein duplicate the obligations arising from the GDPR, but nevertheless - irrespective of the resolution of the above doubts - it should be important for entities organising clinical trials to properly secure data so that their security is not breached (including unwanted access by a third party or loss of availability of data by the controller). It should be borne in mind that safeguards can be both technical (e.g. data encryption) and organisational (e.g. data access policy based on the minimum access principle).

According to GDPR and the practice of the President of the Personal Data Protection Office, it is important not only to IMPLEMENT appropriate safeguards, but also to VERIFY THEIR EFFECTIVENESS and REGULARLY TEST THEM. The data controller should ensure data security not only in its own systems, but ALSO IN THE SYSTEMS OF ITS PROCESSORS (by means of contractual provisions with the entity, as well as regular security audits).



Is the consent for the processing of personal data in the course of a clinical trial still necessary?

The Act repeals the basis for two Polish regulations that indicated the need to collect consents for the processing of personal data in the course of a clinical trial (i.e. consents under the GDPR, which are not consents to participate in a clinical trial), namely the Regulation of the Minister of Health of 2 May 2012 on Good Clinical Practice and the Regulation of the Minister of Health of 12 October 2018 on the templates of documents submitted in connection with a clinical trial of a medicinal product and the application fees for the initiation of a clinical trial. These regulations are now deemed to have been repealed.

The above means that the provisions explicitly indicating that a separate consent for the processing of personal data is necessary for data processing in the course of a clinical trial have been deemed to be repealed. As a consequence, grounds for data processing other than consent may be considered in the course of clinical trials, including reliance on European guidance in this regard (e.g. European Data Protection Board Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR)).

The use of consent as a basis for processing personal data in the course of clinical trials does not seem appropriate for a number of reasons. The above-mentioned opinion of the EDPB indicates that consent is not an appropriate basis for processing in the case of any clinical trial due to doubts about its 'voluntariness'. Similar doubts are expressed in the explanatory memorandum to the Act, where it is pointed out that, *although the processing of personal data of trial participants has so far been based on their explicit consent, both the provisions of the GDPR and the EDPB Opinion issued on the basis thereof, indicate that other legal bases for the processing of personal data - in particular in the form of the basis indicated in Article 9(2) (j) of Regulation 2016/679 (processing is necessary for the purposes of scientific research), which allow for greater consistency with the principles of clinical trials - can be applied. The use of the legal basis based on the necessity of the processing for the purposes of scientific research seems to be the correct position (...).* Also, consent can be withdrawn at any time, which creates a risk for the integrity of the database collected during the trial.

From preliminary consultations with the relevant authorities, it appears that the authorities approving the clinical trial documentation may still require consents for the processing of personal data. However, we have not received any binding information in this regard.

In our view, in the light of the above-mentioned change in the law, it will be justified to consider other grounds indicated in Articles 6 and 9 of the GDPR for the processing of personal data in clinical trials.

Age verification of minors on social media platforms - theory versus practice. Possible tightening of existing requirements in the European market, France a precursor to change.

Agnieszka Jurcewicz-Androsz
Associate, attorney-at-law
agnieszka.jurcewicz-androsz@skslegal.pl
+48 600 782 823

Online danger

Protection of a child in the digital world is an issue of great interest. Access to the web allows minors to be exposed to harmful and illegal content and behaviour that can affect their proper development. Bullying, solicitation for sexual purposes or self-harm, promotion of attitudes leading to unsafe eating practices, phishing, identity theft, cyberbullying by peers, as well as possible access to content and products reserved for adults, are not all the risks of the digital world for children and young people.

Given the above, and the huge popularity of social media platforms such as TikTok, Facebook, Instagram or YouTube among minors (both under 13 and 18 years of age), it is important for the European forum to effectively regulate both the legal and factual issues related to the verification of the age of children registering on these platforms and the possible consent of their guardians to such registration. The solution worked out here could later be applied by providers of other online services.

Age requirements on social media platforms

Officially, a person aged 13 or over can become a user of most social media platforms. Depending on the social media platform, certain features (e.g. the ability to send direct messages, profile privacy settings or the ability to do "live" reporting) and adult content are excluded for those between 13 and 18 years of age. This is to ensure greater safety for children in the digital world. The operation of these functions, however, is subject to the user's indicated date of birth or age as provided during registration.

