KL&MLAW
Kobylańska · Lewoszewski · Mednis

SELECTED UNPUBLISHED DECISIONS OF THE PRESIDENT OF THE DATA PROTECTION AUTHORITY IN 2022 WITH COMMENTARY

The contents of this publication constitute educational and informational material only and cannot be deemed legal advice.

The publication presents decisions issued by the President of the Personal Data Protection Office in 2022. Given that the authors of the publication intended to present the position of the Authority, this publication does not analyze which of the decisions are final, and against which court-administrative proceedings have been initiated before the Provincial Administrative Court in Warsaw.

English translation provided by VERILANG Tax, Legal and Business Translation • Warsaw, PL • info@verilang.online • 0048 691 810 000

Dear Readers,

we bring you a report on unpublished administrative decisions issued in 2022 by the President of the Personal Data Protection Office ('Data Protection Authority', or 'DPA'). In the report, we discuss nearly eighty decisions that we believe are worth paying special attention to, mainly because of their practical dimension and potential impact on the processing of personal data in companies that rely on data in their business models.

We have divided the report thematically, distinguishing in it several main sections centered around particular sectors of the economy or problems that most of you face in your everyday dealings. As you will see, in 2022 the Data Protection Authority has largely focused on problems relating to marketing and employee data, but also on data processing amidst and relating to the COVID-19 pandemic. A large group of decisions we discuss in the report relate to the broader financial sector, both banking and insurance, but also, for example, to debt collection, health care, and e-commerce, and thus to sectors significant to the Polish economy. In our opinion, this shows which of those sectors process the most data, as well as which sectors the Data Protection Authority has paid the most attention to so far. We believe that this trend will continue in 2023 as well.

We hope that we will be able to prepare similar reports with a summary of the decisions of the Data Protection Authority for you in the years to come as well. Every year, we would also like to invite you to a meeting where we will discuss the report and share our observations, and we would be happy to talk to you about your thoughts in this regard. We already encourage you to register your participation in future editions.

Enjoy the reading.

Marcin Lewoszewski

Partner

Marcin.Lewoszewski@KLMLAW.PL

1. Marketing

Geographical criterion to identify an individual, definition of direct marketing

#direct marketing #warning #databases

September 2022

The Data Protection Authority issued a warning to a company for breaching Articles 6(1) and 17(1)(d) of the GDPR by processing the plaintiff's data including their phone number without a legal basis for marketing purposes, and for failing to comply with their data erasure request. In addition, the DPA issued a warning to the company for breaching Article 14(1)(d) of the GDPR by failing to fulfill the information obligation referred to in the aforementioned provision of the GDPR.

The facts

The business of the company is to arrange product shows and demonstrations. To that end, the company makes telephone calls to telephone numbers to which it attaches no other personal data, including the owners of those numbers.

Here, the company made calls to the plaintiff's phone number to invite them to a product show. Despite the company's efforts to collect additional identification data from the above-mentioned individual, it failed to obtain additional data on the plaintiff. In the company's view, the phone number itself does not constitute personal data, so the company considered it unreasonable to remove it from its database.

Key findings

- ✓ In the course of the proceedings, the Data Protection Authority pointed out that in the contemplated case the plaintiff was indirectly identified through their phone number, as this identification made it possible to distinguish a particular person by narrowing the group to which they belonged. Because the phone numbers held by the company were selected on a geographical basis (which allowed narrowing the group of recipients to the area where the shows were held or services were provided), that criterion was an additional feature that individualized a specific natural person.

- ✓ In the opinion of the DPA, the above facts meant that at the time the company obtained that person's phone number, they were already identifiable by the data, so it is irrelevant whether the company had any additional information about them. Given the above, the company's processing of the plaintiff's phone number constituted the processing of their data.

- ✓ The company obtained the plaintiff's phone number by acquiring a data package (phone numbers) based on a data package agreement concluded with entities selling such databases. Importantly, according to the DPA, the agreement could not constitute a premise legalizing the processing. The DPA stated that a different position would imply that it would be possible to consequentially create a legal basis for the processing in a situation where there was no primary grounds under the GDPR.

- ✓ In the contemplated decision, the DPA also provided its own definition of direct marketing. According to the Authority, direct marketing is understood as the totality of the controller's activities, which, through the transmission of information to individual subjects, are aimed at eliciting a reaction from the data subject which converts into the need of a specific product.

- ✓ Based on the above, the Data Protection Authority found that the phone calls made to the plaintiff's phone number were used to promote the image and services of the company and its affiliates. Thus, the company's actions aimed to elicit a response from the plaintiff and to obtain commercial benefits, which translates into them having been undertaken for the purpose of direct marketing.

- ✓ The company complied with its obligation under Article 17(1)(d) of the GDPR only after having received a summons from the DPA to provide explanations in the case, which, side by side with the failure to inform the data subject of the categories of their personal data being processed by the company, constituted a breach of the provisions of the GDPR and, in the Authority's opinion, deserved a warning.

Processing data for marketing purposes after placement of an order in an online store

#entrepreneur #order #online store #marketing

September 2022

The Data Protection Authority ordered an entrepreneur to erase the plaintiff's personal data the entrepreneur held to run their online store account and processed for direct marketing purposes, based on Article 58(2)(c) of the GDPR.

The facts

The plaintiff pointed out that they had consented to the processing of their personal data by the entrepreneur for the sole purpose of 'processing the order', and yet they had been receiving unsolicited marketing messages. In view of the above, they demanded that the entrepreneur erase their personal data processed in connection with their online store account and from the mailing list maintained for marketing purposes. The entrepreneur did not comply with the plaintiff's request, sending further marketing messages to their e-mail address.

Because of the above, the plaintiff filed a request with the Data Protection Authority for an order to erase their personal data. The DPA called on the entrepreneur three times to provide explanations in the case but received no response.

Key findings

- ✓ According to the Authority, the company was authorized to process the plaintiff's personal data to fulfill the order they placed with the company (to perform the contract). In the Authority's view, after that legal relation was complete and the plaintiff challenged the processing of their data, including for direct marketing purposes, further processing of the data was a breach of Article 6(1) in conjunction with Article 17(1)(a) and Article 21(3) of the GDPR.

- ✓ In light of the decision, it is important to emphasize the importance of the controller's submission of explanations in the course of the proceedings before the Data Protection Authority, because in their absence, the Authority can still – and often does – exercise its remedial powers, including warnings.

The right to easily exercise the right to erasure of personal data

#company #warning #contest

September 2022

The DPA issued a warning to the company for breaching Articles 6(1) and 12(2), (3) and (4) of the GDPR by refusing to erase the plaintiff's personal data published on the website of one of the company's online services.

The facts

The company obtained the plaintiff's personal data in the form of a nickname and e-mail address in connection with the user's creation of a user profile on a site administered by the company, and thus, the conclusion of an electronic services contract. By entering a contest organized by the company following the accepted terms and conditions, the plaintiff voluntarily provided further personal data, i.e. a photo with an image of a tattoo and contact details, available within the user profile they had set up. The plaintiff indicated that they had repeatedly requested that the company remove the aforementioned personal data which the company processes on the service website. The company only erased the plaintiff's data when the Authority initiated proceedings.

Key findings

- ✓ In the opinion of the Data Protection Authority, the company's processing of personal data regarding a nickname and the e-mail address fulfilled the premise of Article 6(1)(b) of the GDPR. In turn, the basis for the processing of the remaining data was Article 6(1)(a) of the GDPR.
- ✓ The Authority found that the request for the erasure of data processed by the company as part of the service simultaneously implied the withdrawal of consent to data processing and constituted a declaration of termination of the electronic services contract, and thus the prerequisites legalizing data processing no longer existed.

- ✓ By equating a request for the erasure of data with a notice of termination may have important practical consequences, especially for contracts of a more momentous nature, such as those in the banking sector.

Unsolicited marketing information and data processing without a legal basis

#order #warning #marketing

September 2022

The Data Protection Authority ordered an individual to erase personal data processed without a legal basis, i.e., in breach of Article 6(1) of the GDPR, and imposed a warning for failing to comply with the data subject's right (defined by the DPA as a failure to comply with the information obligation) under Article 15(1) of the GDPR in connection with failure to indicate the source of and the legal basis for the processing of personal data regarding the e-mail address.

The facts

The plaintiff received a marketing message from an individual at their e-mail address. Via e-mail, they replied to the address from which they received the message with a request to comply with the information obligation regarding the source of obtaining and the legal basis for processing their personal data. In the absence of a response from the defendant, the plaintiff filed a complaint with the Data Protection Authority regarding the lack of action on the part of the person sending the marketing information. In the course of the proceedings, the person did not provide explanations or respond to the plaintiff's allegations.

Key findings

- ✓ The person whose actions had been complained about did not indicate any legal basis authorizing them to process the plaintiff's personal data, and the plaintiff themselves denies that there was one. The Data Protection Authority found a breach of Article 6(1) of the GDPR.

- ✓ The Authority found that the person whose actions had been complained about did not comply with the request made under Article 15(1)(g) of the GDPR, even though that was their duty as the controller. However, given the content of the decision (ordering the erasure of data), the Data Protection Authority found that issuing an order to exercise that right was not possible.

- ✓ The Data Protection Authority did not impose a sanction, nor did it address in the substantiation for the decision the failure to explain and respond to the allegations raised by the plaintiff. In practice, this means that it is not in every case that the controller's failure to provide explanations is sanctioned with an administrative fine.

Irregularities and misconduct in complying with a request for the erasure of personal data

#internet #warning #marketing

September 2022

The Data Protection Authority issued a warning to a company operating an online service for unauthorized data processing and sending unsolicited marketing information, despite the plaintiff's request to erase their data (in this case, the e-mail address).

The facts

The plaintiff filed an e-mail request for the erasure of their personal data processed by the operator of the online service.

In their complaint, the plaintiff claimed: '(...) I receive unsolicited marketing information to the address (...). Despite numerous requests in writing, by phone and through forms, the (...) service will not erase the data and continues to send such messages, despite the disclaimer and lack of consent (...)'.

In its explanations, the company replied that it erased the plaintiff's data in November 2018, and in turn, the plaintiff's request from May 2018 went to the wrong department, most likely because the plaintiff incorrectly addressed the request.

