SK&S PRIVACY INSIGHT

Quarterly magazine on data protection law

SOŁTYSIŃSKI KAWECKI SZLĘZAK

In this issue

THE DSA AND DMA FROM A DATA PROTECTION PERSPECTIVE

DATA TRANSFERS OUTSIDE OF THE EEA - CURRENT STATE OF THE LAW

HIGH FINES AND A BAN ON THE AUTOMATED RECOGNITION OF CITIZENS USING BIOMETRICS AND INFORMATION DOWNLOADED FROM THE INTERNET

MORE PENALTIES FOR FAILING TO ADEQUATELY PROTECT WHISTLEBLOWERS' PERSONAL DATA

BROAD INTERPRETATION OF THE SPECIAL CATEGORIES OF PERSONAL DATA ACCORDING TO THE CJEU

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

OCTOBER 2022 | NO. 2

The DSA and DMA from a data protection perspective

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

The European Parliament and the Council of the EU approved two regulations intended to be legal pillars of the future digital sector. The new provisions will apply to entities such as social networks, cloud service providers, and search engines. The regulations will also affect issues related to personal data processing.

New regulations vs. the GDPR

Both the Digital Services Act ("**DSA**") and the Digital Markets Act ("**DMA**") work alongside to the rules laid down by the GDPR or other Union legislation on personal data protection and privacy in communications. On the contrary, these regulations are intended to complement the existing acts, contributing to the creation of uniform standards to protect the individual in the areas of transparency of processing, profiling, and consent. Thus, the basic act in the field of personal data protection remains the GDPR.

The Digital Services Act

The DSA regulates intermediary services provided to recipients established or resident in the Union, regardless of the location of the providers of such services. The providers of intermediary services, hosting services, or online platforms are to be considered providers of indirect services under the regulation. The DSA's purpose is essentially to establish new rules between a platform and a human (service recipient). On 4 October 2022 the DSA was approved by the Council of the EU. The final step will be the publication in the Official Journal of the European Union. The regulations will start to apply fifteen months after its entry into force.

- **Restrictions on online advertising** - The DSA imposes restrictions on the presentation of targeted advertising using profiling. Under the GDPR, the controller is required to inform data subjects about automated decision-making, including profiling, when processing personal data. In this regard, the DSA complements the above provisions by introducing the obligation to present information about the main parameters used to determine the recipient to whom the advertisement is presented and, where applicable, about how to change those parameters. In many cases, the data used to determine the recipient is, in fact, personal data, e.g. age, gender, or interests. In principle, targeted advertising based on profiling using special categories of personal data, e.g. sexual orientation, religious beliefs, or health data, will be prohibited. Moreover, profiling based on basic and special categories of personal data will not be allowed when the online platform provider is aware, with reasonable certainty, that the service recipient is a minor. At the same time, in this case, it will not be permitted to collect additional personal data, including age, to assess whether the recipient of the service is a minor. The recitals to the regulation indicate that an online platform can be considered to be accessible to minors when its terms and conditions permit minors to use the service (e.g. some social media platforms), when its service is directed at or predominantly used by minors (e.g. gaming platforms), or where the provider is otherwise aware that some of the recipients of its service are minors.

- **Dark patterns** - The DSA also bans the use of manipulative interfaces, i.e. interfaces that, because of their colours, shapes, or images, could mislead users, be used to manipulate, or otherwise materially distort or impair the ability to make free and informed decisions. So far, such methods have often been used to collect consents, including consents to process personal data or as part of accepting cookies (e.g. the use of "non-intuitive" colours).

The Digital Markets Act

The DMA applies much more narrowly as it is addressed to the largest entities in the digital services market, the so-called Gatekeepers. The status of a Gatekeeper will be determined by the European Commission after prior notification by an entity that has reached the thresholds indicated in the regulation. The main goal of the regulations is to set the rules between big platforms and business (including smaller entities operating in the digital market), in particular, by increasing competition. Publication of the regulation in the Official Journal of the European Union is scheduled for 13 October 2022. The regulations will start to apply six months after its entry into force.