Verification and processing of children's personal data

Existing European regulations on the processing of children's personal data, if the basis of the processing is consent, allow for self-consent for such processing when information society services are offered directly to a child who is 16 years of age or older (however, member states may provide for a lower age limit, but they must be at least 13). If the child is younger, the processing of the child's data will only be lawful if the child's legal guardian consents (Article 8(1) RODO). In Poland, in the case of children between 13 and 16 years of age, two declarations containing consent to the processing of personal data - of the child, as well as of the child's legal guardian - should be submitted. In turn, the Audiovisual Media Services Directive (2010/13/EU the "Directive"), implemented in Poland into the Broadcasting Act of 29 December 1992, requires the adoption of appropriate measures to protect children from harmful online content, including the use of tools to carry out age verification of users of video-sharing platforms with regard to content that may harm the physical, mental or moral development of minors (Article 28b(3) of the Directive).

It should also be pointed out that Article 8(1) of the RODO, by setting an age limit from which children may in some cases consent to the processing of their own data - implicitly - establishes the need to verify their age (Article 8(2) of the RODO). Thus, Internet service providers should effectively verify the age of users to determine whether a user can have an account on a particular social networking platform at all (so long as he or she is at least 13 years old) and, if so, what settings will be appropriate for him or her in relation to his or her age (on some platforms in Poland, it will depend on whether he or she is 13-16 or 16-18 years old). In addition, when processing personal data on the basis of consent, in the case of information society services offered directly to the child, they are obliged to check the child's age and, if necessary, they should also obtain the consent of his or her legal guardians for the processing of personal data (e.g. in the case of processing the child's personal data in order to present him or her with personalized advertisements). They must make reasonable efforts to do so, taking into account the available technologies on the market.

Children register on platforms by overstating their age

Unfortunately, research conducted in July 2022 by Ofcom (the UK state body that controls and oversees the media and telecoms market) found that a third of children aged 8 to 17 who have a social media profile register with a false date of birth as an adult. It also found that the majority of children aged 8 to 17 (77%) who use social media - where the minimum user age is 13 - currently have a profile on at least one of the big platforms. What's more, the research suggests that 60% of children aged 8 to 12 who use these platforms are registering with their own profile (meaning they are providing false age information). Among this group of minors, almost half set up at least one of their profiles on their own, while the rest using the help of a parent or guardian. The results also suggest that 47% of children aged 8 to 15 with a social media profile declare (by overstating their age when registering) that they are older than 16, and 32% of children aged 8 to 17 falsely declare that they are older than 18. Among the younger age group, 8 to 12 year olds (a group that theoretically should not be able to access such services at all), the study estimates that 39% have a user age profile of 16+ and 23% have an age profile of 18+, also as a result of overstating their age when registering.

The study carried out shows that the way social media platforms verify age, based on a user's declaration of age (most often by providing their date of birth), is ineffective. As a result: (i) a large group of children under the age of 13 have their own profile on at least one of the social media platforms as a result of providing false age data during registration; (ii) children are exposed to content and settings unsuitable for their true age and maturity attained also as a result of overstating their age during registration. Similar conclusions were presented by the Age Verification Providers Association (AVPA) in September 2021, which signalled that there is little or no actual verification of a user's age in most EU Member States when offering goods, content or services online, and that self-declaration is an ineffective solution. Also in recommendation No. 7 of the French data protection authority Commission Nationale de l'Informatique et des Libertés ("CNIL") of 9 August 2021, it appears that 44% of children aged 11-18 have lied about their age on their social media platforms.

Proceedings – protection of children's data

At this point, it is important to mention some of the ongoing and concluded proceedings concerning the processing of children's personal data online in a way that does not comply with RODO. In September 2022, the Irish Data Protection Commission submitted a preliminary decision to other supervisory authorities within the EU, following proceeding investigating TikTok's compliance with the RODO data protection by design and default requirements for the processing of personal data in the context of platform settings for users under 18 and age verification measures for those under 13. We look forward to the decision.

The Information Commissioner Office issued a decision on 4 April 2023 and fined TikTok £12.7 million. The authority pointed out that TikTok, among other things: processed the personal data of children under the age of 13 (i) which is contrary to TikTok's terms and conditions, and (ii) without the consent of legal guardians which is in breach of the RODO. In addition, the company "did not do enough" to check who was using the social networking platform's services and did not take "sufficient action" to delete the data of children under 13.