The Authority noted that the company's action was not intentional: it was the result of an error, as a consequence of which the company failed to process the request within the timeframe laid down in the GDPR.

Key findings

- ✓ In the substantiation for the decision, the Data Protection Authority pointed out that according to Article 12(2) of the GDPR, the controller shall facilitate the data subject's exercise of their rights under Articles 15-22 of the GDPR. To that end, it must adopt relevant procedures.

- ✓ In this regard, the DPA argued that the controller should ensure that requests can also be made electronically, especially when personal data are processed electronically, which in the present case had not been fulfilled and deserved a warning.

Acquisition of personal data packages

#telemarketing #phone number #no legal basis #warning

March 2022

The Data Protection Authority issued a warning for processing personal data regarding a phone number, for marketing purposes without a legal basis, the erasure of data after the statutory timeframe, indicating the source of obtaining personal data after the legal timeframe.

The facts

A company was in the business of arranging product shows and demonstrations, and for that purpose it obtained data packages from a counterparty. After the plaintiff was contacted by phone, they sent a request to erase the personal data linked to their phone number.

The company responded to that request, indicating that in its opinion a phone number does not constitute personal data. The company said that if the plaintiff asked for their data to be erased, the consultants would stop contacting them, and then phoned the plaintiff again. The plaintiff requested access to information about, among other things, the source from which their phone number had been obtained, the legal basis for processing the data, and the reasons for the renewed telephone contact. The company replied that the plaintiff had not confirmed their erasure request and thence the company did not remove their phone number from its database.

Key findings

- ✓ The Data Protection Authority found that the processing of a telephone number constituted the processing of personal data, since the controller, when contacting the data subject, undertook actions aimed at identifying individuals, which identification did not require excessive costs or time.
- ✓ At the same time, the DPA reiterated that if the phone numbers the company had obtained come from a geographical area known to the controller, this information, combined with the phone number, is an additional criterion for individualizing a specific natural person.

- ✓ Invariably, the Data Protection Authority also takes the position that an agreement to share a data package is not a premise which legalizes the processing of personal data. In this context, the Authority also emphasized that a general indication that the data were obtained from a counterparty based on a contract does not mean that the source of data acquisition was effectively communicated.

- ✓ The Authority also noted that in a situation where the data subject had clearly indicated in their original request that they wanted all data associated with their phone number erased, the controller could not require the data subject to confirm their wish to erase their phone number from the database. Therefore, controllers should be aware that in the case of requests that do not raise interpretive doubts, they cannot demand additional confirmation from data subjects of their decision.

Telephone contact despite no marketing consent

#marketing #bank #consent #no legal basis #warning

March 2022

The Data Protection Authority issued a warning to a bank for processing a client's phone number for direct marketing purposes without a legal basis.

The facts

The bank employee telephoned the client whose data were processed to execute contracts with the bank, with a proposal to present ways to increase profits on deposits, along with an invitation to a meeting. After the client emphasized their lack of consent to be contacted by phone for direct marketing purposes, the bank employee reiterated that they had only called with a meeting proposal. In the course of the investigation, the bank stated that it contacted the client due to improper verification of data in the bank's information system.

Key findings

- ✓ Processing personal data for direct marketing purposes may be justified by the legitimate interest of the controller. However, the Data Protection Authority found that the lack of consent under Article 172 of the Telecommunications Law indicates that the client did not expect that their data would be processed by the bank for direct marketing purposes. At the same time, the Authority did not clarify whether the controller could continue to carry out other marketing activities without the use of electronic or other channels, such as snail mail, although since the DPA's decision was connected to the provisions of the Telecommunications Law, it seems that this is how its decision could be interpreted.

- ✓ As it seems, in the contemplated decision the Data Protection Authority has gone as far as to determine that even if the proposal made by telephone concerned products related to the client's contracts, and no details of the offer were provided during the conversation, it was necessary to obtain prior consent for direct marketing. The consent should be provided under Article 172 of the Telecommunications Law instead of Article 6(1)(a) of the GDPR.

Processing of data for marketing purposes after the contract has been completed

#marketing #information obligation #no legal basis #warning

April 2022

The Data Protection Authority issued a warning to the controller for processing data for marketing purposes without a legal basis, failing to comply with its information obligations, and failing to timely respond to the plaintiff's erasure request.

The facts

The company obtained the plaintiff's personal data from a publicly available telephone directory. The company sought the basis for processing the data in its legitimate interest in conducting direct marketing and fulfilling a consumer contract. However, the contract had previously been completed. The company failed to fulfill its information obligation when sending correspondence to the plaintiff: it only informed the plaintiff that their data were not disclosed to third parties and informed them that they could erase their data.

Key findings

- ✓ Conducting direct marketing under Article 6(1)(f) of the GDPR is permissible only if the interests of the controller are overridden by the rights and freedoms of the data subject. The premise is met if the data subject can genuinely expect the data to be processed for direct marketing purposes. This is the case when there is some kind of connection between the individual and the controller. In the opinion of the DPA, the processing of an individual's personal data by an entrepreneur for marketing purposes after the contract between the two parties has been completed would be permissible only if the individual has granted their consent. The processing of personal data based on a contract is permissible until the contract has been completed.

- ✓ Article 4a (1) of the Consumer Rights Law, which allows for the possibility of complying with the information obligation using a website announcement, does not apply to the acquisition of personal data from a secondary source, such as a telephone directory.

Impact of withdrawal of marketing consent from the telecommunications law or the Polish Law on the provision of electronic services on the controller's legitimate interest

#bank #warning #marketing

March 2022

The Data Protection Authority issued a warning to a bank for processing a client's personal data for marketing purposes without a legal basis.

The facts

The bank processed its client's data for direct marketing purposes based on Article 6(1)(f) of the GDPR, having the client's consent to the use of electronic terminal equipment for this purpose, as referred to in Article 172 of the Telecommunications Law and Article 10(1) and (2) of the Polish Law on the Provision of Electronic Services.

Subsequently, the bank's client withdrew any marketing consent given to the bank. Nonetheless, the day after the consent was withdrawn, a bank employee contacted the client to present a marketing offer to them.

As a result, the client first complained to the bank, and then filed a complaint with the DPA, seeking an order to restrict the processing. The bank indicated that the situation was the result of the improper circulation of information within the bank. The advertising campaign was generated while the client's consents were still visible in the bank's system.

Key findings

- ✓ The Data Protection Authority pointed out that a data subject's withdrawal of marketing consents referred to in separate regulations makes the basis of Article 6(1)(f) of the GDPR no longer relevant for the use of (telephone) direct marketing.

- ✓ Unfortunately, the decision does not resolve whether, in such a situation, the bank could continue its marketing activities without the use of telecommunications terminal equipment and automated calling systems (e.g. by sending content via snail mail), based on its legitimate interest.

New owner of a phone number in the context of direct marketing

#phone number #direct marketing #data subject identification

March 2022

The Data Protection Authority ordered a foundation to erase the plaintiff's personal data and imposed a warning for breaching Article 12(3) and (4) in conjunction with Article 15(1) of the GDPR by failing to fulfill its information obligation.

The facts

The foundation's employee called the plaintiff at their landline for the purpose of direct marketing, i.e. to collect donations. When asked about the source of the plaintiff's consent to telephone marketing, the foundation's employee hung up without replying.

In view of the above, the plaintiff requested an order to erase their personal data, accusing the foundation of failing to comply with its obligation to provide information regarding the legal basis, the source and the purpose of processing.

The foundation replied that it did not and had never processed the plaintiff's data, and the plaintiff themselves had never requested compliance with the information obligation or objected to the processing of personal data.

At the same time, the foundation pointed out that its employee contacted a number they had found in a publicly available telephone directory containing companies, institutions and individual customers, and that the marketing activity was supposed to be aimed at another person. Since the foundation's employee did not know or inquire about the plaintiff's personal data, the controller was of the opinion that it did not process the plaintiff's data, and the foundation did not erase the same.

Key findings

- ✓ The Data Protection Authority found that the foundation processed the plaintiff's personal data including the phone number, while stating that at the time when they contacted the plaintiff, the foundation had no information that the disputed phone number belonged to them.

- ✓ The Authority takes the position that the fact that the foundation did not verify the plaintiff as a number holder does not mean that it did not process their personal data. Indeed, a data subject is also a person who can be indirectly verified.

- ✓ The Data Protection Authority once again pointed out that a phone number constitutes personal data within the meaning of the GDPR, as it 'enables direct contact with a specific person and the mere establishment of identity does not require excessive costs.' The Authority thus ignores one of the decisions of the Provincial Administrative Court in Warsaw, in which the Court took the opposite position.

- ✓ The question about the source of consent for telephone marketing asked in the course of the telephone conversation should, in the Authority's opinion, be understood as a request for information as to the legal basis for processing and the source of obtaining the plaintiff's personal data. In the opinion of the Data Protection Authority, the failure to provide this information constituted a breach of Article 12(3) and (4) in conjunction with Article 15(1) of the GDPR.

Objection to data processing

#direct marketing #data subject objection #transparency #banking sector

March 2022

The Data Protection Authority issued a warning for providing unclear and incomprehensible information regarding compliance with a request regarding the objection to the processing of personal data for direct marketing purposes.

The facts

The plaintiff registered on a portal operated by the controller and consented to telephone and e-mail marketing. More than three years later, they revoked the above consents. Since then, the plaintiff's data has not been processed for marketing purposes. All communications that were sent after that date related to the service provided by the controller, including information about changes to the T&Cs or the impending end of the service.

The plaintiff requested the company to stop processing their personal data for marketing purposes, including profiling. In response, the company indicated that the consent could not be revoked as it had never been granted, and the processing is carried out based on Article 6(1)(f) of the GDPR.

The plaintiff then filed an objection to the processing of personal data. In turn, the controller explained that the justification for its previous response had been misconstrued, but despite the mistake, the data subject's objection was effective.

Key findings

- ✓ The Authority shared the position found in the case law, i.e. that marketing activities are not so much to inform, but rather to persuade the recipient to take a certain action by influencing the recipient's emotions. Thus, the DPA considered that not only regulatory information, but also messages regarding the termination of service (potentially aimed at encouraging the customer to renew the contract) do not constitute marketing communications.

