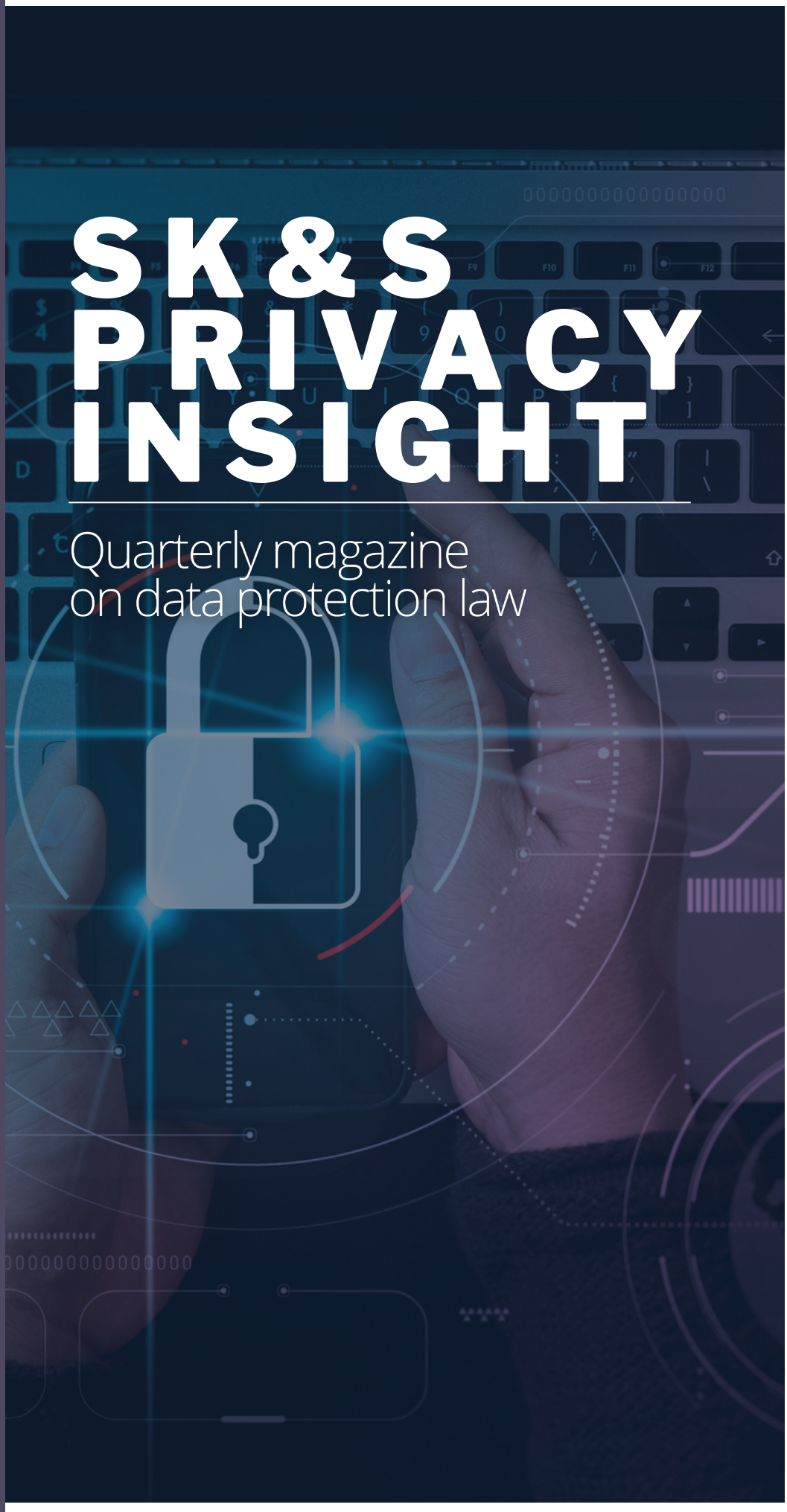


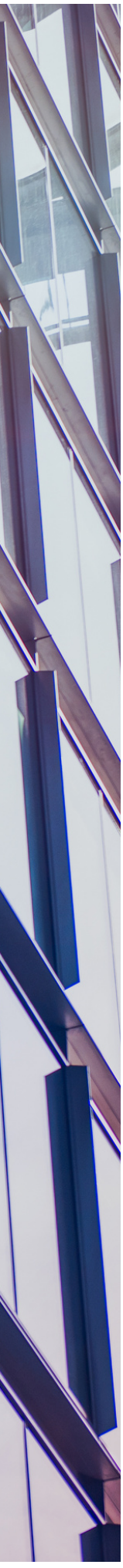
SK&S PRIVACY INSIGHT

Quarterly magazine on data protection law

SOŁTYSIŃSKI KAWECKI SZLĘZAK

In this issue

FEBRUARY 2023 | NO. 3



Dear Readers,

Please find enclosed the next issue of our Data Protection Law Quarterly.

The end of 2022 has been hectic in this field, both in the area of legislation - the Digital Services Act and the Digital Markets Act came into force - and in the decisions and rulings issued. 2023 promises to be just as busy. In the EU work is underway on, among others, the Data Act; in Poland, we can expect the adoption of the Electronic Communications Law.