- **The prohibition of data merging** - The regulation introduces a general prohibition on merging personal data from different sources without properly granted user consent. This is intended to reduce the advantage of the largest platforms over other players in the digital services market. Under Article 5 of the DMA, Gatekeepers may not do any of the following:

    1. process, to provide online advertising services, the personal data of end users using third-party services that make use of the Gatekeeper's core platform services ;

    2. combine personal data from the relevant core platform service with personal data from any further core platform services or from any other services provided by the Gatekeeper or with personal data from third-party services;

    3. cross-use personal data from the relevant core platform service in other services the Gatekeeper provides separately, including other core platform services, and vice-versa; and

    4. sign in end users to the Gatekeeper's other services to combine personal data.

In the case of refusal or withdrawal of consent for online advertising, the Gatekeeper will not be able to ask for consent again for the same purpose more than once within a period of one year. At the same time, in such a situation, the lack of consent should not result in restrictions on the platform's basic functionalities.

- **Duty to report on profiling methods** - The DSM places great emphasis on the transparency of the Gatekeepers' actions. This will be reflected in the obligation to submit to an independent audit, a description of the basis on which consumer profiling is performed. The audit will examine whether personal data is used for profiling, its purpose, duration, impact of such profiling on the Gatekeepers' services, and the steps taken to effectively enable end users to become aware of the use of such profiling, as well as steps to obtain their consent or provide an opportunity to refuse or withdraw consent. Such report will be submitted to the European Commission.

Summary

The DSA and DMA regulations are an important step towards regulating digital services in the European Union. A crucial element from the perspective of personal data protection is the compatibility of the new regulations with existing laws, resulting in the creation of a coherent system to protect the individual in the digital world.

Data transfers outside of the EEA - current state of the law

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

Since the judgment of the EU Court of Justice that is known as the Schrems II judgment (our alert on this topic is available here), the issue of transfers of personal data outside of the EEA - particularly to the United States - continues to be highly controversial. Below, we highlight the key issues that companies should consider when considering data transfers outside of the EEA.

The practical importance of transfers for business operations

The changing state of the law on data transfers outside of the EEA poses a number of challenges for data controllers, particularly **in the context of using solutions from international providers (e.g. the use of advertising technology, e.g. adtech and the use of other solutions from providers such as Facebook or Google)**. The transfer regulations cover situations where data ultimately goes to a third country and is stored there (data at rest) and situations where data is transferred via a country outside of the EEA (data in transit), as well as where data located in the EU is just accessed from outside of the EEA. **The concept of transfer is very broad and can encompass a wide range of situations related to the day-to-day operation of a business, and potentially even force a change in existing processes.**

Consequences of Schrems II at the EU level - new clauses and recommendations

The Schrems II judgment not only invalidated the Privacy Shield (the basis for transfers to the United States requiring no additional steps on the part of controllers), but also identified additional requirements for transfers. Above all, the judgment shows that **simply relying on standard contractual clauses issued by the European Commission may not be sufficient**. According to the aforementioned judgment, **the effectiveness of these clauses should be assessed in each case in light of the legal circumstances of the non-EEA state and, if necessary, additional data safeguards should be implemented**. Indeed, standard contractual clauses are merely a contract which may not always prove to be effective in light of the applicable laws.

Consequently, **the European Data Protection Board issued recommendations for the implementation of additional - accompanying the standard contractual clauses - safeguards to ensure the effectiveness of the protection of personal data during transfers**, in particular, in light of legislation allowing third-country authorities access to data. The recommendations indicate examples of measures that may complement the standard contractual clauses, including organisational and technical measures and additional contractual measures. The purpose of implementing these measures is to ensure the substantive equivalence of the protection of transferred data with that which is granted in the EU. Controllers may use these guidelines to properly supplement the standard contractual clauses they use.

In addition, the **European Commission has adopted new standard contractual clauses** which are now one of the mechanisms the GDPR allows for data transfers outside of the EEA. These are clauses that controllers should rely on if they want to initiate new transfers and if they have not identified another basis for doing so (e.g. adequacy decisions).