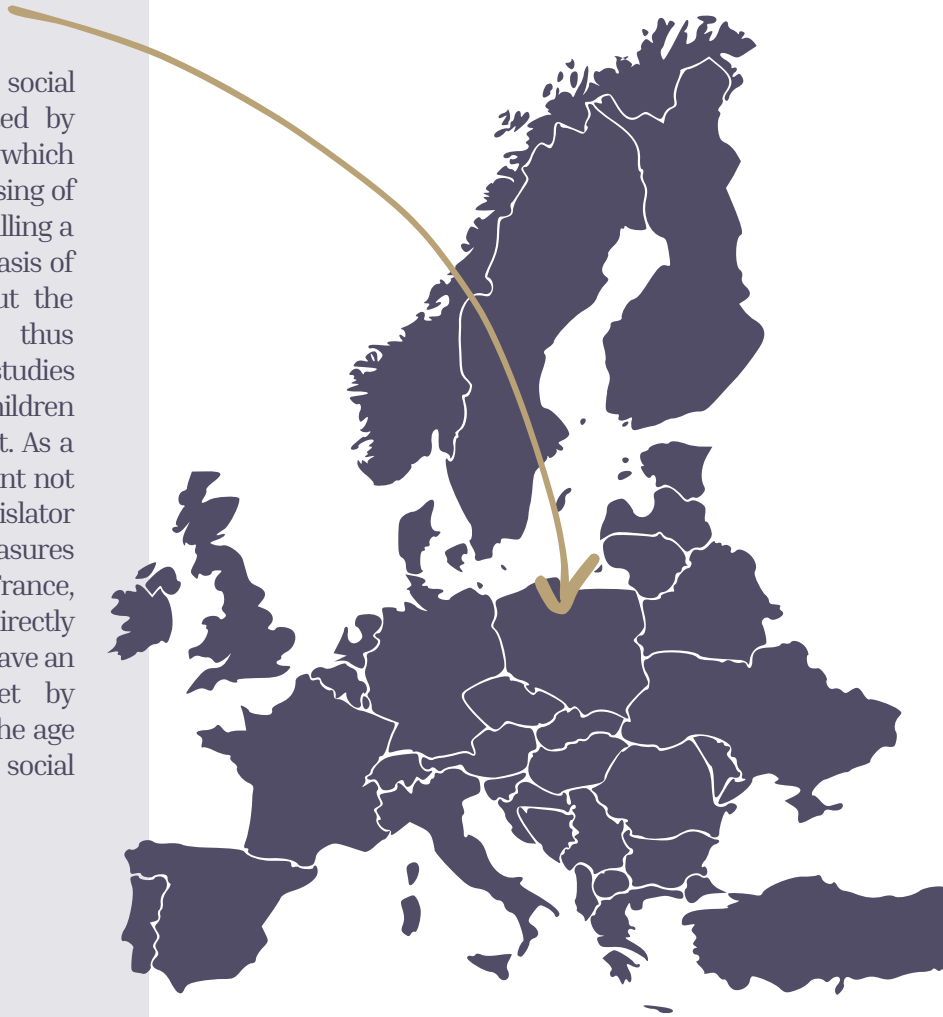
Potential solutions

The above indicates that the age-setting mechanisms used by social media platforms are not effective. On the other hand, it is difficult to find solutions that are both simple and adequate. This is confirmed by a CNIL opinion of 22 September 2022, which concludes that current age verification systems are either (i) too intrusive (e.g. those using credit card or facial analysis; it was pointed out that if they were to be used at all, they should be used through a trusted third party) or (ii) very easy to circumvent by the user such as the age declaration. The opinion clearly indicates that age verification should guarantee the confidentiality of the information and the principle of minimising the data collected should be respected. CNIL is developing a demo programme that, through an independent third party and its system, would verify the age of the user respecting these principles.