A brief summary of legislative activities can be found below. We also provide information on recent UODO decisions and court rulings, as well as short articles on changes to employee sobriety testing, and dark patterns in apps and search engines.

We encourage you to read this issue and, if it is not too late, we would like to wish you a Happy New Year!

Agata Szeliga
Partner

Changes in the area of personal data protection in 2023

2023 promises to be an exceptionally busy year for lawmakers. Below is a summary of the main pieces of legislation regarding personal data and privacy that are expected to enter into force or be the subject of legislative work.

Regulations at the EU level

Regulation of the European Parliament and of the Council on a Single Market For Digital Services and amending Directive 2000/31/EC

(Digital Service Act)

Intermediary services (mere conduit, caching, hosting). The regulations will cover a broad category of intermediary services, from simple websites to Internet infrastructure services, and Internet platforms and search engines.

Stage of work:
Finished

- **16 November 2022** – entry into force
- **17 February 2024** – DSA rules apply for all regulated entities, (selected provisions of the DSA will apply in early 2023)

Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts

Introduction of rules for the use of software based on models using artificial intelligence and machine learning technology. Provisions of the act supplement the provisions on automated data processing in the GDPR.

Stage of work:
In progress

Effective date:
The date is unknown

Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828

(Digital Market Act)

Responsibilities of Gatekeepers, i.e. the largest digital platforms with a key role in the digital services market.

Stage of work:
Finished

- **1 November 2022** – entry into force
- **2 May 2023** – DMA rules start to apply

Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC

(Regulation on Privacy and Electronic Communications) (E-Privacy)

Supplementing the GDPR's provisions in the field of online privacy, including the use of information about the user's end device (e.g. the use of cookies and cases where it is necessary to collect consent to track users). E-Privacy also applies to using data from electronic communications and sending direct marketing.

Stage of work:
In progress

Effective date:
The date is unknown

Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, and (EU) No 909/2014

Introduction of unified requirements for the security of networks and IT systems supporting business processes in the financial sector necessary to achieve a high and common level of operational digital resiliency among entities in the sector.

The scope of DORA's application intersects with the scope of the KNF Cloud Communiqué.

Stage of work:
Finished

- **16 January 2023** –entry into force
- Application from **17 January 2025**

Regulation of the European Parliament and of the Council on the European Health Data Space

Creating a centralised health database and supporting the use of health data across the EU. Also, strengthening the rights of individuals concerning their personal data concerning health. Creation of a system enabling the secondary use of electronic health data for the purposes indicated in the regulation.

Stage of work:
In progress

Effective date:
The date is unknown

Regulation of the European Parliament and the Council on harmonised rules on fair access to and use of data

(Data Act)

Determining the rules of access to data and data transfer between cloud service operators. The act sets out clauses that are prohibited in data access and data sharing agreements.

Stage of work:
In progress

Effective date:
The date is unknown

Polish regulations

Act on the protection of whistleblowers

(Ustawa o ochronie osób zgłaszających naruszenia prawa - draft from 5 January 2023

Provide protection to those who report or publicly disclose information about violations of the law obtained in a work-related context.

Stage of work:
In progress (at the draft stage at the Government Legislation Centre)

Effective date:
The date is unknown. (The planned date of the adoption of the project by the Council of Ministers: First quarter of 2023)

Law of Electronic Communications

(Prawo Komunikacji Elektronicznej, PKE)

Replacement of the Telecommunications Law in its entirety, including in the scope of marketing consents and cookie regulations.

Stage of work:
The law has completed its first reading in the Polish Parliament

Effective date:
The date is unknown

Employees' sobriety checks and remote work in the context of the GDPR - amendment to the Labour Code

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

On 13 January 2023, the Parliament passed a law amending the Labour Code and certain other laws ("**Act**"), rejecting all amendments proposed by the Senate. The Act is awaiting the President's signature and publication.

The Act grants employers the right to conduct preventive sobriety checks for alcohol and substances acting similarly to alcohol if this is necessary to ensure: (a) the protection of the life and health of employees and other persons, or (b) the protection of property. Sobriety checks must not violate the employee's dignity or other personal rights and may only be conducted using methods that: (a) do not require a laboratory test, and (b) use a device that has a valid document confirming its calibration or verification. Sobriety checks may be conducted on employees who work at the place of work but also on those who work remotely. Further, not only employees within the meaning of the Labour Code but also those employed on a basis other than an employment contract or conducting business activities may be subject to the checks. The Act also regulates remote work issues.

What regulations does the Act contain and what should we pay attention to in terms of personal data protection?

Sobriety check

- The Act gives employers **a legal basis to process special category personal data (sobriety information is a form of health information)**. The GDPR permits the processing of special category personal data where it is necessary for the fulfillment of obligations and the exercise of specific rights by the controller in the field of labour law, insofar as this is permitted by the law of the Member State with adequate safeguards for the data subject's fundamental rights and interests (Article 9(2)(b) of the GDPR).

- The employer may process a limited **range of data**, i.e. **the date and time of the examination and its result**. This information should be included by the employer in the employee's personal file **and, as a rule, it is deleted no later than one year from the date of its collection** (a longer deadline applies if a penalty is imposed on the employee or if the information constitutes evidence in proceedings).