- ✓ The Data Protection Authority also argued that the unclear and incomprehensible information about compliance with the

objection request constituted a breach of Article 12(1) in conjunction with Article 21(2) and 21(3) of the GDPR, which resulted in a warning. The fact that the controller acknowledged the objection after the first request remained irrelevant to the decision, since the fact that the data subject was forced to make a new request proves the defectiveness of the controller's initial response.

- ✓ Therefore, controllers should keep in mind that it is not only the fact of acknowledging the data subject's request that is evaluated by the Data Protection Authority, but also the manner in which the data subject's rights are exercised, which must meet the prerequisites laid down in the GDPR.

Impact of the company's failure to respond to the data subject's request

#company #warning #marketing #spam

May 2022

The Data Protection Authority issued a warning to a company for breaching Article 12(3) in conjunction with Article 15(1) of the GDPR by failing to respond to a plaintiff's request for access to the personal data processed by the company within the period specified in Article 12(3) of the GDPR. The DPA also issued a warning for breaching Article 15(1) of the GDPR by failing to comply with the plaintiff's request for access to the personal data processed by the company.

The facts

The company obtained the plaintiff's personal data in connection with an order they placed on the company's website. The plaintiff requested that the company allow them access to information regarding the circumstances in which they granted their consent for processing their data for marketing purposes, while in their subsequent e-mails to the company they requested information regarding the source of acquisition and the category of their data as processed by the company.

The plaintiff sent their correspondence regarding the above to the company's e-mail address, as well as to the address from which the marketing offers had been sent to them.

The plaintiff did not receive any response to the above correspondence. Explaining the lack of response to the plaintiff's requests, the company replied that they had not been answered due to a technical error in the e-mail system, which classified the plaintiff's messages as spam.

Key findings

- ✓ The Data Protection Authority emphasized that even messages classified by the mail server as 'alleged spam' must be processed by the controller as a valid exercise of the data subject's rights granted under the GDPR. It is the controller's responsibility to ensure that the data subject is able to exercise their rights under the GDPR.

- ✓ The e-mail address provided by the company is used to contact the company on data protection issues. The situation in which the plaintiff cannot exercise their right, despite a properly submitted request, should therefore be treated as the result of the company's misconduct.

- ✓ A GDPR-based request sent to any of the company's e-mail addresses binds the company. The addressee to exercise the rights of data subjects is the controller as such, and if it receives a request, it must process it. The above conclusion is particularly relevant for large organizations that contact data subjects through multiple communication channels (e.g. dedicated e-mail addresses, hotlines, social media etc.).

- ✓ As it seems, even if the controller provides a specific communication channel for correspondence regarding GDPR-based requests, if such a request (or any such correspondence, in fact) is sent to another address, the controller must respond to it.

- ✓ The company responded to the plaintiff's request too late, and it did not grant the request for access, but only informed the plaintiff about the erasure of data, which, in the opinion of the Data Protection Authority, constitutes a breach of both Article 12(3) in conjunction with Article 15(1) of the GDPR and Article 15(1) of the GDPR as such. Therefore, the decision suggests that in the case of a request for access to data, if the controller decides to erase the data, it should first effectively acknowledge the right provided for Article 15 of the GDPR, and only then erase the personal data.

2. Financial sector

Effect of disclosure of personal data printed on envelopes

#bank #warning #envelopes #secrecy of correspondence

September 2022

The Data Protection Authority issued a warning for the processing of customers' personal data regarding the disclosure of personal data printed on envelopes available to unauthorized entities, in breach of Article 6(1) of GDPR. In the remaining scope, the DPA discontinued the proceedings.

The facts

A bank processed its clients' personal data in connection with their contracts for banking products.

The customers notified the bank that it had sent correspondence regarding the concluded contracts to wrong addresses, despite the fact that the bank's system showed the correct address of the plaintiffs. The bank replied that due to a system error, the correct address could not be saved, and the letters had been sent to different addresses than the ones provided as valid by the plaintiffs.

Key findings

- ✓ In the opinion of the Data Protection Authority, in the contemplated case the personal data of the plaintiffs contained on the envelopes of correspondence addressed to incorrect addresses was disclosed to unauthorized recipients, which could not be supported by any of the premises legalizing the processing of personal data expressed in Article 6(1) of the GDPR.

- ✓ However, the most interesting part of the ruling relates to the content of the correspondence. Indeed, the Authority argued that the case should be considered in terms of breaches of personal rights, such as the secrecy of correspondence, while stating that it has no jurisdiction to resolve it.

- ✓ According to the Authority, breaches of the right to secrecy of correspondence are also subject to the sanctions set forth

in the Criminal Code; however, the Data Protection Authority found that it lacked jurisdiction in this area as well.

- ✓ Therefore, the decision calls into question all previous decisions of the DPA relating to personal data contained in the contents of lost correspondence. In particular, it may prove relevant to the appeal proceedings against the decision in which the Data Protection Authority imposed an administrative fine on the controller for failing to report a personal data breach and failing to communicate data breach to the data subjects consisting precisely in losing (misplacing) of a shipment that contained bank documents containing personal data.

- ✓ The Authority also made an important ruling with regard to the plaintiffs' demand to order that the controller bring the processing operations into compliance with the provisions of the GDPR, in particular by posting correspondence only to their current address. In this regard, the Data Protection Authority pointed out that its assessment can only concern actual data breaches, and that the demand addressed to the Data Protection Authority cannot concern the controller's hypothetical actions which may only occur in the future.

A bank processing personal data in connection with debt collection

#bank #claims #warning

September 2022

The Data Protection Authority issued a warning to a bank for breaching Article 6(1) of the GDPR. The breach consisted in processing the plaintiff's personal data without a legal basis after recording the plaintiff's debt in the bank's losses account. The DPA refused to grant the plaintiff's request to order the processing of their personal data.

The facts

The bank pointed out that it obtained the plaintiff's personal data for the purpose of executing the bank account agreement. The bank later received a properly drafted termination notice from the plaintiff. As the bank found a debt on the plaintiff's part, it blocked the use of the account in question; however, in the bank's systems the client's account was active due to the ongoing collection process. As a result of the mistake, the bank processed the plaintiff's personal data, even after the plaintiff's debt was recorded in the losses account, in order to collect the debt.

Key findings

- ✓ The Data Protection Authority pointed out that 'if every case of processing a debtor's personal data were to be considered as harming their rights and freedoms, there would be, on the one hand, an unjustified protection of defaulters, and on the other hand, a breach of the principle of freedom of economic activity.' Accordingly, the processing of the debtor's personal data in this case did not breach the plaintiff's rights and freedoms. With the entry of the debt in the bank's losses, the aforementioned basis for processing became irrelevant.

- ✓ The Authority emphasized that it is only authorized to assess the legality of the processing of the plaintiff's personal data, so the question of the existence/non-existence of claims or the fairness and scope of civil law claims does not fall within its jurisdiction.

- ✓ The above conclusion seems to deviate from the Authority's established practice, in which it emphasizes that only the active pursuit of existing claims justifies the processing of personal data.

Request to indicate the legal basis for debt assumption as a non-data protection issue

#fund #refusal to grant a request #debtor data

July 2022

The Data Protection Authority refused to grant the plaintiff's request with regard to the irregularity of the controller's processing of their personal data, consisting in the transfer of their personal data without a legal basis to a law firm engaged in debt collection. In the remaining scope, the DPA discontinued the proceedings.

The facts

In their complaint, the plaintiff challenged the controller's sharing of their personal data with the law firm and pointed out that the law firm did not respond to their letters with questions about the transfer of their personal data. The controller was the plaintiff's creditor and processed their personal data as part of a debt collection process. It made the plaintiff's data available, under a data processing agreement, to the law firm, which handled debt collection.

Key findings

- ✓ The Data Protection Authority pointed out that the processing of personal data in connection with claim collection against the plaintiff, the controller's debtor, should be considered necessary for purposes arising from the company's legitimate interests within the meaning of Article 6(1)(f) of the GDPR.
- ✓ The Authority also found that the provision of the plaintiff's personal data to the law firm was legally permissible under Article 28(3) of the GDPR.

- ✓ What is of particular importance, the Data Protection Authority emphasized that the plaintiff's request to provide the basis on which their debt had been assumed by the law firm could not be considered a request containing a demand under Article 15(1) of the GDPR, since it did not concern personal data, but a civil case, not pending before the Data Protection Authority.

Failure to timely comply with a request

#bank #warning #request #timeframe

August 2022

The Data Protection Authority issued a warning to a bank for failing to comply with a request to erase personal data regarding phone number and e-mail address within the timeframe specified in Article 12(3) of the GDPR.

The facts

The plaintiff requested that the processing of their personal data be stopped, and their e-mail address and phone number erased.

Within one month the bank replied that due to the need to analyze the request and due to a large volume of similar requests resulting from the GDPR entering into force, it is necessary to extend the statutory timeframe for responding by another two months. Subsequently, in another letter and in breach of the statutory timeframe laid down in the previous letter, the bank replied that it would be possible to grant the request only after the plaintiff submitted an additional instruction to change the form of delivering statements or to abandon the delivery of statements due to the service used by the plaintiff.

The plaintiff disagreed regarding the need to provide the indicated instructions to the bank and again demanded erasure of their personal data. The bank neglected any response to the plaintiff until the DPA initiated administrative proceedings. As the proceedings began, the bank granted the plaintiff's request, nearly a year after the original one.

Key findings

- ✓ The Data Protection Authority highlighted the inconsistency of the bank's actions, which first decided that granting the plaintiff's request would be possible only after they submitted additional instructions, and then erased their data, despite the fact that the aforementioned instruction had not been submitted. Controllers should therefore pay attention to the reasonableness and consistency of their actions.

- ✓ The decision refers to the division of the bank taking place at the time. In the Authority's view, both the bank which received the warning and the successor bank were equally obliged to consider the plaintiff's request.

Responsibility to forward and comply with a request

#vindication #processor #controller #data copy

August 2022

The Data Protection Authority ordered the controller to provide a copy of the plaintiff's personal data, even though the request had been received by the processor who could fulfill it as well.

The facts

The company and the debt collection company cooperated in the field of debt processing. In order to perform the contract, the parties entered into a data processing agreement.

The plaintiff, in turn, had a contract with the company, which was terminated because the plaintiff failed to fulfill their obligation to return the provided equipment by a certain date. As a result, a debit note was issued by the company, and in order to collect that debt, the company entrusted the processing of the plaintiff's personal data to a collection company.