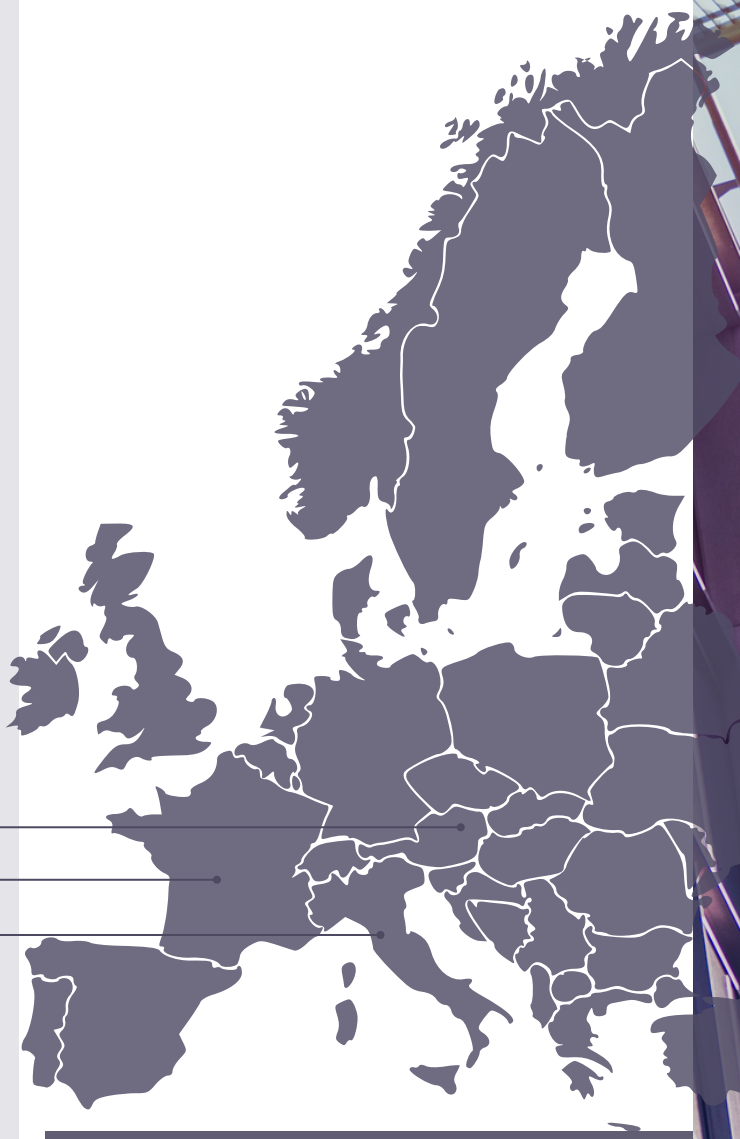
In the case of transfers, the main problem may be that the regulations of a third country allowing its authorities access to data provide overly broad and unverified access to Europeans' data that is not blocked by standard contractual clauses. Such regulations were a determining factor in the invalidation of the Privacy Shield and are being used to undermine the ability to send data to the US in decisions by supervisory authorities and the CJEU.

Decisions of supervisory authorities and practices of other state bodies

The President of the Office for Personal Data Protection (PUODO) has not yet issued its own guidelines related to data transfers but refers to actions at the EU level. However, we can expect PUODO's own position on transfers to be revealed as 5 out of 101 complaints lodged against controllers using Facebook and Google's solutions, carrying out, i.a. data transfers to the USA, have been submitted to Poland (these complaints were lodged by the NYOB foundation after the Schrems II ruling).

Although, in Poland, no information has yet been given on the proceedings pending as a result of these complaints, supervisory authorities in other EU countries have already issued decisions in some cases. **Some supervisory authorities (Spain, Luxembourg) have rejected complaints on the grounds that controllers have stopped using the tools indicated in the complaint.** Interestingly, according to the information obtained from the NYOB, this circumstance did not determine the rejection of complaints in all jurisdictions.

Decisions>>



Some supervisory authorities (Austria, France, Italy) indicated that, by using Google tools making transfers to the United States, controllers were in breach of the GDPR because - despite the standard contractual clauses concluded - the US intelligence services had broad supervisory rights over the tool providers, and adequate protection through the aforementioned clauses was not provided.