- The employer is obliged to **regulate the rules of sobriety checks on the same basis as in the case of surveillance** so the regulations on sobriety checks should be included in the collective labour agreement, work regulations, or a notice if the employer is not covered by a collective labour agreement or is not obliged to establish work regulations, and should indicate, in particular, the manner of conducting the checks, their frequency, the categories of employees covered by the checks, etc. Employees should be informed of the possibility of carrying out such checks no later than 2 weeks before they begin; new employees must be told before they are allowed to work.

- The introduction of sobriety checks at the employer **also requires changes/updates to data protection documentation**, including:

  - preparing authorisations for persons conducting sobriety checks on behalf of the employer to process the related personal data, as well as commitments undertaken by these persons to keep the data confidential;

  - updating the information clause for the new processing of personal data; and

  - updating the record of processing activities by adding a new process and retention policy;

- The employer's introduction of preventive sobriety checks should be preceded by a **risk analysis** and, if a high risk of the violation of rights or freedoms is identified, **also by a data protection impact assessment (DPIA)**.

- The need to conclude a data processing entrustment agreement when entrusting the conduct of employee's sobriety checks to an external entity, e.g. an external security company.

Remote work

- The employer will be required to **define procedures for the protection of personal data** and provide training in this regard, as necessary. The employee will be required to confirm that they are familiar with these procedures and to apply them.

- The procedures should regulate, in particular, the rules for the use of electronic equipment (private as well as provided by the employer), and the rules for the circulation of documentation in the company (paper as well as electronic). The employer will be required to provide appropriate measures to ensure the security and confidentiality of personal data processed through remote work.

- The employer's introduction of the possibility of remote work should be preceded by a **risk analysis**, and if a high risk of the violation of rights or freedoms is identified, also by a **data protection impact assessment (DPIA)**.

The Act is available **here** (the version passed by the Parliament on 1 December 2022 after reviewing the Senate's amendments).

Dark patterns in light of the new regulations

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

Dark patterns - definition

By dark patterns we mean the interfaces and mechanisms used on websites that lead users into making unintended, unwilling, and potentially harmful decisions, including decisions regarding the processing of their personal data. In addition to data protection laws, dark patterns may also violate consumer protection laws.

Examples of dark patterns:

- displaying choice buttons differently (e.g. consent - in green, refusal - in red),

- repeating requests to the user to make a choice, in particular, through the frequent display of pop-ups,

- presenting a 'wall' of information to get acceptance of certain practices,

- presenting too many options that make it difficult to make a choice or cause the user to overlook certain settings; as a result, the user may opt out of or overlook data protection settings, and

- making the unsubscribe process more difficult than the subscription process.

Dark patterns in light of the GDPR

The GDPR's provisions do not directly regulate dark patterns. However, by its nature, dark patterns may lead to violations of fundamental data protection principles, in particular, the principles of lawfulness, transparency, or accountability (Articles 5(1)(a) and 5(2) GDPR). Mechanisms that make unsubscribing more difficult than subscribing make such consent defective under Article 7(3) GDPR. Meanwhile, presenting a "wall of text", e.g. as part of information about the processing of personal data, breaches the obligation to inform data subjects in a concise, clear, intelligible, and easily accessible form in clear and plain language (Article 12 GDPR). In the context of dark patterns, it is also worth mentioning the principle of data protection by design and the principle of data protection by default (Article 25 GDPR). The issue of dark patterns in light of the GDPR was not widely addressed by supervisory authorities in their decisions. This does not mean that the problem has been completely overlooked. In 2022, the **European Data Protection Board issued Guidance 3/2022 on dark patterns in social media platform interfaces**, in which, basic mechanisms of dark patterns and recommendations are presented. Nevertheless, it was decided to take a more decisive step by directly regulating dark patterns in new legislation intended to form the pillars of the EU digital market.

Dark Patterns and the new regulations

The first regulation that directly addresses dark patterns is the Digital Services Act (DSA). According to Article 25 DSA, providers of online platforms shall not design, organise, or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions. Originally, this regulation was intended to apply to all providers of intermediary services* (i.e. mere conduit, caching, hosting services). However, as a result of the compromise, the group of addressees was limited to providers of online platforms. Recital 67 DSA gives a helpful interpretation for understanding dark patterns on web platform interfaces. At the same time, it is pointed out that legitimate practices, for example, in advertising, that are in compliance with Union law should not, in themselves, be regarded as constituting dark patterns.

The second regulation addressing dark patterns is the Digital Markets Act (DMA). The circle of addressees of the new obligations is limited to gatekeepers, i.e. the largest digital platforms with a key role in the digital services market. The DMA indicates that gatekeepers should not engage in behaviour that would undermine the effectiveness of the prohibitions and obligations laid down in the DMA. Such behaviour includes the design used by the gatekeeper, the presentation of end-user choices in a non-neutral manner, or using the structure, function, or manner of operation of a user interface or a part of it to subvert or impair user autonomy, decision-making, or choice. Meanwhile, Recital 63 DMA indicates that gatekeepers are not allowed to make it unnecessarily difficult or complicated for business users or end users to unsubscribe from a core platform service.

Summary

Dark patterns have been present in the digital world for years. With new regulations that directly address these issues and existing guidelines, we can expect regulators to be more active in that field. Now is good time to review the mechanisms in place for compliance with these regulations.