The plaintiff requested a copy of their personal data from the collection company, but did not receive a response, so they renewed their request.

The debt collection company, as a processor, did not pass on the information about their request to the company, which was the plaintiff's data controller.

Key findings

- ✓ The entity to which the controller entrusts personal data is only required to assist the controller in fulfilling its obligations, including fulfilling data subjects' requests.
- ✓ The responsibility for failure to fulfill the requests rests solely with the controller. The processor cannot take over the controller's administrative and legal responsibilities.

Copying identity documents to fulfill legal obligations

#banks #copy identity documents #AML

June 2022

The Data Protection Authority did not find any irregularities in a bank's copying identity documents during the conclusion of a bank account agreement and an electronic banking agreement, considering Article 6(1)(b) of the GDPR and Article 49(1)(1) of the AML Law as the legal basis for copying the IDs.

The facts

The plaintiff indicated that during the execution of the bank account agreement and the electronic banking agreement, they were informed by a bank employee that a scan of their identity document was an obligatory condition for the conclusion of the agreements. The bank indicated that it processes the plaintiff's personal data, among other things, for the purposes of fulfilling its obligations under the bank account agreement, the e-banking agreement, fulfilling its obligations related to the execution of financial security measures, and storing data for the purposes of preventing money laundering and the financing of terrorism. The bank also claimed that before copying the plaintiff's ID, it had carried out an assessment of money laundering and terrorist financing risks for the plaintiff, as a result of which it found that the risk was standard.

Key findings

- ✓ The Data Protection Authority found that the bank was obliged to apply financial security measures in connection with the conclusion of agreements with the plaintiff, i.e. the establishment of permanent business relations with them.

- ✓ In the Authority's view, the determining circumstance was that the plaintiff's agreement with the bank concerned a product that posed the greatest risk of money laundering or terrorist financing, i.e. a bank account.

- ✓ The decision is noteworthy as it becomes a certain ‘breakthrough’ in the previous line of DPA rulings, which generally limited the possibility of a bank copying identity documents to incidental cases strictly justified by the circumstances.

Sending information about amendments to tariffs and T&Cs versus marketing information

#bank #discontinuation #request #trade information

July 2022

The Data Protection Authority refused to uphold the complaint on irregularities in the processing of personal data by a bank, involving the processing of the plaintiff's personal data without a legal basis. In the remaining scope, the DPA discontinued the proceedings.

The facts

In connection with the receipt of correspondence from the bank regarding changes to the tariff of fees and commissions and the terms and conditions for opening and maintaining accounts, which the plaintiff considered to be marketing information and commercial offers, she requested that their personal data be erased from the bank's system. The plaintiff and the bank were bound by a savings and checking account agreement, which the plaintiff had not terminated.

The bank explained that due to its statutory obligation, it had to keep the plaintiff's data and inform them of any changes to the T&Cs.

Key findings

- ✓ The Authority argued that due to the agreement between the parties, the bank had to send the plaintiff information on changes to the tariff and T&Cs pursuant to Article 29(1) of the Payment Services Law. It also stated that the said correspondence containing the aforementioned information constituted neither marketing nor commercial information. Therefore, controllers sending data subjects information related to the performance of an agreement should bear in mind that consent is not the legal basis for processing in this regard.

- ✓ Further, the Authority stated that it is not within its jurisdiction to examine whether an agreement is valid and legally effective, since the DPA deems an agreement a legal action, which is not subject to review and which produces legal effects until it has been challenged in the form and manner prescribed by law.

Processing of erroneous data until updated by the data subject

#bank #warning #no basis for processing #marketing #data accuracy principle

March 2022

The Data Protection Authority issued a warning for processing an e-mail address despite the lack of a legal basis.

The facts

When opening an account, the client provided a wrong e-mail, i.e. an address of a person with the same first and last names. As a result, the bank was sending correspondence to the e-mail address of a third party. That person demanded that the processing of their personal data be discontinued, but the bank refused, replying that only the bank's client, who had originally provided a wrong e-mail address, could change it.

The client then updated their e-mail address, but as a result of a previously prepared advertising campaign, an e-mail was sent to the wrong e-mail address. The message addressee filed a complaint against the bank.

The Data Protection Authority issued a warning to the bank for sending an e-mail to an old e-mail address despite the fact that the client had already corrected it. The DPA replied that 'from that [data correction] moment on, the company lost the legal basis for processing that e-mail address."

Key findings

- ✓ The Authority took the position that the basis for processing is lost when the data are corrected by an authorized data subject, despite the fact that the controller had already known that it had been processing inappropriate data.

- ✓ The decision indirectly implies that until the controller determines correct data, it may process erroneous data or data the correctness of which raises serious doubts. This is a particularly interesting ruling in light of the DPA's other decisions, including one in which the Authority, nonetheless imposing an administrative fine, resolved that the controller must process valid and accurate data.

Debt annotation affixed on an envelope

#correspondence #debt #warning

March 2022

The Data Protection Authority issued a warning for irregularities in the processing of personal data involving the disclosure of personal data to unauthorized parties by placing debt information on an envelope.

The facts

An entrepreneur addressed mailings to the plaintiff, placing the following information on the envelopes: first and last names, mailing address, and in addition, on the back of the envelope – an annotation reading 'Collection Department. Call for payment.' The annotation referred to the creditor's unit responsible for handling correspondence. The plaintiff argued in the course of the proceedings that the annotation harmed the reputation of its business.

Key findings

- ✓ The Authority held that because the debt was annotated with a name and address, this information identifies an individual and, consequently, constitutes personal data.

- ✓ In the opinion of the Data Protection Authority, only personal data that is necessary for the delivery of correspondence should be placed on the envelope, and information on debt cannot be considered as such. Placing such an annotation meant redundant data were disclosed to unauthorized parties, such as postal service employees.

- ✓ The Data Protection Authority found that affixing a debt annotation cannot be justified by designating the creditor's unit responsible for drafting the letter, in order to facilitate the internal recording of correspondence. According to the Authority, it is the controller's responsibility to implement such organizational arrangements as will be sufficient to ensure that personal data are processed lawfully, with confidentiality and to the minimum extent necessary to achieve the purpose of the processing. Organizational facilitation within the controller's organization is not an excuse for breaching data protection regulations.

Method of identifying the data subject

#bank #warning #identity verification

March 2022

The Data Protection Authority ordered a bank to comply with the former client's request, i.e. to provide information about the recipients of their personal data to whom the data were disclosed.

The facts

A former client of the bank requested details of entities to which the bank provided their personal data, using the e-mail address they used when they were the bank's client and providing additional identifying information in the e-mail. In response, the bank refused to comply with the request by e-mail, without justifying the decision, and offered the data subject visit a branch, in accordance with the controller's procedures.

In view of the above, the data subject filed a request with the Authority to order compliance with the information obligation within the extent requested. During the proceedings, the bank indicated that the only way to provide the requested information to individuals who are not currently the bank's clients would be at the branch, where the identity of the former client could be verified.

Key findings

- ✓ The Authority argued that in the case of an acquisition of a brokerage house by the bank, the latter also assumed the brokerage house's obligations as a controller with regard to exercising the data subjects' rights.

- ✓ According to the Data Protection Authority, if the controller refuses to comply with a request if the data subject has provided identification data, it is the controller's duty to demonstrate that the data were insufficient to verify the identity of the person who made the request.

- ✓ The decision in question is a manifestation of the need to make it easier for data subjects to exercise their requests: as it seems, the controller cannot force the data subjects to use specific communication channels if they can sufficiently demonstrate their identity through channels other than those indicated by the controller.

Compliance with the information obligation under Article 105a (3) of the Banking Law

#bank #creditworthiness assessment #credit risk analysis #claims limitation

September 2022

The Data Protection Authority ordered the bank to cease processing a former client's data processed under Article 105a(3) of the Banking Law for the purpose of assessing creditworthiness and analyzing credit risk, and to stop processing data 'processed without a legal basis for the purpose of defending against possible claims.'

The facts

Since the client was at least 60 days late with their due payment, the bank processed their data under the terms laid down in Article 105a(3) of the Banking Law and for the purpose of defending against possible claims, until they are time-barred.

According to the Authority, the bank could not prove if and when it informed the client of its intention to process their data under Article 105a(3) without their consent, as it had been obliged to do. The client filed a complaint against the bank.

Key findings

- ✓ The Data Protection Authority pointed out that in order to process data under Article 105a(3) of the Banking Law, the bank must inform the data subject of the same in a manner which makes it possible to determine when the data subject received the information. The information can be provided in any form; however, a mere confirmation of posting the correspondence with a copy of its contents is insufficient to prove compliance with the information obligation.

- ✓ The Authority upheld its line of jurisprudence, according to which the controller's failure to identify an existing or an actively asserted claim precludes the possibility to process data for the purpose of establishing, pursuing and defending against claims.

- ✓ Interestingly, the Authority has abandoned its practice of using the erasure order and used an order to stop processing data for specific purposes.

Data disclosure in a claims seizure notice

#enforcement agent #warning #minimization rule

September 2022

The Data Protection Authority issued a warning to a court enforcement agent for breaching Article 6(1) of the GDPR for disclosing inadequate data of the plaintiff (i.e., the names of the plaintiff's parents) in the seizure notice served in the course of an ongoing enforcement action.

The facts

The enforcement agent conducted enforcement proceedings against the plaintiff based on an enforcement title, i.e. a payment order under the writ of payment procedure by the District Court, certified as enforceable.

The enforcement agent sent the bank a notice of seizure of claim from the plaintiff's bank account. The notice included the plaintiff's personal data comprising, among other things, the plaintiff's parents' names.

Key findings

- ✓ As noted by the Data Protection Authority, there is no provision in civil procedure indicating unambiguously which data should be provided to identify the debtor enforced when carrying out enforcement against a bank account. This means that the identification of the debtor should be carried out by providing their data contained in the enforcement order, but no more than is necessary to allow the debtor to be identified by the entity, to whom the seizure was directed.

- ✓ According to the DPA, the disclosure of the plaintiff's data in the form of their parents' names for the purpose of seizure of claims from the bank account by the enforcement agent should be considered inadequate for the purpose of their processing, and thus incompatible with the data minimization principle expressed in Article 5(1)(c) of the GDPR. The Data Protection Authority did not question the enforcement agent's provision of the plaintiff's name, PESEL (personal identification) number, date of birth and residential address, since, in the Authority's view, those data unambiguously identified the plaintiff.