Other measures are also being taken at a local level, e.g. in Denmark, the use of Google solutions in schools has been banned.

The above decisions are also likely to serve as guidelines when assessing transfers to other third countries that do not offer the same protection as the EEA.

PLEASE NOTE!

Where transfers of personal data outside of the EEA have so far been carried out based on previously applicable standard contractual clauses, it is necessary to update them. As of 27 December 2022, only the standard contractual clauses issued in June 2021 may be used!

What should controllers willing to transfer data do?

First of all, it should be borne in mind that, for non-EEA countries for which an **adequacy decision has been issued, the considerations indicated in this article do not apply. The decision is a basis for transfers and it is not necessary to add additional safeguards.**

A list of countries for which such decision

When basing transfers on the other grounds indicated in Article 46 of the GDPR, you should:

- identify the data transfer operations outside of the EEA;
- assess whether there are laws or practices in place in the relevant non-EEA state that may affect the effectiveness of the transfer and collateral basis used;
- identify and implement complementary measures, if any, so that the level of protection of the data transferred is substantively equivalent to that under EU law; and
- reassess, at appropriate intervals, the measures in place and the applicable legal provisions.

A Transfer Impact Assessment (TIA) is typically implemented to fulfill the above steps. A TIA is an impact and security implications analysis of the transfer of personal data to a country outside of the EEA for which an adequacy decision has not been issued. It serves to meet the GDPR's accountability requirements. It should be pointed out that such analysis is also required by the provisions of standard contractual clauses.

Is it always worse outside of the EEA?

The focus on transfers to third countries often results in less attention being paid to law enforcement authorities' access to data within the EU itself. It is also worth noting that, here, controversy often arises over access by third parties (including state services) to information on citizens. By way of example, the Panoptykon Foundation, which works for the benefit of privacy, has repeatedly drawn attention to the fact that, in Poland, state agencies have the possibility of surveillance without adequate control, and **cases concerning this have reached the ECHR**. Thus, the model adopted in the guidelines and decisions so far, in which there is an assumption that transfers outside of the EEA are risky (some even forbidden) and their execution requires many additional steps, and that data in the EEA is generally safe, creates the impression of protection remaining largely on a theoretical level.

INTERESTING FACTS

High fines and a ban on the automated recognition of citizens using biometrics and information downloaded from the internet

Data protection authorities in a number of countries, including Greece, Italy, and France have issued decisions regarding breaches of data protection law by Clearview AI, including imposing significant financial penalties on the company (e.g. EUR 1.000.000,00 in Greece and Italy, and GBP 7.500.000,00 in the UK). The supervisory authorities also issued orders to cease the activity and delete databases.

Clearview AI's practices consisted of collecting images from social media and other public sources in an automated manner (web scraping). The mechanism stored any image identified as a human image, along with information about the file (e.g. link to the source page and information about where the image was taken). This data was then identified by an algorithm and matched with other images in the company's database. Access to the database was then sold to private companies and law enforcement or intelligence forces. Once a particular photo was uploaded to the services, these entities were able to identify a specific person and obtain other information collected about that person in the Clearview AI database (a list of all collected photos with links to specific pages and data collected during the web scraping). Thus, the processing of personal data, including biometric data, was conducted (the processing of photos is considered to be the processing of biometric data if it is processed by special technical methods that allow for the unambiguous identification of a natural person or the confirmation of their identity; this results directly from recital 51 of the DPA).

It should be emphasised that, despite the company's creation of an elaborate system, it is now facing a ban on its planned activities in many countries. This shows how important the practical application of the privacy by design concept is.

The authorities' actions described above are part of a broad discussion on the rules for using facial recognition mechanisms. At the EU level, there are voices calling for a ban on the use of cameras using artificial intelligence to scan and identify people's faces in public spaces, and – as reported by POLITICO – the supporters of such an approach are forming a growing group in the European Parliament. On the other hand, employers would like to use such solutions for access to particularly critical information or organisers of mass events could use it to ensure security. Reconciling these interests may be difficult without additional legislation or guidelines, so it is worth observing the work and discussions on such regulations currently taking place within EU structures.