* Examples of intermediary services mentioned in Recital 29 DSA: (i) "**mere conduit**" services: Internet traffic exchange points, wireless access points, virtual private networks; "**caching**" services: the sole provision of content delivery networks, reverse proxies, or content adaptation proxies; "**hosting**" services: cloud computing, web hosting, paid referencing services, or services enabling sharing information and content online, including file storage and sharing.

JUDGMENTS & DECISIONS

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

Licence plates are not personal data - continuation of the previous line of case law of the Supreme Administrative Court

The Supreme Administrative Court (NSA), in a judgement of 3 November 2022 (case no. III OSK 1522/21), upheld the NSA's previous position, according to which, vehicle licence plates are not personal data.

The case concerned a request to gain access to a video-recorder of a police car made under the access to public information procedure. The police refused to grant access to such recording, indicating that it showed images of other persons stopped (apart from the image of the applicant) as well as makes, models, and registration numbers of the vehicles, and thus, providing access to the recording would constitute an infringement of the right to privacy of these persons. The Voivodship Administrative Court agreed with the above argumentation, stating that:

having at one's disposal the registration number, make and colour of the vehicle, it is possible - not necessarily in a simple and easy way (...) - to determine the personal data of the owner of the vehicle (...).

The NSA disagreed with the above argumentation, instead relying on its previous position in its judgment of 14 May 2021 (case no. III OSK 1466/21) which held that:

a car registration number is not subject to the protection stemming from the right to privacy, as it identifies a car and not ***a person****; it should be referred to standard registration numbers consisting of letters and digits, which do not allow associating a car with its owner, and to cases where a car with a registration plate is located or presented without being connected with other information relating to the space-time or in connection with other data, including the image of the persons travelling with it'. (...) Thus, if the definition of 'personal data' refers to natural persons -* ***data relating to a thing (a car) does not constitute information as referred to in Article 4(1) of the GDPR if the identification of the holder of that thing can only be done by accessing the relevant registers or catalogues.***

President of the Polish DPA's position

The President of the Personal Data Protection Office, when giving his opinion on the changes to the Traffic Law in 2020, presented a different position. In the President of Polish DPA's opinion, licence plates constitute the personal data of the vehicle owner as it is information through which it is possible to identify - indirectly - the person who is the owner of the vehicle.

The President of Polish DPA's position is available here

Position of the European Data Protection Authorities

European Data Protection Authorities also take a different position to the NSA, e.g. the UK's DPA ICO, the French DPA CNIL, or the Italian DPA GPDP, which consider that licence plates constitute personal data.

The NSA's judgment of 3 November 2022 is available here

No need to verify reputable processors?

In many decisions, the Polish Data Protection Authority (PUODO) has stated that if the data controller entrusts personal data to another entity (i.e. allows this entity to process data on its behalf and for its benefit, e.g. in connection with the provision of cloud or marketing services), **it is necessary both to sign an appropriate data processing agreement and to perform cyclical verifications of the processor's data security assurance**. This has created a challenge for data controllers, especially small and medium-sized companies using standardised services.

In a recent judgment (judgment of the Voivodship Administrative Court in Warsaw of 19 April 2022 (case no. II SA/Wa 2259/21)) the court stated that controllers entrusting data to good-standing, professional entities ensure the application of organisational and technical measures required by the GDPR (in the case considered by the court, Microsoft was assessed to be such good-standing entity). In such case, when verifying compliance with GDPR's security requirements, it is sufficient to note the fact of concluding the agreement and the steps taken at the launch of the service and to refer to the entity's good standing. Of course, such good standing should be verified (e.g. by checking whether the processor has been sanctioned for breaches of data protection legislation).

It should also be borne in mind that some well-known entities may not be considered as having good standing in the context of personal data protection, e.g. if a decision finds them in breach of personal data protection. Thus, reliance on the good standing of a processor should involve ongoing and careful verification of the market and should be adequately justified in internal documentation.

The judgment of the Voivodship Administrative Court of 19 April 2022 is available

Open Register of Beneficiaries infringes on fundamental rights (including rights to protection of personal data)

By its judgment of 22 November 2022, in joined cases C-37/20 and C-601/20, the Court of Justice of the European Union ("CJEU") declared invalid Article 1 para. 15(c) of Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Article 30(5), (5a) and (9) of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing, as it allowed Member States to make information on the beneficial owners available to any person.

According to the wording of the AML Directive, Member States are obliged to provide access to data on beneficial owners in all cases and to each person. The final scope of the data to be made available was left to the discretion of the Member States. The Directive allowed the data to be made available to any person, including by making them public.

In the judgment, the CJEU emphasised that communicating the information contained in the register to an unlimited circle of addressees may interfere with the fundamental rights to respect for the private and family life of individuals (Article 7 of the Charter of Fundamental Rights of the European Union) and the right to the protection of their personal data (Article 8 of the Charter of Fundamental Rights of the European Union).

It has been emphasised that the public provision of information, e.g. the financial situation of individuals in the register, may lead to the misuse of such knowledge and consequently, create a significant threat to the fundamental rights of the beneficiaries. In the CJEU's view, granting public access to data to protect the public interest is not proportionate in the context of the risks of violating rights described above.