Obligation to update mailing address

#bank #discontinuation #correspondence

May 2022

The Data Protection Authority discontinued the proceedings against a bank with regard to its processing of the plaintiffs' residential address assigned to the bank's client.

The facts

The plaintiffs indicated that they regularly received correspondence addressed to the name of another entity. As a result, they contacted the bank with information that the address provided was incorrect, requesting that it be removed from the bank's databases.

The bank informed the plaintiffs that the addressee of the correspondence was the bank's client and provided their address as the correct one. The bank argued that only the client can request a change of address and asked the former client to update their personal data in this regard.

Key findings

- ✓ The Data Protection Authority pointed out that where more than one person provides the same residential address for correspondence, the address concerns both of them to the same extent. In the Authority's opinion, this type of personal data concerns all such data subjects independently. The DPA also argued that each person is free to state their residential address, as it is that person who bears the consequences of not receiving mail at the address they have provided.

- ✓ The Authority also rightly noted that the bank is not in a position to verify the accuracy of the data regarding the residential address provided by the client, and by posting correspondence to an address other than the one provided by the person concerned, it would fail to exercise due diligence in dealing with that person, which would make it impossible to effectively serve correspondence upon them. At the same time, insofar as the plaintiffs made a request to

the bank regarding the address assigned to the bank's client, they made a request regarding third party data, which consequently made it impossible to comply with such a request under the GDPR.

3. Insurance sector

Employee's error in data processing, extension of time to comply with requests

#insurer #employee error #request compliance

September 2022

The Data Protection Authority issued a warning to a company for breaching Article 6(1) of the GDPR by processing the plaintiff's personal data in connection with the insurance policy contract without a legal basis. In the remaining scope, the DPA refused to grant the request.

The facts

The company obtained the plaintiff's personal data in connection with the conclusion of a third-party liability and comprehensive motor insurance contracts. Due to an employee's error, the plaintiff's data were mistakenly used in a motor insurance contract concerning another client of the same insurance company. The company informed the plaintiff that their application had been accepted for processing; however, it could not be processed within a month due to the significant number of requests received in connection with the application of GDPR.

Key findings

- ✓ In the opinion of the Data Protection Authority, the company processed the plaintiff's personal data without being grounded in any of the premises laid down in Article 6(1) of the GDPR. On the other hand, the plaintiff's personal data had not been disclosed to a third party as the above-mentioned contract, incorrectly concluded using the plaintiff's personal data, was sent only to the plaintiff.

- ✓ The Data Protection Authority pointed out that the company provided the plaintiff with a comprehensive response as to how the above-mentioned situation occurred and informed the plaintiff that their data had not been disclosed to any unauthorized persons.

- ✓ According to the Authority, the company also correctly informed the plaintiff of the necessary extension of the one-month timeframe for responding to the request resulting under Article 12(3) of the GDPR, indicating the reasons for

the delay, i.e. the large number of requests, which is a particularly significant conclusion from the perspective of controllers handling numerous requests from data subjects.

Unauthorized disclosure of personal data of the insured to the aggrieved party

#insurance #warning #insurance policy

September 2022

The Data Protection Authority issued a warning to an insurance company for breaching Article 6(1) of the GDPR by providing an unauthorized person with access to personal data contained in a copy of an insurance contract.

The facts

The insurance company processed the plaintiff's data in connection with the execution of a real estate insurance contract.

As part of the company's claims settlement process, during the inspection of the damage a company employee disclosed the plaintiff's personal data contained in the insurance policy to a third party – the aggrieved neighbor.

The company requested that the aggrieved party destroy the document containing the plaintiff's data, which the aggrieved party did, according to the Authority's findings.

During the proceedings the company explained that it apologized to the plaintiff and pointed out to the employee's misconduct, which was an incidental error.

Key findings

- ✓ The DPA pointed out that the aggrieved party had not requested the company to provide them with a copy of the documentation, so no premises referred to in Article 29(6) of the Insurance and Reinsurance Activity Law occurred, and so the disclosure of the plaintiff's personal data to the aggrieved neighbor could not be grounded on Article 6(1).

- ✓ The Authority found that the one-time nature of the data disclosure justified the imposition of a warning on the controller. At the same time, the Authority did not analyze the contemplated event in terms of the personal data breach provisions (Articles 33 and 34 of the GDPR).

Compliance with information obligation regarding information on financial operations

#insurance #information obligation #request

July 2022

The Data Protection Authority refused to grant a motion to order compliance with a request for access to data on financial operations pointing out that such information does not constitute personal data.

The facts

The plaintiff demanded that an Insurance Company comply with its information obligations towards them, including the provision of a range of information, including information on operations performed on their participation units account.

The Insurance Company complied with the plaintiff's request, save for the information regarding operations on their participation units, indicating that this is financial information and as such does not relate to an identified or identifiable natural person, and therefore does not constitute personal data.

Key findings

- ✓ The Data Protection Authority resolved that information on financial operations does not constitute personal data because it does not serve to identify the characteristics of the plaintiff.

- ✓ The Authority made a reference to a ruling by the Provincial Administrative Court stating that 'information on the balance in the Individual Participation Units Account (...) and (...) information about any operations performed on the Individual Participation Units Account during the term of the insurance contract (...) is not personal data processed by the personal data controller (...) and, consequently, the above information is not the information that can be effectively requested from the personal data controller as part of a request for compliance with the information obligation (...).'

4. COVID and health information

Making client service conditional on production of a medical certificate

#bank #warning #medical certificate

September 2022

The Data Protection Authority issued a warning for breaching Articles 9(2) and 7(4) of the GDPR in connection with the collection of personal data contained on the exemption certificate for covering the mouth and nose, without the plaintiff's consent.

The facts

In 2021, during the COVID-19 pandemic restrictions, the plaintiff, when visiting their bank branch without their mask on, was asked by a bank employee to show a medical certificate regarding contraindications to wearing a mask, on pain of being denied direct service by the employee.

The bank pointed out that every employee has a statutory duty to take care of the welfare of the workplace, which was manifested in the authorization to request the clients to produce certificates of exemption from the obligation to wear a mask. The controller also argued that it did not obtain or record the client's certificate and did not process their personal data in this regard during the proceedings.

Key findings

- ✓ The Data Protection Authority pointed out that the mere acquisition of information about a particular person's exemption from the obligation to cover their mouth and nose, even without recording the same, should be qualified as the processing of special categories of personal data.

- ✓ The Authority emphasized that in the absence of relevant regulations, only the client's voluntary consent authorizes the bank to process their personal health data. However, making client service at the bank's facility conditional on the presentation of the aforementioned certificate means that the client's consent cannot be considered voluntary.

Voluntariness as a condition for valid consent

#employer #warning #masks

July 2022

The Data Protection Authority issued a warning to a school's headmaster for processing personal data about a teacher's health, in breach of Article 9(1) of the GDPR.

The facts

During the COVID-19 pandemic restrictions, the plaintiff teacher informed their employer that they had obtained a medical certificate stating that they were absolutely contraindicated to wear a mask or a visor. The certificate contained the teacher's personal data, including their health information.

The school's headmaster demanded that the employee produce the aforementioned certificate, as her representation in this regard was insufficient in their opinion. The teacher displayed the certificate on their phone screen, claiming in their complaint to the Data Protection Authority that they did not do that voluntarily.

Key findings

- ✓ The Data Protection Authority pointed out that the regulations in effect during the COVID-19 pandemic in 2021 provided for a narrow, closed catalog of persons authorized to process personal data on contraindications to wearing a mask or a visor by specific individuals. That catalog did not comprise school headmasters or employers, and therefore, according to the Authority, in the present case the employer should have exempted the plaintiff from wearing their mask based on their representation which did not contain specific data about their health condition.

- ✓ The decision in question is one of the few resolutions issued in 2022 in which the Data Protection Authority addressed the construction of one of the principles provided for in the GDPR regulations, i.e. the fairness principle.

- ✓ According to the Authority, a situation in which the plaintiff eventually produced a certificate containing their health data even though they had informed the controller that they did not

intend to provide him with the same, as the controller was not authorized to require them to do so under the law, indicates a lack of voluntariness in her actions and a breach of the fairness principle by the controller.

- ✓ Given that the plaintiff requested that a penalty be imposed on the controller, the Data Protection Authority argued – as in other rulings issued in proceedings initiated at the request of data subjects – that while it is within its jurisdiction to impose administrative fines, this is its autonomous competence which the Authority will not exercise at the plaintiff's request.

COVID-19 infection and disclosure of child's personal data to the Health Inspectorate

#COVID-19 #warning #disclosure

June 2022

The Data Protection Authority refused to grant the request regarding irregularities in the processing of personal data of the plaintiff and their minor child by the School and Kindergarten Complex.

The facts

Following a confirmed case of COVID-19 in a student from the plaintiff's child's class with whom the child had contact, the school headmaster disclosed the data of the plaintiff and their son with the State District Sanitary Inspector (hereinafter: SDSI) in order to maintain safe and hygienic learning conditions and to prevent infection on the premises. The scope of the data provided included: the child's first and last names, date of last contact, the child's PESEL number, home address, and the plaintiff's phone number. In letters to the school, the plaintiff stated that they did not consent to the disclosure of personal data to the SDSI.

Key findings

- ✓ The Data Protection Authority pointed out that the school's disclosure of the plaintiff's and their child's personal data for the purpose of conducting epidemiological investigations in connection with a COVID-19 infection in a person in the vicinity of the minor complies with Article 6(1)(c) of the GDPR in conjunction with Article 32a(1) and (2) of the Polish Law on Prevention and Control of Infections and Infectious Diseases in Humans (PCI Law), and adequate for the stated purpose.

- ✓ Having received the SDSI summons, the school had to disclose the data requested by the entity in order to enable proper conduct of epidemiological proceedings, including the determination of ‘persons in contact’ with a person infected with COVID-19 and the address of possible isolation or quarantine by the sanitary services, as well as contact details of the parents in order to inform them of the duty to isolate or quarantine. No consent was required in this process, as the processing was based on Article 6(1)(c) of the GDPR.