The French administration is taking steps to force owners of social media platforms to reliably check the age of their users. Legislation adopted in May by the French Parliament is to, among other things, force the owners of social media platforms (e.g. TikTok, Instagram or YouTube) to verify the age of their users and require parental consent for those under 15. Parents are also to be empowered to delete the social media account of a child under the age of 15. Hefty penalties of up to 1 per cent of a company's annual global turnover are foreseen for non-compliance with the above rules. Technical solutions - verifying the age of users will have to be approved by ARCOM (*l'Autorité de régulation de la communication audiovisuelle et numérique i.e. the regulatory authority for audiovisual and digital* communications) and CNIL. ARCOM would also be empowered to sue service providers failing to comply with existing regulations. A version of the law is currently being worked on by both chambers of the French parliament. In addition, a system of double anonymity is being tested in France. Users verify their age or digital identity on a third-party site or platform, which generates a token. The token is then used on a website that requires age verification.

Situation in Poland

In theory, an account on most social media platforms can be created by children from the age of 13, which immediately involves the processing of their data for the purpose of fulfilling a contract and often also on the basis of legitimate legal interest, without the need for separate consent, thus involving parents. As the studies indicated above show, children overestimate their age by default. As a result, they have access to content not intended for them. The Polish legislator is not currently planning measures similar to those implemented in France, but it should be assumed that indirectly the French regulation may also have an impact on the Polish market by indicating viable ways to verify the age of users registering on social networking platforms.



Summary

Verifying the age of users online is complicated in particular by the lack of effective technical means to carry out effective age verification while respecting confidentiality and minimising data. The current testing of new technical solutions and the planned technical guidelines of the French regulators may set a general trend for the verification of children's data in Europe.

New tool for data transfer to the US is on the way

Maciej Jakubowski
Associate, attorney-at-law
maciej.jakubowski@skslegal.pl
+48 882 630 942

Since the CJEU ruling in the Schrems II case, the transfer of personal data to the United States has faced many difficulties. Works to find a remedy are in progress. Recently, the European Data Protection Board issued an opinion on the proposed solutions.

Data transfer under the GDPR

The GDPR sets out rules for data transfers to third countries, i.e. transfers of personal data to recipients located outside the European Economic Area. The transfer will generally take place in situations where data is made available to a controller in a third country, or where data is stored on servers located outside the EEA. The size of the transfer or its frequency is not relevant in determining the principles on which the transfer should rely. The main goal of the regulation's provisions is to ensure that the level of protection guaranteed by the GDPR is not weakened when personal data is transferred to third countries or international organizations. Therefore, various tools have been introduced to legalize the transfer. One of them is the so-called adequacy decision issued by the European Commission (EC). Under it, a third country can be deemed to offer an adequate level of protection, which means that data can be transferred to another entity in that third country. In such cases there are no additional conditions and the data exporter does not have to provide further safeguards.

Data transfer to the United States

There was a time when the transfer of personal data to the United States was possible based on the adequacy decision called Privacy Shield. The situation changed after the judgment of the Court of Justice of the EU (CJEU) in Case C-311/18 (Schrems II).

In the course of the proceedings, the Court examined the scope of application of the GDPR, the rules for transferring data to third countries, the competence of supervisory authorities including the admissibility of transferring personal data to the United States. One of the main outcomes of the judgment was that the level of protection provided by Privacy Shield was deemed inadequate, which led to the annulment of the decision. Since then, the transfer of data to the US requires additional actions from entities interested in legalizing such a transfer. Often these actions require additional costs and labor.

Work on a new adequacy decision

Currently, both sides, the US and the EU, are taking steps to develop new solutions, which would end with a new adequacy decision for the US. In February, the European Data Protection Board issued a non-binding **Opinion 5/2023** on the draft EC decision. On the one hand, EDPB was pleased with introduced changes, including the principles of necessity and proportionality of data collection by US intelligence services and a new mechanism for judicial remedies for EU data subjects. On the other hand, they expressed concerns on issues of data subjects' rights or bulk data collection. EDPB's opinion is not binding. The Commission might take it into account when preparing the final text of its decision on the appropriate level of protection. The draft decision will then be submitted to a committee of member state representatives for approval. The Commission is expected to adopt a final adequacy decision in mid-2023. The adoption of the new adequacy decision should stabilize the issue of data transfer to the US.

JUDGMENTS & DECISIONS

Principles of the controller's liability in case of a hacking attack – the Supreme Administrative Court (NSA) overturns PUODO's decision on Morele.net

The second-highest penalty imposed by the Polish Data Protection Authority (PUODO) (PLN 2,830,410, equivalent to EUR 660,000) on Morele.net Sp. z o.o. has been overturned by the NSA. The case is now back before the PUODO.