By overturning the Directive's provisions, the judgment has no direct effect on national law; however, in the future, the judgment will have a significant impact on the practice of bodies keeping registers of real beneficiaries, including the Polish Central Register of Real Beneficiaries, e.g. by shaping the interpretation of the notion of legal interest by administrative bodies when providing information from the register. In jurisdictions which, unlike Poland, have chosen to keep registers public (e.g. Luxembourg), the ruling has led to a change in existing regulatory practice and the removal of registers from the internet. Many commentators consider the ruling controversial as it strikes at the principle of the transparency of authorities' actions and is a step backwards in the development of AML/CFT regulations. However, in our view, one has to agree with the view that the public disclosure of the full register may lead to an unnecessary infringement of the fundamental rights of the persons disclosed within, and that the expected effect of the Directive may also be achieved if the register is made available to a narrower public or if the scope of the information made available is limited.

The CJEU judgment of 22 November 2022 is available here

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

A search engine operator must dereference information if the person requesting the removal proves that such information is manifestly inaccurate

The case was initiated as a result of a request made to Google by two managers of a group of investment companies. The request was to remove designated links and images from the list of search results appearing when their names were entered in the search engine. The links included in the request led to articles which were critical of the investment model implemented by the group which the managers considered to be untrue. The request was disregarded by Google which referred to the professional context of the content and the impossibility of determining whether it was true or not.

The case eventually landed in the CJEU which considered it by analysing the interplay between the right to freedom of expression and information and the right to privacy.

The CJEU held that the right to freedom of expression and information cannot be considered to override the right to privacy if at least part of the information contained in the link turns out to be inaccurate and of little relevance to the content as a whole.

Of course, as the CJEU pointed out, it should be borne in mind that the right to data protection is not an absolute right. As a general rule, the right to privacy should be considered as overriding the right of internet users to access information. Nevertheless, each situation must be assessed on a case-by-case basis in light of the specific circumstances, the nature of the information, the impact of the information on the privacy of the individual, the role of the individual in public life, and the public interest in the disposal of the information. Where the information is inaccurate, the CJEU's approach indicated above can be applied.

How is "inaccuracy" of information determined?

The person requesting the removal of the links has to demonstrate the manifest inaccuracy of the content (while the content is of little relevance). **The person should only provide evidence which can reasonably be required of him or her** since the CJEU sought to avoid placing a heavy a burden on the data subject.

On the other hand, as the CJEU points out, the search engine operator cannot be obliged to play an active role in the taking of evidence. The operator must take into account all the rights and interests at stake and consider all the circumstances of the specific situation. **Thus, the operator will be obliged to remove links if it receives relevant and sufficient evidence, adequate to support the request to remove the links and prove that the information is inaccurate.**

If adequate evidence is not received, the operator may refuse to comply with the request although it must have in mind that the requesting person may appeal to a court or supervisory authority.

New obligations for operators who are informed about proceedings

The CJEU has required search engine operators to inform internet users that proceedings (administrative or judicial) are underway for content that may prove to be inaccurate if they become aware of such proceedings.

Separate analyses of photographs

According to the judgment, **the publication of photographs in the form of thumbnails must be assessed carefully as such publication may constitute a particularly serious interference with the right to privacy. If the request for deletion also concerns photographs, a separate analysis (the weighing of interests) is necessary**. The information value of the photos should be taken into account regardless of the context of their publication on the source website. Also, the assessment should consider all content accompanying the display of the photos in a search engine. A separate assessment is required for the situation where photographs are placed as illustrations of articles and opinions and the situation where photographs are displayed outside the context in which they were published on the originating website.

The CJEU judgment of 8 December 2022 is available here

Accountability principle – how say "less is more" does not work in the case of the GDPR

Often, in the context of GDPR, we think about creating excessive documentation, e.g. information clauses, registers, and security policies. Such actions are justified in light of **the accountability principle**. Under Article 5(2) of the GDPR, the controller is responsible for compliance **and must be able to demonstrate compliance**.

In this context, it is worth going back the €17 million fine imposed by the Irish DPA on Meta Platforms (formerly, Facebook) in March 2022.

The investigation was initiated following the notification of twelve data protection breaches between 7 June 2018 and 4 December 2018. During the proceedings, the authority examined compliance with the GDPR and, in particular, the implementation of security measures. Ultimately, the decision focused not on the assessment of security measures but precisely on the implementation of the principle of accountability, in the context of documenting the security measures in place, and how they were implemented. In the decision imposing the penalty, the authority repeatedly emphasised that the documents provided by Meta Platforms during the investigation could be considered analogous to industry best practice and the state of the art. However, **it was not demonstrated that the measures described in the documentation were actually implemented in the organisation**.

The decision's main conclusion is that when it comes to compliance with the GDPR, the saying that "less is more" does not work. **Under the principle of accountability, the controller should not only be able to demonstrate that it has the required data processing documents in place but also be able to prove how the procedures described in these documents have been implemented and how they are actually carried out**.

The decision is available here

Interesting decisions of the President of Polish DPA in the fourth quarter of 2022

In the fourth quarter of 2022, the President of the Personal Data Protection Office issued several interesting decisions.

1. Decision on P4 sp. z o.o. (Play) – a fine for the lack of appropriate technical and organisational measures

On 16 November 2022, the President of the Polish DPA imposed on P4 sp. z o.o. - a provider of telecommunications services of the Play brand - **an administrative fine of almost PLN 1.6 million** for the controller's failure to implement appropriate technical and organisational measures to ensure a level of security corresponding to the risk of data processing by means of IT systems used to record the personal data of subscribers to prepaid services. This led to an unauthorised person gaining access to such data.