More penalties for failing to adequately protect whistleblowers' personal data

The inadequate protection of whistleblowers' personal data was the reason behind another fine imposed by Italian data protection authority, the GPDP (*Garante Per La Protezione Dei Date Personali*). In a decision dated 4 April 2022, the GPDP imposed fines - both in the amount of EUR 40,000.00 - on the controller, Perugia Public Hospital; and the processor, ISWEB S.p.A., the provider of the system for handling whistleblower notifications.

According to the GPDP's findings, access to the web-based whistleblowing application, based on open source software provided by ISWEB S.p.A., was possible through systems that, without being properly configured, recorded and stored users' browsing data which made it possible to identify individuals using the application, including potential whistleblowers. In addition, employees were not provided with any information about the processing of their personal data for whistleblowing purposes, and the data protection impact assessment (DPIA) was not carried out. This process was also not included in the register of processing activities. In the GPDP's opinion, the controller did not establish adequate technical or organisational measures to ensure an adequate level of security, taking into account the specific risks arising from such processing, which required the implementation of a whistleblowing management system compliant with the "*Privacy by design*" and "*Privacy by default*" principles.

With respect to the processor, the GPDP found a violation in ISWEB S.p.A.'s failure to regulate its relationship with its hosting provider (the lack of a data processing agreement) both when acting as a processor (for the Public Hospital) and when acting as a separate data controller (for its internal services, e.g. employee management or accounting and administrative activities).

The GPDP decision with respect to the data controller is available here

The GPDP decision with respect to the processor is available here

Broad interpretation of the special categories of personal data according to the CJEU

On 1 August 2022, the Court of Justice issued a ruling (in case C-184/20) in which it ruled, i.a. on the scope of special categories of personal data referred to under Article 9 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) "GDPR".

The case is the result of a request by the Lithuanian Chief Ethics Commission (the body responsible for combating corruption) to a director of a public institution to make a declaration of so-called private interests. The scope of this declaration includes, i.a. the following information:

- name, surname, natural person identification number, and national insurance number;
- the identification of the legal entity of which the declarant or their spouse, cohabitant, or partner is a member or partner;
- the identification of close or other persons known to the declarant or data with which the relationship could give rise to a conflict of interest.

Part of the above information is subject to publication on the website of the Chief Ethics Commission. The director of the public institution brought the case before a Lithuanian court which, in turn, raised doubts about the compatibility of the anti-corruption legislation in Lithuania and the GDPR, including, i.a. Article 9(1) of the GDPR.

In this case, the Court of Justice indicated that Article 9 of the GDPR ***must be interpreted as meaning that the posting, on the website of a public authority responsible for the collection of statements of private interests and the control of their content, of personal data which may indirectly reveal the sexual orientation of an individual constitutes processing involving special categories of personal data within the meaning of those provisions.***

The Court of Justice held that:

- the mere information on the name of the spouse or cohabiting partner of the declarant's so-called 'legal interest' may provide some information on the life or sexual orientation not only of the declarant, but also of the declarant's spouse, cohabiting partner, or partner (recital 119 of the judgment);
- the scope of Article 9(1) of the GDPR should include data which, by means of intellectual association or deduction, indicates the sexual orientation of an individual (recital 120 of the judgment); and
- the broad interpretation of Article 9(1) of the GDPR is in line with the objective of the GDPR to guarantee a high level of protection of the fundamental rights and freedoms of natural persons and, in particular of their private life, with regard to the processing of personal data concerning them (recital 125 of the judgment).

The Court of Justice's judgment certainly tightens the obligations imposed on controllers. It requires controllers to think more deeply about whether particular personal data can be used by association to disclose special categories of personal data.

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

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

JUDGMENTS & DECISIONS

Another ruling on data processing in recruitment

The Provincial Administrative Court in Warsaw has ruled that an employer has the right to process job candidates' data after the recruitment process is completed to defend against possible claims of discrimination in a ruling dated 4 August 2022 (ref. II SA/Wa 542/22). The court stated that:

- The controller has a legal interest, under Article 6 (1) (f) of the GDPR, to process (solely by storing it) the job candidate's personal data to defend against claims by both the job candidate and other persons who participated in the recruitment process which can be effectively asserted for the statute of limitations for claims from the employment relationship under Article 291 of the Labour Code, i.e. for a period of 3 years from the date the claim became due.