The penalty concerned a leak of customer data of an online store, as a result of which a hacker sent SMS messages aimed at obtaining access to data in the bank account of the store's customers. The **PUODO found that the controller used insufficient safeguards during data processing which did not protect against the hacking attack, including, among other things, using inadequate authentication methods to access the data.**

The PUODO's decision was upheld by the Provincial Administrative Court in Warsaw (judgment of September 3, 2020, ref. II SA/Wa 2559/19). Nevertheless, the NSA disagreed with both PUODO and the Provincial Administrative Court.

Technical security of personal data

The NSA's verdict raises an important issue regarding adequate data security. The NSA stated that the controller (processor) is not responsible for the mere fact of an illegal act of a third party (hacker) that led to unauthorized access to data, but for the inadequate level of security measures in place allowing such access. This is because unwanted access to data by a hacker can occur even if the highest level of security is applied. Thus, **it follows from the judgment that the obligation to adequately secure data is in a duty of care, not of result.** As the NSA points out, "*a violation of the provision is not determined by the mere circumstance of unauthorized access to data, since such a state of affairs is potentially possible even with the highest level of security.*"

This is important, because from the PUODO decision in the Morele.net case it resulted that the controller would be responsible for any unauthorized access to data, despite the fact that the GDPR requires that safeguards are tailored to the specific situation, including the risk to data subjects of processing their data. The NSA's ruling "rationalizes" the requirements and increases legal certainty. The NSA also points out that the implementation of technical measures should be based on a risk assessment and that the assessment of the adopted security measures should be "dynamic." Safeguards that could have been objectively required of the entity on the date and in the circumstances of unauthorized access to the data (rather than measures that are effective in every case) should be considered adequate.

Organizations processing data should therefore be sure to meet organizational and technical standards that are aligned with current risks. In addition, a proper risk analysis will help justify the above measures. These measures will be strong arguments in cases of data protection breaches, including possible hacking attacks.

Rules of PUODO's proceedings

The NSA also pointed out that PUODO staff did not have the authority to evaluate the security measures implemented by the data controller at the time of the decision, and that an expert opinion should have been conducted during the proceedings. The PUODO did not make it plausible that it had the knowledge to evaluate the technical measures in the precedent-setting case under consideration. However, the NSA stressed that it is questionable whether PUODO handled cases similar to the one in question in their past practice and whether it had the competence to assess the correctness of the technical measures without appointing an expert. In addition, the NSA pointed out that at the time of the proceedings and decision, the GDPR was a relatively new regulation. This thesis is controversial because such knowledge should theoretically be expected from PUODO employees. PUODO itself filed a letter to the NSA on the matter, pointing out that "*the NSA's ruling undeniably and in a precedent-setting manner calls into question the independence of the PUODO as a supervisory body, as well as undermines its competence and the substantive qualifications of its employees, which are necessary to perform the tasks for which the body was established.*"

The NSA also had doubts about the objectivity of the PUODO. The court pointed out that the authority should take into account a party's requests for evidence seeking to prove facts which are favorable for it, if there are doubts or gaps in the necessary information. This is also important from the perspective of a party's right to defence.

The NSA also pointed out that in the case under review, the PUODO did not provide the party with the conclusions of the security measures analysis, preventing it from actively addressing them and making them known to the party only after the decision was issued.

The above encourages active participation in the proceedings before the PUODO and the expression of doubts about the PUODO's approach to the case by submitting appropriate motions for evidence to challenge the unfavorable understanding of the situation.

The ruling is available here

Employee's errors cannot justify any delay in notification of data protection breaches

The Voivodship Administrative Court in Warsaw dismissed P4 sp. z o.o. complaint against the decision of the President of the Polish DPA imposing an administrative fine of PLN 100,000.00 on the company for failing to notify the President of Polish DPA within 24 hours of discovering a personal data protection breach.

In the proceedings before the President of Polish DPA, P4 explained that notifying the President of Polish DPA of the personal data protection breach after 24 hours was related to inadvertent mistakes made by the employees of the law firm responsible for sending the correspondence. In the President of Polish DPA's opinion, employee errors cannot justify the delay in notifying the supervisory authority. The Voivodship Administrative Court agreed with this position.