The President of the Polish DPA dealt with the case again (after the first President of the Polish DPA's decision on the matter was appealed to the Voivodship Administrative Court, the case went to the President of the Polish DPA for reconsideration) and once again, the President of the Polish DPA found an infringement by the controller.

In this case, in a notification to the President of the Polish DPA of a breach of personal data protection, the controller reported that an unauthorised person gained access to the personal data of almost 115,000 individuals (access to confirmation records of prepaid services) in the scope of names and surnames, PESEL numbers, series and numbers of identity cards, telephone numbers, NIP numbers, and names of entities. Due to the scope of the disclosed data, the breach resulted in a high risk of a violation of the rights and freedoms of natural persons.

In the opinion of the President of the Polish DPA, the violation of the protection of subscribers' personal data occurred as a result of exploiting the vulnerability of the IT system. The procedures implemented by the controller did not contain regulations on regular testing, measuring, or assessing the effectiveness of the adopted technical and organisational measures to ensure the security of processing. Despite the solutions adopted, the controller was not able to detect system vulnerabilities due to the lack of regular testing. In fact, the controller did not undertake such measures at all (the last review of technical and organisational measures was conducted at the administrator in May 2018). According to the President of the Polish DPA, the lack of such arrangements contributed to the personal data breach.

The decision is available here

2. Decision in the case of P4 sp. z o.o. (Play) – a fine for failing to notify of an infringement and the failure to notify

On 3 November 2022, the President of the Polish DPA imposed **an administrative fine of PLN 250,000** on P4 sp. z o.o. for failing to notify the President of the Polish DPA of a personal data protection breach within 24 hours [a shorter deadline than under Article 174a(1) of the Telecommunications Law] of the discovery of the breach, and failing to notify the affected subscriber of the breach.

In this case, the infringement consisted of the automatic sending of a telecoms contract to the e-mail address provided by the customer (an option selected by default in the system) which, however, eventually turned out to be incorrect. The customer immediately informed the controller of the mistake and requested its deletion. The provision of an e-mail address was not necessary for the conclusion of the contract; it was only for the purpose of sending the contract. The contract contained, i.a. data such as first name and surname, residential address, PESEL number, ID card series, and number and telephone number. The President of the Polish DPA became aware of the breach from the person to whom the email with the contract was sent (this person has the same surname as the client affected by the breach). Until the President of the Polish DPA initiated proceedings, the controller did not treat the incident as a data protection breach.

According to the President of the Polish DPA, the controller obtained information about the infringement twice, i.e. the first time at the moment of obtaining information from the customer about the erroneously indicated e-mail address, and the second time with the receipt of the President of the Polish DPA's call for explanations in the case. However, the controller took no action and did not analyse the incident. The controller only notified the President of the Polish DPA of the data protection violation when the President of the Polish DPA initiated proceedings and after reviewing the case file (almost two months later). The controller did not notify the President of the Polish DPA of the breach within the statutory deadline and consequently, also failed to notify the subscriber whose data had been leaked of the incident to enable that subscriber to take preventive measures.

According to the President of the Polish DPA, the controller did not take sufficient technical and organisational measures to enable the verification of the e-mail addresses provided by the customers or additional security for the copies of the contracts sent (e.g. access password sent separately).

The decision is available here

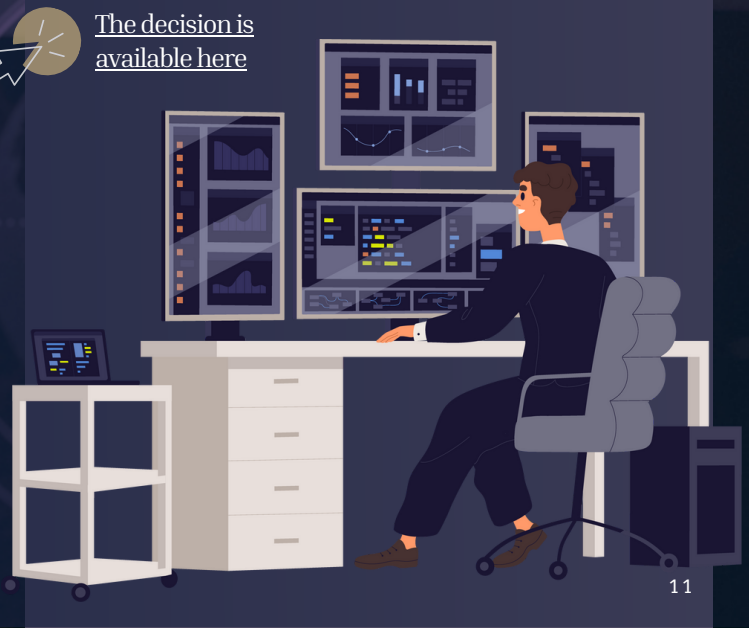
3. Decision in the case of the Head of the Dobrzyniewo Duże Commune - fine for a lack of security on laptops

On 2 November 2022, the President of the Polish DPA imposed an administrative fine of **PLN 8,000** on the Head of the Municipality of Dobrzyniewo Duże for processing personal data in a manner that does not ensure the adequate security of personal data by failing to implement adequate technical and organisational measures and consequently, failing to demonstrate compliance with the principle of "integrity and confidentiality". This constitutes a breach of the principle of "accountability".