- The controller's legal interest in storing the data of a participant in a recruitment process for a known, predetermined period of time (the statute of limitations on employment claims under Article 291 of the Labour Code) with the potential possibility of using the data in the process does not affect or adversely affect the legal situation of participants in the recruitment process.

- The condition of legitimate interest referred to in Article 6 (1) (f) of the GDPR may relate to a situation that does not exist yet, i.e. a purpose arising from the legitimate interests the controller pursues may be the need to prove the need to assert or defend against a possible claim that does not exist yet. Such processing is not in the nature of "back-up" processing.

Let's recall the PUODO's position on this subject (presented as of 2018).

As a rule, the employer should permanently delete the personal data of a candidate with whom it has not decided to conclude a contract of employment, immediately after the end of the recruitment process, i.e. after signing the employment contract with a newly hired employee, unless other prerequisites authorising the controller to process their data have been fulfilled. The extension of the storage period for application data should therefore be an exception to the rule of immediate deletion and should be particularly justified. In the authority's opinion, it is inadmissible to process personal data "as a backup" with the assumption that the data may possibly be useful in the future, and with reference to the provisions on the statute of limitations for civil law claims.

The judgment of the Provincial Administrative Court goes in the right direction. If the judgment becomes final, employers will have a real chance to defend themselves against possible claims by non-employees, as well as be in a better position to implement their obligation to prevent discrimination in employment.

The Provincial Administrative Court ("WSA") upheld the penalty imposed on Millennium Bank S.A. by the President of the Office for Personal Data Protection ("PUODO")

In its ruling of 1 July 2022, in considering the complaint of Millennium Bank S.A. against the decision of PUODO (II SA/WA 4143/21), the WSA dismissed the complaint and upheld the decision imposing the penalty of PLN 363,832. The judgement is not final.

PUODO imposed the penalty due to finding violations of data protection, involving losing the package that held the client's bank documentation by a delivery service, and the controller not reporting the violation.

In the decision, which was contested later by the controller in court, PUODO critically assessed the actions the controller took on account of the violation, in particular:

- not reporting the violation to PUODO should be considered entirely unjustified based on the given state of facts, especially considering:
  1. a.the internal risk evaluation carried out by the bank based on ENISA indicated a medium level of a risk of violating an individual's rights; and
  2. b.the data lost due to the incident included data covered by banking secrecy, e.g. account numbers and ID number (PESEL), and
- the bank's failure to act regarding this incident indicates a high level of the controller's culpability which is confirmed by the execution of the controller's duties, after finding the violation, that made it impossible for the person whose data was lost to exercise their rights (e.g. by a BIK alert notification).

Simultaneously, PUODO contested, in full, the controller' argumentation based on the thesis that the controller of the data included in lost documentation was really the delivery service and it is them who should report to PUODO.

The WSA fully agreed with PUODO. The court stressed that:

- assessing the risk of violating the individual rights of a person whose data was lost should be done from that person's perspective, and that lack of a precise notice, and meeting the requirements of Art. 34 para. 2 of the GDPR prevents the realisation of their rights. A proper notice should include a precise and descriptive introduction of available rights and their purpose is to minimise the consequences of the violation;
- considering that some of the lost documents included data covered by banking secrecy, it is obvious that the Bank shipping the consignment was the data controller. Regarding that data, the Bank independently chose the purposes and means of data processing – in contrast to the data included in the consignment designation which (to the extent necessary for delivery) can be administered by the delivery service; and
- to evaluate the risk of violating individual rights, it is crucial to assess the risk of losing control over data, not only to consider the use of that data.

The judgment is also important for postal operators since it states that they are generally not to be considered as the data controllers of the data included inside the consignment (with which contents they are often not even familiar). However, they are the controllers of data included in the consignment designation – the sender's and recipient's data – to the extent necessary for delivery.