The Voivodship Administrative Court confirmed that, indeed, P4 had not fulfilled its obligation to notify the supervisory authority of the breach in time. The Voivodship Administrative Court also stated that the President of Polish DPA properly determined the amount of the fine, which is adequate to the infringement found and fulfils the intended functions of being both repressive and preventive.

The judgment is available here

Compensation for violation of data protection laws

We have another ruling on the violation of personal rights with personal data in the background. The amount of compensation, in this case, was PLN 20,000, which was relatively high for this type of case. The District Court, in a December 5, 2022 ruling (XXV C 559/22), determined that the Supreme Administrative Court made available online the personal data of women who were working as bailiff assessors in a manner that did not comply with data protection laws. At issue was an un-anonymized excerpt from a ruling of the Supreme Administrative Court, which was publicly available in the Central Database of Administrative Court Decisions between 2016 and 2021, and concerns a particularly sensitive issue, as per disciplinary proceedings. The discovery caused the woman to experience feelings of fear, insomnia, lack of appetite, and a nervous breakdown. The person realized that anyone could have found out about her professional history which contained an element of disciplinary proceedings. In addition to considerations on the grounds of personal rights, the court stressed that the failure to properly anonymize the plaintiff's data and the subsequent posting of a court decision containing non-anonymized data in the Central Judgment Database constituted a violation of the provisions of the GDPR, which in Article 6 lists the cases in which the processing of personal data (and therefore its publication) is lawful.

The judgment is available here

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

Interesting decisions of the President of the Polish DPA in the first quarter of 2023

1. Decision in the PIONIER law firm case - penalty for processing data without legal basis

Personal data cannot be processed without legal basis

On 30 November 2022 the President of Polish DPA imposed a **fine of PLN 45,000.00** on the partners of the PIONIER law firm civil partnership for violating the rules of personal data processing by processing the data of potential clients of the controller, including health data, without legal basis, in particular without obtaining consent for data processing.

The activity of the partners consists of providing legal assistance in representing clients injured mainly in traffic accidents before insurance companies and courts in order to obtain compensation in their favour. The partners established contact with potential clients on the basis of Press materials, information in social media, etc. During the first conversation with potential clients, verbal consents were obtained to process client data until a contract was concluded. The shareholders did not record the orally-obtained consents in any way.

In the President of Polish DPA's opinion, the controller should be able to demonstrate **the legal basis for data processing to the supervisory authority, including explicit consent to data processing**. In this case, the shareholders were unable to provide evidence of such consents.

The decision is available here

2. Housing association decision - penalty for failing to report a data breach, failing to notify affected persons, failing to have a data processing entrustment agreement in place

On 7 February 2023 the President of Polish DPA imposed **an administrative fine of PLN 1,500.00** on a housing association for several failures in the activity of the controller, including failure to report a data protection breach, failure to notify the persons affected by the breach, and failure to have an agreement to entrust the processing of the personal data of the members of the housing association.

In this case, the theft of a copy of a notarial deed held by the housing association's administrator resulted in a breach of the protection of the personal data of the members of the association. The housing association did not choose to notify the President of Polish DPA of the breach. In the opinion of the President of Polish DPA, the controller was obliged to provide a notification because the risk of negative consequences for the members of the association was higher than negligible.

What is more, according to the President of Polish DPA, the administrator should also notify about the incident the persons whose data was in the stolen document in order to enable them to counteract any potential harm related to the theft of the document. The administrator's failure to take such action was also the reason for the penalty imposed on the housing association.

The association also failed to enter into a data processing entrustment agreement with the association administrator. The administrator also failed to verify the processor before entrusting that entity with the personal data of the community members for processing.

The decision is available here

3. Failure to cooperate with the supervisory authority exposes the controller/processor to a financial penalty

The tasks of the supervisory authority include, inter alia, monitoring and enforcing the application of the provisions of the GDPR in its territory. In order to fulfil these tasks, the supervisory authority has been granted a number of powers, including the right to obtain from the controller and processor access to all data and necessary information, access to premises, equipment and means of data processing. The controller's / processor's non-cooperation with the supervisory authority is subject to financial sanctions where the lack of such cooperation hinders the authority's prompt and thorough investigation of the case.