In this case, the subject of the breach was the theft of a company laptop with documents containing personal data inside it from the flat of an employee of the Municipal Office. The laptop was protected from unauthorised access only by a password and its drive was not encrypted.

The controller, despite conducting a risk analysis and determining the risk of a threat in the form of computer theft and determining an appropriate technical security measure in the form of the encryption of the computer's hard drive, did not follow the conclusions of the analysis. In the President of the Polish DPA's opinion, this demonstrates a lack of the implementation of technical and organisational measures and thus, a failure to ensure an adequate level of security.
Therefore, it is not only the implementation of procedures that is important but also their application by controllers.

The decision is available here



About the factors determining the risk of the financial consequences of violations

Rules for issuing fines - insights from the Data Protection Authority

When a data protection breach is identified, controllers and their advisors often seek to assess the risk of a administrative fine. Based on the UODO's publications, including those contained in the DPA's newsletter for DPO (No. 10/2022), we present our interpretation of the regulator's approach:

- A fine is only one of PUODO's possible decisions which can be issued as a result of a breach (other possible decisions are, among others, a reminder and the imposition of an obligation to bring data processing operations in line with the GDPR).
- In the case of a data leakage (loss of data confidentiality, e.g. data being sent to an unauthorised third party or accessed by such party), the risk of an administrative fine is high. UODO's practice confirms this; to date, all administrative fines imposed due to insufficient technical and organisational data protection measures have been imposed due to loss of confidentiality (e.g. due to a third party gaining access to the database as in the case of Morele.net or due to the theft of equipment as in the case of SGGW).
- If the breach of data security rules only led to a loss of availability (without loss of confidentiality, e.g. ransomware activity), it is more likely that a reminder will be issued, especially if the taken corrective measures are shown to have significantly reduced - in the DPA's opinion - the risk of the breach reoccurring. It should be pointed out that all of the examples of decisions in the form of a reminder shown in the DPA's most recent report (report for 2021) indeed relate to security breaches resulting in data encryption made by third parties (these are individual examples selected by the DPA). However, it cannot be assumed that, each time, such case will only end in a reminder since breaches are assessed on a case-by-case basis.
- As part of its investigations, UODO also seeks to shape data security practices. Thus, during data security breach investigations, the DPA primarily verifies the following issues:
  - the risk analysis carried out by the controller (including its completeness and comprehensiveness) - in our opinion, it is also important that the results of this analysis are actually implemented within the controller's processes, also while selecting adequate data security measures;
  - the manner and frequency of verifying the security measures in place in terms of their effectiveness, in particular, as can be seen from the DPA's report for 2021 - in terms of vulnerabilities, errors, and their possible impact on the systems and their possible effects on the systems and actions taken to minimise the risk of their occurrence;
  - data backup procedures (which should be sufficiently detailed and should ensure control of the correctness of their creation and the effectiveness of the restoration of personal data) and their effectiveness (e.g. when backups are kept with data used by the controller on an ongoing basis, they may be subject to ransomware attacks which contradicts the function of backups); and
  - IT systems and equipment used for data processing.
- In cases where a controller fails to notify data subjects of a breach, even though the DPA has requested such notification, administrative fines are generally imposed (of course, this refers to a situation in which the controller is passive, not a situation in which it denies the need to comply with the notification). As indicated in the above-mentioned report, only one decision in 2021 concerned non-compliance with an request for action from the DPA (a fine imposed on a health business), and this request concerned precisely the notification of a breach to data subjects.

Not all breaches of the GDPR's provisions may result in damages Opinion of the Advocate General of the CJEU in Case C-300/21

In Case C-300/21 pending before the CJEU, Advocate General Manuel Campos Sánchez-Bordona issued an opinion on the prerequisites for the right to compensation under Article 82 of the GDPR.

Pursuant to Article 82 of the GDPR, any person who has suffered material or non-material damage as a result of a breach of the GDPR's provisions has the right to obtain compensation from the controller or processor for the damage suffered. The regulation contained in Article 82 of the GDPR constitutes what is known as *private enforcement*. This allows any person whose data has been breached to seek judicial protection themselves. Liability under Article 82 of the GDPR applies to both material and non-material damage.

However, the interpretation of Article 82 of the GDPR raises doubts as to the prerequisites for liability under this provision. One of these concerns is the prerequisite of fault. The wording of the Polish language version of Article 82 of the GDPR indicates that this liability is based on the fault principle (a fault covered by a presumption, the rebuttal of which is incumbent on the defendant controller or processor). However, a comparison with the wording of the other linguistic versions of Article 82 of the GDPR supports the view that fault is the prerequisite of this liability. The foreign language versions assume that a controller or processor can be exempted from liability if they prove that they are not responsible for the event that caused the damage ("proof of non-responsibility"). Therefore, it is being raised that liability under Article 82 of the GDPR is rather strict liability.

Case C-300/21 concerns a complaint by a customer of the Austrian postal service, Österreichische Post AG, which published address databases that collected information on the political sympathies of the Austrian public. Using algorithms, Österreichische Post AG recognised people as target groups for election advertising for specific political parties. This data was not passed on to third parties.