Monitoring is still resulting in problems

In recent months, there have been some interesting rulings issued by the European supervisory authorities and courts regarding violations related to the processing of personal data in connection with monitoring.

- In a judgment handed down in Ireland (*Doolin v The Data Protection Commissioner [2022] IECA 117*), the Court found that CCTV monitoring had been implemented at the workplace to ensure health and safety at work. The employer informed the employees of the aforementioned processing purposes. The employer, when investigating an incident occurring at the workplace, became aware of the CCTV recordings from the employees' canteen (a tea room). Subsequently, the employer used these CCTV recordings to conduct disciplinary proceedings against the respondent. In the respondent's view, such purpose for using the recordings did not fall within the purposes for which the CCTV was conducted. Ultimately, the court agreed with the employee and found that the processing for the disciplinary proceedings was not lawful and therefore, violated the purpose limitation principle under Article 5.1.b. of the GDPR.

- In Luxembourg, the supervisory authority ("CNPD"), when carrying out an inspection at one controller, found that the controller had not regulated, in its internal documentation, the rules for the processing of employees' personal data for the CCTV monitoring carried out. In addition, the controller could not demonstrate why CCTV monitoring was necessary. The administrator explained that he informed his employees verbally about the CCTV monitoring being carried out; the CNPD considered this to be insufficient. Additionally, the CCTV monitoring provided the constant supervision of employees at their workstations and also covered the area of neighbouring properties. Thus, the CCTV monitoring did not ensure the privacy of the employees and went beyond the purpose limitation principle under Article 5.1.c. of the GDPR. The CNPD also found that the third parties were also not informed about the CCTV monitoring. The controller also carried out GPS monitoring of cars rented to its customers. The customer only learned about the GPS monitoring of these cars from the content of the contract; the CNPD also considered this to be insufficient. Information about the presence of geolocation devices was also not communicated to employees. As a result, the CNPD imposed a fine of almost EUR 5,000.00 on the controller.

- In Poland, in a case concerning the Capital Centre for Intoxicated Persons, the Polish DPA found an infringement of the GDPR's provisions, i.e. Article 6.1. in conjunction with Article 5.1.a. of the GDPR. The breach consisted of the processing of personal data without a legal basis, i.e. the recording and capturing of sound (voice) through the monitoring system operated at the controller. The controller indicated that the purpose of such personal data processing is, i.a. to exercise continuous surveillance of persons for security purposes. The recorded sound (voice) is processed by the controller for a period of 30-60 days (or longer if the recording is to be secured for proceedings). On the other hand, the controller indicated Article 6.1.c of the GDPR as the legal basis for such processing, including the Act on Upbringing in Sobriety and Counteracting Alcoholism, the acts implementing this Act and the statutes of the facility. In its decision, the Polish DPA indicated that the recording of sound (voice) within the framework of video monitoring should be considered redundant and inappropriate and consequently, does not follow from the provisions of the GDPR or the Act on Upbringing in Sobriety and Counteracting Alcoholism.

The above-described cases confirm that, irrespective of the country in which a controller operates, the controller must inform those data subject to monitoring about any monitoring objectives and the monitoring information should be documented. In addition, the monitoring carried out must not be overly extensive.

Information stored in cookies does not always constitute personal data

The Provincial Administrative Court of Warsaw, on 11 July 2022 (ref. II SA/Wa 3993/21), reversed PUODO's decision in which the authority imposed a warning on the company iSecure sp. z o.o., accusing it of, among other things, providing third parties with a user's personal data (obtained by cookies installed on the user's computer) without a legal basis. The court found that:

- PUODO did not explain on what basis it determined that there was a reasonable probability of identifying the user in connection with the IP address and cookie IDs. The Supreme Administrative Court judgment cited by PUODO (19 May 2011, file I OSK 1079/10) clearly indicates that IP addresses cannot always be treated as personal data; moreover, the judgment indicated the conditions for qualifying an IP address as personal data but PUODO did not explain whether they were met in this case. The data protection authority has *"a priori"* assumed that both IP addresses and cookie IDs are personal data.