Disclosure of personal sick leave data to a newspaper editor

#disclosure #special category data #press

September 2022

The Data Protection Authority issued a warning for breaching Article 5(1)(a) and Article 9(1) and (2) of the GDPR, consisting in the disclosure of health data by an acting director to a newspaper editor without a legal basis. In the remaining scope, the DPA discontinued the proceedings.

The facts

The acting director of the company disclosed personal data regarding the plaintiff's health to the co-author of an article published in the newspaper. The plaintiff informed the co-author of the article that they had been incapacitated for work and remained on sick leave. The plaintiff demanded that their personal data be removed from the article in question.

Key findings

- ✓ The DPA emphasized that information about the plaintiff's inability to work constitutes information about the plaintiff's medical condition, and therefore falls into a special category of personal data (Article 9(1) of the GDPR).
- ✓ According to the DPA, there was no legal basis for disclosing the aforementioned data, and no exception under Article 9(2) of the GDPR occurred that would justify their processing, which constitutes a breach of the GDPR.
- ✓ Significantly, the Authority found that the demand for erasure was without merit since the controller of the data processed in the article was the publisher, not the editor. In the Authority's view, issuing a decision against the publisher would mean going beyond the complaint's demand, and therefore it was inadmissible. The DPA also argued that although carrying out inspections of the processing of personal data falls within its jurisdiction, such actions would not be taken at the request of the data subject.

- ✓ At the same time, the Authority did not address the possibility of invoking the so-called press exception in the case at hand, which would exclude or restrict the application of certain provisions of the GDPR to press materials.

Passing on personal data by public authorities to enforce vaccination obligations

#hospitals #vaccinations #data necessity

July 2022

The Data Protection Authority ordered the State District Sanitary Inspectorate to erase personal data only to the extent that it included both plaintiffs' parents' first names. In the remaining scope, the DPA refused to grant the request.

The facts

The plaintiffs, parents of a minor child, failed to comply with the vaccination requirement regarding their minor. They questioned the legal basis for data transfer by the hospital and the outpatient facility, as well as further data processing by the SDSI.

The hospital obtained the plaintiffs' data while the plaintiff and her child were in the hospital, in order to put the data in their respective medical records.

According to the plaintiffs, the SDSI came into possession of their personal data and the data of their minor son illegally, and the data were transferred to the above-mentioned entities by the hospital and the outpatient facility illegally. The SDSI processed the plaintiffs' personal data in order to enforce the obligation to vaccinate the minor.

Key findings

- ✓ Information on vaccination (or lack of vaccination) was considered by the Authority as special category data.
- ✓ The transfer of the personal data of the plaintiffs and their minor son to the SDSI by the outpatient facility and the hospital was purposeful and adequate, as it enabled the SDSI to carry out its supervision of the implementation of the vaccination requirement.

- ✓ The scope of data obtained for the enforcement of the vaccination obligation should include data necessary and sufficient for effective enforcement of the vaccination obligation: the first names of the plaintiffs' parents were deemed unnecessary for effective administrative enforcement.

Data processing to counter COVID-19

#health data #COVID-19 #warning

March 2022

The Data Protection Authority issued a warning to a controller for unlawfully processing employee health data through health surveys.

The facts

The company processed employee's personal data obtained through the so-called 'health questionnaires.' The purpose of the company collecting the data provided in the aforementioned questionnaires was to protect the health of its employees and prevent the spread of COVID-19. The scope of the personal data processed included: the employees' first and last names, body temperature, their current health condition (cough, shortness of breath).

Key findings

- ✓ In 2022 the Data Protection Authority issued numerous decisions regarding health data processing for the purpose of preventing the spread of COVID-19. According to the Authority, if a controller collects health data even for the purpose of preventing the spread of a disease, it must invoke at least the guidelines of the Chief Sanitary Inspector issued for the entity or process the data with the consent of individuals. Otherwise, the processing of health data is not supported by Article 9(2) of the GDPR and is unlawful. In doing so, the Data Protection Authority did not refer to Article 207 of the Labor Code, which was often cited by controllers as the legal basis justifying the collection of data on employees' health status.

- ✓ On the sidelines of the above ruling, the Authority's statement that in the case of joint controllers, the legal basis for data processing is Article 26 of the GDPR, concerning the arrangements of joint controllers, deserves attention. The above statement was not supported by an in-depth analysis, so at this stage it is not possible to definitively determine whether the presented view is an expression of the Authority's well-established position.

Data cannot be secured by the Data Protection Authority

#pharmacy #data disclosure #security #PESEL #warning

March 2022

The Data Protection Authority issued a warning for disclosing personal data regarding the PESEL number on a prescription to an unauthorized person.

The facts

The plaintiff learned from the Online Patient Account that a medical prescription had been issued and filled for them. In the absence of a response from the pharmacy and the National Health Service, the plaintiff asked the DPA to explain the reasons for the situation and to take measures to secure their personal data. Analysis of the evidence showed that the data were disclosed due to an obvious clerical error by the pharmacy technician, who misplaced digits in the PESEL number given on the prescription previously written by the doctor.

Key findings

- ✓ The Data Protection Authority pointed out that the entrepreneur (the pharmacy) had failed to fulfill its obligations under data protection laws by allowing an unauthorized person to access the plaintiff's personal data and by processing the plaintiff's personal data unreliably and illegally. Therefore, the DPA found a breach of Article 5(1)(a) and Article 6(1) of the GDPR.

- ✓ The Data Protection Authority also emphasized that it does not have the powers to secure the plaintiffs' personal data and that the entities equipped with tools appropriate to secure the data are law enforcement agencies. As it seems, the Authority did not exercise its authority to impose a temporary or total restriction of processing by the controller, assuming that the plaintiff's intention was to physically secure their personal data.

Vaccination obligation versus data processing

#vaccination #infectious diseases #health

July 2022

The Data Protection Authority identified the legal basis for transferring data to the State District Sanitary Inspector ('SDSI), i.e. laws imposing legal obligations in the field of preventive health care and the public interest in the field of public health, which is the prevention of infectious disease epidemics.

The facts

The plaintiffs filed a complaint with the DPA about irregularities in the processing of their personal data and the data of their minor son by the hospital, by making them available to the SDSI. In their complaint, the plaintiffs wrote that they had received a letter from the SDSI regarding the preventive vaccination of their minor son. According to the plaintiffs, the SDSI came into possession of their data and the data of their minor son unlawfully and, in their opinion, the data were provided by the hospital.

The Authority determined that the parents with legal custody of their minor son failed to comply with the vaccination requirement regarding their minor. In the course of the investigation it was established, that the hospital whose actions were challenged in the complaint did not pass on data to the SDSI, and therefore the proceedings in this regard were discontinued. The vaccination data processed by the SDSI came from the outpatient facility.

Key findings

- ✓ The Authority pointed out that the SDSI processing of the personal data of the plaintiffs and their minor son was legally based on Article 5(1)(1)(b) of the Polish Law on Prevention and Control of Infections and Infectious Diseases in Humans, according to which persons residing or staying in Poland must undergo preventive vaccinations pursuant to the rules laid down in that Law.

- ✓ This is another decision by the Data Protection Authority which shows that the processing of vaccination data means the processing of health data, for which it is necessary to establish a legal basis in the provisions of law.

Access to patient data by a doctor for a purpose other than the provision of medical services

#health data #processing basis

October 2022

The Data Protection Authority issued a warning for breaching Article 9(1) in conjunction with Article 5(1)(a) of the GDPR, consisting in accessing and obtaining the plaintiff's personal data through the Electronic Services Platform of the Social Insurance Institution (PUE system) without a legal basis.

The facts

The patient filed a notice of possible crime by a doctor. That same month, the doctor obtained their personal data from the PUE system. The system login was not accompanied by the issuance of a medical certificate or a cancellation thereof. In view of the above, the patient complained about the processing of their personal data by the doctor.

The doctor indicated that they accessed the patient's personal data in order to transfer the patient's chart to the main archive under Article 24(1) and (2) of the Polish Law on Patients' Rights and Patients' Ombudsman. The doctor also indicated that the purpose of the access was to check whether the patient remained on sick leave and whether their leave had been canceled or terminated.

Key findings

- ✓ The Data Protection Authority found that none of the premises laid down in Article 9(2) of the GDPR were met in the case, which meant a breach of the principle of lawfulness of processing. The Authority thus applied a broad definition of compliance with the law, i.e. going beyond Article 6(1) of the GDPR. The Data Protection Authority treated the exceptions in Article 9(2) of the GDPR as legal grounds for processing, independent of those listed in Article 6(1) of the GDPR.

- ✓ The Data Protection Authority also emphasized that even if, in principle, the doctor had a legal basis for processing the patient's health data, given the nature of the services they provided, there were no such grounds in the present case.

Requirement to produce a vaccination certificate

#COVID-19 #consent #sports activities #no legal basis #warning

April 2022

The Data Protection Authority issued a warning for processing personal data contained in the COVID-19 vaccination certificate without a legal basis.

The facts

The plaintiff was interested in swimming courses organized by an entrepreneur. However, they were informed by the entrepreneur's representative that before each class there is a verification of vaccination status regarding COVID-19, and that the production of a certificate is voluntary, but necessary to attend the classes.

The entrepreneur indicated that it runs swimming courses for children and infants, and due to anti-COVID-19 regulations, the limit of unvaccinated people at the courses is exhausted each time due to the participation of 5 children who cannot be vaccinated due to their age.

Key findings

- ✓ According to the Authority, the regulations providing for limits on unvaccinated persons who can take part in activities do not formulate a legal basis for the processing of personal data contained in the COVID-19 vaccination certificate. The data contained in the certificate is health data (Article 9(1) of the GDPR) and, unless any other prerequisite of Article 9(2) of the GDPR has been met, they can only be processed with the consent of the data subject.

- ✓ If participation in the class is conditional on the presentation of a vaccination certificate, the consent given for the processing of personal data is not voluntary, and personal data are processed without a legal basis.

- ✓ Entrepreneurs who verified vaccination certificates during the pandemic restrictions can more than likely expect similar decisions unless they did not record the results of COVID passports verification.

Doctor’s access to patient’s PUE account

#doctor #Social Security #health data #no legal basis #warning

April 2022

The Data Protection Authority issued a warning for accessing and obtaining the patient’s personal data through the Electronic Services Platform of the Social Insurance Institution (PUE system), without a legal basis.