Lack of cooperation with the supervisory authority may take different forms, but the most common is not answering the controller's / processor's correspondence or leaving such correspondence unanswered.

Examples of decisions in which the President of Polish DPA has imposed administrative financial penalties in this respect are available here:

- Decision
- Decision
- Decision

4. Private carriers used for data processing at data controller

The PUODO imposed a fine of PLN 30,000.00 on the Szczecin-Center District Court in Szczecin due to the failure to implement adequate security measures for data processing using portable storage devices.

The aforementioned Court suffered a data protection breach in the form of the loss of three data carriers containing personal data, including two private carriers that were not encrypted.

As it turned out, despite the existing ban on the use of private media, the controller did not supervise employees' compliance with the ban and did not implement technical measures corresponding to the ban (e.g. USB port locks). The controller should have verified the implementation of the organizational measure of banning the use of private media.

The PUODO stressed that data carriers should have been verified by the IT department and secured against unauthorized access by third parties (especially if lost).

Failure to implement the above measures led to a violation of personal data protection.

The decision is available here

INTERESTING FACTS

Italian regulator first to deal with ChatGPT

ChatGPT, a chatbot developed by the Open AI company that is capable of answering questions using natural human language and can also mimic other people's writing styles, using the Internet as its database, is breaking new records in popularity. Meanwhile, Italy became the first EU country to block its operation within its borders in March 2023 with immediate effect.

Indeed, the Italian DPA found that there were privacy concerns related to the ChatGPT operating model including:

- Lack of adequate information explaining what data is collected by Open AI
- Lack of a sufficient legal basis to justify the mass collection and storage of personal data to "train" the algorithms underlying the platform
- Despite the fact that the service is aimed at people over the age of 13, there were no features which verified the age of users.

Thus, the supervisory authority called on Open AI to take appropriate corrective actions. The developers of ChatGPT did not wait to make corrections. They introduced a new privacy policy and an "incognito" mode. In addition, users are informed that activating a conversation means confirming that the user is at least 13 years old and has parental consent to use the service. The service also requires a date of birth during registration [see our article on age verification policies].

It is worth highlighting the extent of privacy improvements made, cooperation with the regulator and the pace of work. As a result, as of April 27, 2023. ChatGPT has been made available again in Italy. On the other hand, the above shows that not all relevant issues are always taken into account at the solution's design stage in accordance with the privacy by design principle, and especially in such important cases, the regulator's quick reaction allowed for quick elimination of irregularities.

Illegal processing of employee health data - Finnish supervisory authority penalty

The Finnish supervisory authority imposed an administrative fine of €230,000.00 on Viking Line Oy Abp (a passenger ferry management company) for unlawful processing of employee health data.

The Finnish supervisory authority's proceedings were initiated by a complaint from a former employee who requested access to his personal data, including information about his sick leave and diagnostic information. According to the former employee, the controller had stored his health data in the personnel system for 20 years. In addition, according to the complainant, some of the recorded diagnosis information was incorrect, as it was not possible to enter all diagnosis codes into it. The complainant, despite his request, did not receive all his personal data stored in the systems of his former employer.

According to the Finnish Data Protection Act, it is unlawful to store diagnosis information in combination with other employment data.

According to the Finnish supervisory authority, the controller is entitled to process information in the personnel system about when and for how long the employee was absent from work due to illness (permissible reason, payment of sick pay). However, information on the reason for sickness absence, e.g. illnesses, injuries, diagnostic information, should not be stored in conjunction with the HR system. **Health information must be kept separately from other personal data concerning the employee.** Health data should be deleted immediately when its storage is no longer necessary. The Finnish supervisory authority found that incorrect diagnosis information had been stored for too long and could pose a risk to the legal protection of the individual. The controller did not take measures to ensure that the data it stored was accurate and free of errors. In addition, Viking Line Oy Abp failed to adequately inform its employees about the processing of their personal data.

The decision is available here

High fine for WhatsApp Ireland for data protection breach - Irish supervisory authority

The WhatsApp Ireland platform has been fined an administrative fine of €5.5 million by the Irish supervisory authority (Data Protection Commission - DPC) following a binding decision by the European Data Protection Board in a dispute resolution case dated 5 December 2022.