- The GDPR's provisions do not resolve whether Internet identifiers themselves, e.g. IP addresses or cookie IDs, should always be treated as personal data or as one factor ("traces") that can identify an individual (recital 30 of the GDPR uses the phrase *"may (...) result in leaving traces which, in particular in combination with unique identifiers and other information obtained by servers, can be used to create profiles and to identify those individuals"*).

- There is no basis to conclude that an IP address (regardless of whether it is a fixed (static) or variable (dynamic) address), regardless of who owns it and what the possibilities are of using it to identify an individual, should always be treated as personal data. The same conclusion applies to cookie IDs (consider recital 26 of the GDPR to verify this).

The ruling definitely deserves attention as there is a lack of rulings on this subject in Poland. However, the judgment raises reasonable doubts, particularly regarding the court's position on IP addresses. The judgment is not final.

Interesting decisions of the President of the Office for Personal Data Protection ("PUODO") during the third quarter of 2022.

During the third quarter of 2022, PUODO issued a series of decisions. Their common denominator was the assessment of the risk of a data controller violating an individual's rights. Below is an overview of a few particularly interesting decisions.

1. Decision in the case of Esselmann Technika Pojazdowa sp. zo.o. sp. k.

In this case, the data controller (Esselmann Technika Pojazdowa sp. z o.o. sp. k.) lost its employee's labour certificate. Information about irregularities in data administration was reported to PUODO by the District Chief of Police.

PUODO imposed a penalty of PLN 16,000 for not reporting the violation. In the reasoning of the decision, PUODO stated that losing a document as important as a labour certificate that includes a large quantity of information creates a high risk of an individual's rights being violated.

PUODO also pointed out that, when assessing the risk of violation and consequently, the obligation of reporting a violation to PUODO, the material issue is not if the person whose data was in question made any claims towards the data controller or if anyone actually viewed the data. Instead, the important issue is if, as a result of a document being lost, a third party has the hypothetical possibility to view the data.

2. A third penalty for the Chief National Surveyor

On 5 July 2022, PUODO imposed another administrative penalty of PLN 60,000 on the Chief National Surveyor ("**GGK**"). The reason for the penalty was the failure to report a violation to PUODO and to inform persons whose data was disclosed.

During the beginning of April 2022, for more than 48 hours, Internet users had access to land register numbers published on the site: www.geoportal.gov.pl.

In the decision, PUODO pointed out that land register numbers should be considered personal data, as they enable one to easily determine the personal data of land owners, e.g. ID numbers (PESEL), names, surnames, parent's names, as well as addresses.

The decision confirms the established practice of PUODO to treat land register numbers as personal data. In the reasoning of the decision, POUDO cited the judgement of the Provincial Administrative Court (WSA) in Warsaw (II Sa/Wa 2222/20)[1]. That judgement also concerned the GKK and the court supported PUODO's opinion.

PUODO also stated that assessing the risk of violating individual rights should be done from the perspective of the person affected by the violation and not from the perspective of the data controller's interests, as was argued by the GKK. Failing to inform an affected person about the violation prevents them from properly judging the risk of their rights being breached.

3. Clinical Centre of the Warsaw Medical University

PUODO imposed a penalty of PLN 10,000 on 6 July 2022 due to the failure to report a violation of data protection and to inform the persons whose data was disclosed.

The violation was that the doctor working for the data controller mistakenly placed the data of the wrong patient on a referral to a specialist clinic. Because the mistake involved the name of the patient, the data controller stated that the mistake should not be considered a violation as it did not enable a specific individual to be identified so it was only considered a "non-existing" person. Therefore, the controller decided not to report the violation to PUODO and not to inform the person whose data had been disclosed.

Considering the fact that other types of data included in the referral did enable an individual to be identified (name, address, and ID number), PUODO didn't agree with controller's reasoning and stated that a violation did occur and should have been reported. In PUODO's opinion, the high risk of an individual having their rights violated was also because the disclosed data was "specific data" as defined under Art. 9 of the GDPR and was covered by medical confidentiality.

PUODO stated that the fact that the controller knowingly neglected to carry out his duties also contributed to the penalty being imposed.

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

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

www.skslegal.pl