The facts

A patient filed a complaint with the DPA about unauthorized access and a doctor’s acquisition of their personal data from the PUE system. The doctor replied that they had obtained such access based on an unlimited authorization to obtain information about the patient’s health status, issued under Article 26(1) of the Polish Law on Patients’ Rights and Patients’ Ombudsman, and processed the data to check the patient’s health status in connection with a planned endomitosis procedure. The plaintiff claimed that they informed the health care facilities by telephone that they would not consent to the doctor’s access to their medical records, as well as that since they filed for divorce, the doctor is not their attending physician and does not have permission to access data about the patient’s health.

Key findings

- ✓ The DPA stated that a doctor can access the patient’s PUE system, but not in an arbitrary manner, and only for the purpose of issuing a medical certificate (Article 55a paragraphs 1, 2 and 3 of the Polish Law on Social Insurance Cash Benefits during Illness and Maternity).

- ✓ At the same time, Article 26 (1) of the Polish Law on Patients' Rights and Patients' Ombudsman cannot be the basis for processing personal data. A doctor needs to provide another legal basis for processing personal data if they want to access a patient's special category data. Even if the authorization issued under that provision allowed access to medical records, it would apply to a specific health care facility, and not access to the PUE system.

Prescription issued using another patient's personal data

#medical facility #warning #prescription

March 2022

The Data Protection Authority issued a warning to a medical services company for sharing a patient's personal data with third parties in breach of Article 5(1)(a) and Article 9(1) of the GDPR.

The facts

The company's patient files contained information on two individuals with very similar personal data. The doctor mistakenly issued two prescriptions using the plaintiff's personal data and handed them to another patient. The prescriptions were filled by a pharmacy employee who did not notice that a mistake had been made.

The plaintiff learned that a prescription had been issued using their personal data without their knowledge, and consequently filed a complaint with the Data Protection Authority.

Key findings

- ✓ The Data Protection Authority recognized the company as the controller and the doctor as the person authorized to process personal data on behalf of the company.
- ✓ Information on prescribed medications falls under special category of data, and the Authority found a breach of Article 9(1) of the GDPR. In finding a breach of Article 5(1)(a) of the GDPR, the Authority used a broad definition of lawfulness.
- ✓ Despite the fact that there was a breach of confidentiality (disclosure of personal data to unauthorized persons) in the case at hand, in its resolution the Data Protection Authority only concluded that the processing was unlawful. However, the Authority did not evaluate the event in terms of a personal data breach subject to notification to the Authority, and possibly also notification to the data subject.

5. Publicly available data

Processing of personal data appearing in publicly available records

#erasure #KRS #publicly available data

September 2022

Pursuant to Article 58(2)(c) of the GDPR, the Data Protection Authority ordered the company to erase a plaintiff's personal data regarding their name from the company's database and the websites on which it was made public.

The facts

Via the National Court Register (KRS) and the Official Gazette (MSiG) the company, obtained the plaintiff's personal data in terms regarding their first and last names, the PESEL number and their position. The plaintiff requested that the company remove their personal data both from the company's database and from the websites where the company published the information. The company refused, indicating that it was unsure of the plaintiff's identity as the person making the request.

Key findings

- ✓ The Data Protection Authority pointed out that the acquisition of business data found in publicly available sources may be supported by Article 6(1)(f) of the GDPR. However, given that the plaintiff had no longer held any position in an entity subject to entry in a publicly available register for several years, the purpose of the company's processing of such data ceased, and its further processing was not justified under Article 6(1) of the GDPR.

- ✓ At the same time, the Data Protection Authority pointed out that the processing of data not currently subject to registration is certainly no longer necessary for the openness of legal transactions, and those interested in current data can access it on their own via the KRS and the MSiG. Any reference to the company's websites after typing the plaintiff's name into an Internet search engine unquestionably breaches their privacy rights.

- ✓ The decision in question is important from the point of view of the controllers who base their activities on the processing of data contained in public records, as the Authority appears to have made the legality of the processing partly dependent on the accuracy of the data.

Commercial use of MSiG data

#public records #data scraping #MSiG

July 2022

The Data Protection Authority refused to grant the request.

The facts

The plaintiff declared bankruptcy, and that information, along with the plaintiff's publicly available data, was posted by the controller on its website. The company processed the plaintiff's personal data from the Official Gazette (MSiG) citing its legitimate interest in providing commercial information services. The plaintiff filed a complaint with the Data Protection Authority to oblige the company to erase the data. As the bankruptcy proceedings were terminated, the controller granted the plaintiff's objection and erased their data.

Key findings

- ✓ The Data Protection Authority pointed out that the processing and public release of publicly available bankruptcy data constitutes the realization of the legitimate interest of providing information services as offered by the controller.
- ✓ According to the Authority, the legitimate interest conditioning the legitimacy of the processing of personal data also existed after the conclusion of the bankruptcy proceedings against the plaintiff. Consequently, the controller did not have to grant the plaintiff's objection.
- ✓ At the same time, the Authority stated that the fact that the plaintiff's data were publicly available further supported the lack of grounds for assuming that the processing of the data by the controller even potentially infringed the plaintiff's privacy. The latter statement is particularly relevant from the point of view of all entrepreneurs whose data are available in publicly accessible registers. As it seems, the Data Protection Authority allows a broader possibility of use in terms of such data by representatives of the private sector.

6. Labor issues

Need to put phone number on a shipment

#processing rules #warning #shipment

September 2022

The Data Protection Authority issued a warning to a controller for breaching Article 6(1) in conjunction with Article 5(1)(a), (b), (c) and (f) of the GDPR by making the plaintiff's data, which included mobile and landline telephone numbers, available to unauthorized persons by writing the numbers on an envelope addressed to the plaintiff.

The facts

The plaintiff was the controller's employee under an employment contract and served as secretary of the district board. In connection with the scheduled meeting of the district board presidium, a parcel was sent to the plaintiff through the postal operator, on which the plaintiff's first and last names, address, mobile and landline phone numbers were placed. The controller explained that the plaintiff's phone numbers were placed on the parcel to make it easier for the courier to contact the plaintiff and because they were necessary when the parcel was posted.

Key findings

- ✓ In the first place, the Data Protection Authority pointed out that the disposal of an employee's phone number is voluntary. In a situation where the employer obtains the phone number as part of a recruitment, it declares a single purpose for processing the data. Thus, using the same for a new purpose, such as posting documents, requires obtaining the employee's consent.

- ✓ In the case in question, the plaintiff's data were processed for the purpose of notifying them of the date of the presidium meeting, and this was, in the Authority's opinion, lawful (Article 6(1)(b) of the GDPR). However, in the opinion of the DPA, in order to post a letter, it is necessary to process data only in terms of the first and last names and home address, which makes the inclusion of a private telephone number and, even more so, a second (landline) telephone number, a breach of the principle of data minimization (Article 5(1)(c) of the GDPR) and results in the impossibility of basing this

processing on the legal basis contained in Article 6(1)(b) of the GDPR.

- ✓ The plaintiff had never agreed to provide their phone numbers by placing them on letter envelopes. In further, having analyzed the evidence, the DPA pointed out that providing a phone number for the courier company's postal service was not required in this case and was only associated with an additional fee. As a result of the disclosure of the plaintiff's phone numbers, their data could be accessed by unauthorized persons, including, in particular, employees of the courier company's service point, as the breach lasted from the moment of posting the parcel until its delivery.

- ✓ The Authority also referred to breaches of other data processing principles indicated in Article 5 of the GDPR, claiming, among other things, that the principle of purpose limitation occurred, as the controller further processed the plaintiff's personal data regarding their mobile and landline telephone numbers in a manner incompatible with the purposes for which the data were collected.

- ✓ On the other hand, given that the plaintiff's personal data had been disclosed to unauthorized entities, the employer failed to ensure adequate data security. The controller's action did not rely on any basis for personal data processing under Article 6(1) of the GDPR, and consequently also breached the principles of legality, fairness and transparency. With regard to the principle of transparency, the Data Protection Authority clarified that the breach consisted in the failure to specify all the purposes for which the plaintiff's personal data would be processed with their consent.

Processing of employee's personal data after termination of employment

#contract #employment contract

June 2022

The Data Protection Authority discontinued proceedings under Article 105 § 1 of the Code of Administrative Procedure with regard to the allegation that an employer made a plaintiff's data available to another entity. In the remaining scope, i.e. as regards irregularities in the processing of the plaintiff's data by the employer, involving the processing of their personal data after the termination of their employment, the DPA refused to grant the request.

The facts

The plaintiff was an employee of a company which processed their personal data in connection with the plaintiff's employment under an employment contract. The plaintiff claimed that the company denounced them to another company in order to hinder their employment opportunities with that entity, after their employment had been terminated.

Key findings

- ✓ As pointed out by the Data Protection Authority, given the provisions of the Labor Code, the company must keep the plaintiff's personal data for ten years following the date of termination of employment with the company. That means that the company processes the plaintiff's personal data based on Article 6(1)(c) of the GDPR, and thus the plaintiff's request that the company erase their personal data has no legal justification.

- ✓ In addition, the analysis of the evidence by the Data Protection Authority did not show that there had been a transfer of the plaintiff's data to another company. Consequently, the DPA discontinued the proceedings as irrelevant.

Disclosure of the plaintiff's personal data in response to a court witness subpoena

#company #warning #litigation

September 2022

The Data Protection Authority issued a warning to a company for breaching Articles 6(1) and 5(1)(a) of the GDPR. The breach consisted in the company disclosing the plaintiff's personal data (address, PESEL number and information on pending court proceedings) to third parties for the purposes of litigation.

The facts

The plaintiff was an employee of the company, but after a certain period their employment contract was terminated with in accordance with Article 52 § 1(1) of the Labor Code.

Consequently, the plaintiff initiated legal proceedings to defend their rights. In the case at hand, the company disclosed the plaintiff's personal data to individuals who received responses to individual subpoenas as witnesses from the company's legal department.