The dispute in this case primarily concerns the legal basis on which WhatsApp Ireland relied in processing users' personal data following the platform's 2018 update to its terms of service. According to WhatsApp Ireland, the user, by accepting the updated terms of service, entered into a contract with WhatsApp Ireland and therefore the legal basis for the processing of personal data is Article 6(1)(b) of the GDPR. According to the complainant (a user from Germany), WhatsApp Ireland relied on consent as the basis for the processing of personal data (when updating the terms and conditions, users were asked to click "I agree and continue").

Following an objection (under Article 60(4) of the GDPR) by several of the supervisory authorities to the draft decision submitted by the DPC in this case - the case was referred to the EROD (under Article 65 of the GDPR). The EROD found that WhatsApp Ireland generally could not rely on a contract as a legal basis for the processing of personal data. Consequently, the EROD instructed the Irish supervisory authority to take into account the breach of Article 6(1) of the GDPR and the breach of the principle of fairness under Article 5(1)(a) of the GDPR.

The DPC's and the EROD's decisions are available here

Data processing in the advertising business - Spanish code of conduct for advertising businesses

Since 28 January 2023, a code of conduct for advertising business operators approved by the Spanish supervisory authority (Agencia Española de Protección de Datos - AEPD) has been in force in Spain. The AUTOCONTROL (Association for the Self-Regulation of Commercial Communication) Code of Conduct "Data Processing in Advertising Activities" **focuses primarily on the handling of complaints by data subjects against the activities of businesses related to unsolicited advertising (spam)**.

One of the most common grounds for complaints submitted to the AEPD is precisely spam. The submission of complaints through AUTOCONTROL will allow complaints to be dealt with more quickly under the mediation procedure applicable to the processing of data for advertising purposes. The Code provides for voluntary and free mediation. The mediation procedure is to last 30 days. The controller's representative has 15 days in which to present a settlement solution. If the mediation procedure fails, the complaint will be forwarded to the supervisory authority.

The Code is available here

Does our dog's name constitute our personal data?

In most cases - no.

However, the UK's Data Protection Authority (Information Commissioner's Office, ICO) has issued a decision showing that in certain cases a pet's name can constitute personal data of the owner.

The case at hand concerned a request for information regarding a police dog. The request was made by a person injured by that dog who requested, inter alia, the name of the dog and its handler, as well as the dog's police records, documentation of its training, etc.

However, entering the dog's name in an internet search engine revealed the name of the dog's handler (this data was included in newspaper articles found on the web). Given the possibility of identifying the dog's handler by the dog's data, it was concluded that the dog's name constituted personal data.

The authority stated that the assessment is the same with regards to people from the handler's work who, even if the information was not public, would know who owned a particular dog once its name was disclosed to them. Thus, in the discussed situation, the dog's name identified its handler, albeit indirectly (personal data is information that allows both direct and indirect identification of the data subject).

However, this decision relates to an exceptional situation where the details of the dog and handler were disclosed online and the name of the police dog specifically identified its handler and allowed him to be recognized by other police personnel. It should also be noted that other information relating to the dog did not allow its handler to be identified and therefore did not qualify as personal data.

In our view, this approach does not justify the general assumption that an animal's name will constitute personal data of its owner or keeper. In most situations, the animal's data will not constitute personal data of its owners since they do not allow even indirect identification. This should be borne in mind; after the described decision was issued, conclusions started to be spread suggesting that as a consequence of this decision the data protection rules should also apply to all animal names.

The decision underlines how important it is to consider the context of a particular case when assessing whether specific information constitutes personal data, and how complex it can be to determine whether or not information is personal data. Indeed, the ICO has not stated that an animal's name is always personal data of its owner/handler. The specific circumstances will determine the assessment in this regard. The same rules apply to the assessment of all other information that can be linked to a specific person.

AUTHORS:

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

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

Maciej Jakubowski
Associate, attorney-at-law
maciej.jakubowski@skslegal.pl
+48 882 630 942

Agnieszka Jurcewicz-Androsz
Associate, attorney-at-law
agnieszka.jurcewicz-androsz@skslegal.pl
+48 600 782 823

Katarzyna Wnuk
Associate, attorney-at-law
katarzyna.wnuk@skslegal.pl
+48 602 151 178

www.skslegal.pl