The action of Österreichische Post AG sufficiently angered one customer, who felt offended by the fact that Österreichische Post AG recognised him as being sympathetic to a particular political party, which caused him great agitation and loss of trust, as well as a feeling that his character had been compromised. He also did not consent to his personal data being processed for such purposes. The applicant claimed €1,000 in damages for non-material damage (internal discomfort). The courts of both instances dismissed the claim, holding that damages beyond agitation and emotional states (mere discomfort or ordinary feelings of unpleasantness) can be compensable. The case went to the Austrian Supreme Court, which referred three questions to the CJEU for a preliminary ruling.

Is damage a prerequisite for compensation or is a mere breach of the GDPR sufficient?

In the Advocate General 's view, material or non-material damage is a necessary condition for compensation under Article 82 of the GDPR. The opposite answer, i.e. to consider that a mere breach of the RODO provisions gives rise to a right to compensation - irrespective of the fact of damage - would lead to the recognition of criminal liability under the GDPR. In the Advocate General's view, there are no grounds for such interpretation. The GDPR clearly separates the scope of liability for violations in the public law sphere (the possibility for supervisory authorities to impose fines) and in the private law sphere (the possibility for data subjects to claim damages). The Advocate General also emphasises that the interpretation of Article 82(1) of the GDPR does not give rise to a presumption of harm if the GDPR's provisions are breached.

Does the amount of compensation depend on other requirements of EU law in addition to the principles of effectiveness and equivalence?

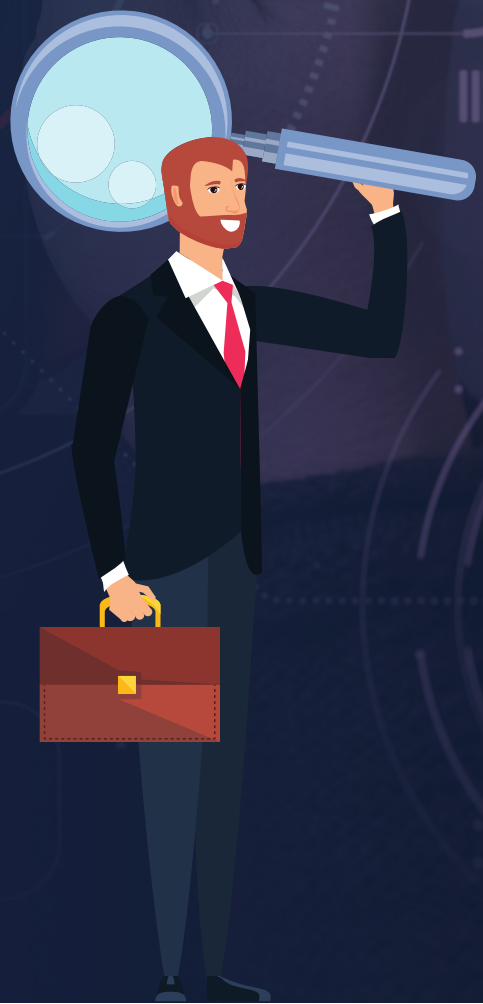
The Advocate General pointed out that the principles of effectiveness and equivalence are not essential as RODO harmonises the regulation of damages. Article 82(1) of the GDPR provides an independent basis to establish the existence of a claim for damages. At the same time, the Advocate General points out that the GDPR does not regulate the calculation of damages. The Advocate General did not exclude the possibility that national legislation may apply to determine damages.

Is the gravity of the breach itself relevant to a finding of non-material damage?

The Advocate General notes that not every non-material damage is compensable. It is important to distinguish between GDPR breaches where there is non-material damage compensable by way of damages and "other inconveniences" resulting from non-compliance with the GDPR provisions which, due to their minor size, would not necessarily give rise to a right to compensation. In the Advocate General's view, "anger or agitation" caused by a breach of the GDPR provisions does not merit compensation.

The Advocate General's opinion may raise doubts as an attempt to limit the right to compensation for non-material damages. The Advocate General allows for the possibility that Member States may create their own 'thresholds' or other national rules that may limit the expressly provided full compensation for non-material damage under the GDPR. In this context, the CJEU's ruling may have important implications for the practice of national courts.

The opinion of the Advocate General of the CJEU in case C-300/21 is available here



INTERESTING FACTS

DPA sectoral audit plan 2023

On 18 January 2023, the Polish DPA (UODO) has published the sectoral inspections plan for 2023. This plan indicates that UODO is planning to inspect:

- authorities processing personal data in the Schengen Information System and the Visa Information System (SIS and VIS) under the provisions of the Act of 24 August 2007 on the participation of the Republic of Poland in the Schengen Information System and the Visa Information System, implementing acts and European Union regulations;
- entities processing personal data in mobile applications in the scope of securing and sharing personal data processed in connection with the use of the application; and
- entities that process personal data using web applications in the same scope as the control of mobile applications.

Interestingly, the first two audited sectors were already indicated in the 2022 inspection plan. UODO's report for 2022, in which a comment related to the repetition could be made, has not yet been published.

It is important to note that inspections related to applications (mobile and web) are not limited to a specific type of entity/sector. Thus, potentially, any data controller may be subject to an audit in this scope. It is also possible that the UODO will start issuing guidelines (and decisions) on relevant topics related to privacy in apps, e.g. cookies or profiling.

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

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

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

www.skslegal.pl