Key findings

- ✓ The Data Protection Authority pointed out that the company had not demonstrated any of the premises under Article 6(1) of the GDPR that would entitle it to process the plaintiff's data involving the disclosure of personal data to other parties, nor had it demonstrated that such parties had approached the company with a request for access to such data.
- ✓ In the case at hand, the DPA, having regard to the company's cooperation with the Authority during the course of those proceedings and the one-time but irreversible effect of the breach, resolved that it was sufficient to exercise the right provided for in Article 58(2)(b) of the GDPR, and issued a warning to the company.
- ✓ The decision is important from the point of view of employee data, to which only a limited group of individuals should have access, only to the minimum necessary extent.

Need to precisely determine legal basis for data processing

#contract of mandate #information obligation #labor code #order

March 2022

The Data Protection Authority ordered compliance with the information obligation by indicating the legal basis for processing the contractor's personal data, the recipients or categories of recipients of their personal data, and the periods of processing of their personal data.

The facts

A company submitted an information clause to the contractor, in which it included the purposes of processing personal data. Regarding the basis for processing personal data, it indicated that the data would be processed: 'in accordance with the provisions of the Labor Code.' The submitted information clause did not contain information about the recipients or categories of recipients of personal data (despite the conclusion of a data processing agreement with an accounting office) or the periods of data processing. The plaintiff claimed, among other things, that the information obligation had not been fulfilled, that the company had not delivered a copy of the information clause, and that information clause contained their PESEL number.

Key findings

- ✓ According to the DPA, entrepreneurs must accurately indicate the basis for the processing of personal data, which cannot be left to the conjecture of the data subject. The indication that an entrepreneur processes the contractor's personal data based on the Labor Code is therefore incorrect, since the provisions of the Labor Code do not apply to contracts of mandate.

- ✓ The Data Protection Authority argued that the requirement for an employee to provide their PESEL number in an employee information clause, as evidence indicating that a specific employee has read the clause, does not constitute a breach of the provisions of the GDPR, as the data are processed for the purpose of fulfilling tax and social security obligations. As it seems, the Authority equated the legality of

processing the PESEL number for the purpose of fulfilling the employer's statutory obligations with the situation when such information is processed only for the purpose of ensuring sufficient traceability or distinguishability of the employee or contractor. The settlement is particularly interesting, given the special importance that the DPA attributes to the PESEL number, as well as the relevance of the consequences that the Authority assumes if such information is covered by a breach of personal data protection.

- ✓ The Authority's position that the failure to physically provide a copy of the information clause to an employee or contractor does not, in itself, constitute a breach of the GDPR as long as the person in question could learn about the information obligation may also be important from the controllers' perspective. The popularization of the above-mentioned opinion of the Data Protection Authority would in practice allow controllers to reduce the number of printed information clauses, and, as a consequence, probably also reduce costs.

Repeated employee error resulting in unlawful data processing

#entrepreneur #warning #employee error

October 2022

The Data Protection Authority issued a warning to an entrepreneur for breaching Articles 6(1) and 17(1)(d) of the GDPR by processing a plaintiff's data including their e-mail address without a legal basis and failing to comply with their request for data erasure submitted pursuant to Article 17(1)(d) of the GDPR.

The facts

In their complaint, the plaintiff pointed out that they had never used the entrepreneur's services and had never subscribed to its newsletter. No contract had ever been concluded between the entrepreneur and the plaintiff regarding services offered by the entrepreneur (Article 6(1)(b) of the GDPR). Nor was there any other premise based on which the entrepreneur could process the plaintiff's personal data and conduct marketing activities towards them. The entrepreneur processed the plaintiff's data as a result of an employee error. The plaintiff requested that the entrepreneur erase their personal data, which the entrepreneur did. However, as a result of the same mistake, i.e. the misspelling of an e-mail address of the entrepreneur's other customer with the same name as the plaintiff, the plaintiff's e-mail address was again entered into the entrepreneur's database and the plaintiff again received a marketing e-mail, despite their previous erasure request.

Key findings

- ✓ As pointed out by the Data Protection Authority, it was possible to avoid the error of entering the wrong e-mail address of the entrepreneur's customer and thus avoid unlawful processing of the plaintiff's e-mail address. The entrepreneur's employee should have been more diligent in reading the e-mail address or should have taken other measures to exclude the possibility of an error due to which an incorrect e-mail address is recorded in the database. This is yet another decision in which the DPA highlights that the controllers must process valid and accurate data.

Repeated employee mistakes as a threat of administrative penalty by the Data Protection Authority

#association #error #warning

September 2022

The Data Protection Authority issued a warning to an association for breaching Article 6(1) of the GDPR by processing the plaintiff's personal data to send them commercial correspondence without a legal basis. In the remaining scope, the DPA discontinued the proceedings.

The facts

An association obtained the plaintiff's data in connection with their donations to the association. After the plaintiff's initial request for their data to be erased, an investigation was carried out, as a result of which the processing of such data was limited to processing within the extent and for the purposes required by the applicable tax and accounting regulations. Thus, the plaintiff's objection to sending correspondence to his address was granted.

However, as a result of an error by an association employee, the plaintiff was included in a subsequent mailing, and as a result, the plaintiff received correspondence regarding possible future donations. After identifying the source of the error, the association ceased to process the plaintiff's personal data, beyond what was required by applicable law.

Key findings

- ✓ The Data Protection Authority stated that it is unacceptable 'for a data controller to be permanently mistaken about the erasure and restoration of personal data.' Any such mistake indicates a failure to apply appropriate technical and organizational measures to secure data processing in accordance with applicable law. Unsupported statements by an entity may prove unreliable in the future.
- ✓ The DPA indicated that if similar breaches occur in the future, it will be obliged to take additional actions it is authorized to take under the law, and which may lead to the imposition of an administrative fine on the association.

- ✓ Thus, this is another ruling by the Authority which should draw the controllers' attention to the necessary and regular training of employees in handling data subjects' requests.

No authorization for unauthorized parties to process employee data

#HR #authorizations #restriction of access

September 2022

The Data Protection Authority issued a warning for a disclosure of personal data regarding non-renewal of an employment contract and information on the plaintiff's financial situation as the reason for non-renewal of their employment contract in the presence of unauthorized persons.

The facts

The plaintiff's superior told them, in the presence of two other company employees, that the plaintiff's fixed-term employment contract would not be renewed. The plaintiff's superior said that the reason for not renewing the contract would be, among other things, the plaintiff's good financial standing.

According to the company's position, the persons present at the conversation were carrying out international development projects involving the plaintiff and therefore, in the company's opinion, their presence was required. In no manner had the company authorized the aforementioned persons to process personal data.

Key findings

- ✓ Employee information, including information on specific events, such as termination of an employment contract or non-renewal of the same may only be available to a limited number of persons at the employer's. Such persons include, for example, managers supervising the workplace on the employer's behalf, legal advisors providing legal services for the employer, or HR personnel.

- ✓ This is an important ruling from the point of view of employers who more often than not terminate employment contracts in the presence of witnesses. As implied by the contemplated ruling, witnesses must not be casual company but should be correctly authorized to process personal data, with the scope of their duties justifying the disclosure of employee information to them.

Monitoring of business e-mail

#monitoring #employer #e-mail

September 2022

The Data Protection Authority found breaches of data protection provisions in connection with the use of monitoring of business e-mail and issued warnings and ordered the erasure of personal data obtained in connection with the monitoring.

The facts

The employer, while the plaintiff was absent from work, checked the contents of the plaintiff's company computer, including e-mail monitoring. The plaintiff's private correspondence was located on the company mailbox.

In its explanations the company replied that the reason for using the tools to conduct the inspection was to determine whether the plaintiff used the devices properly and only for business purposes. The company emphasized in its explanations that it did not monitor employees' e-mails under Article 22^3 § 1 of the Labor Code. As a result of the checks, the company determined that the plaintiff used the computer provided to them for purposes unrelated to their work.

The company had not established, as required under Article 22^2 § 6 of the Labor Code, the purpose, scope and manner of use of business mail monitoring at the workplace and had not regulated those issues in the work regulations.

Key findings

- ✓ The company breached the principles of personal data processing, as it had not specified the purpose and scope for which personal data obtained in the course of applying the monitoring were processed. It also carried out the challenged inspection activities in breach of the principles of legality, reliability and transparency.
- ✓ The Data Protection Authority made it clear that the processing of personal data via monitoring of business e-mail will be lawful, as long as the prerequisites set forth in the Labor Code provisions relating to monitoring have been met.

Creating a Facebook account for an employee

#employer #warning #Facebook

April 2022

The Data Protection Authority issued a warning to the Special Needs School and Educational Center ('Center') for breaching Article 5(1)(a) and (b) and Article 6(1) of the GDPR by using the plaintiff's personal data to create a Facebook account. In the remaining scope, the DPA denied the plaintiff's request.

The facts

The plaintiff was an employee of the Center, and the latter processed their data in connection with the performance of employment service tasks and employee benefits arising from the employment relationship. The Center created a Facebook account for each of its teaching personnel and indicated that the plaintiff's personal data used to create the account was widely known to parents and students and was also available on the Center's website. The basis for processing the plaintiff's data to create the Facebook account the Center alternatively indicated was Article 6(1)(e) or (f) of the GDPR.

Key findings

- ✓ According to the Authority, the Center failed to prove that they had met the prerequisites indicated in Article 6(1)(e) or (f) of the GDPR, authorizing it to process the plaintiff's data by creating their Facebook account. At the same time, the DPA did not find other prerequisites, listed in Article 6(1) of the GDPR, based on which the Center could lawfully process the plaintiff's personal data for this purpose.

- ✓ The DPA also emphasized that the Center used the plaintiff's personal data from the dataset 'Employees, contracts of mandate, former employees' processed for the purpose of performing employment tasks and resulting from the employment relationship and employee benefits. In the opinion of the Data Protection Authority, setting up the plaintiff's account on the social networking site does not fall within the scope of tasks related to employment services arising from the employment relationship and employee benefits. Thus, the plaintiff's personal data were processed contrary to the purpose for which they were collected.

- ✓ However, it has to be assessed in the second step whether there is a negative condition in the given circumstances, i.e. whether there are interests or fundamental rights and freedoms of the data subject that override the legitimate interests of the controller or a third party.

Online disclosure of personal data by a company without a legal basis

#company #warning #online publication

September 2022

The Data Protection Authority issued a warning to a company for breaching Article 5(1)(c) in conjunction with Article 6(1) of the GDPR, consisting in disclosing personal data including the plaintiff's first and last names, as well as information regarding cash payment as compensation for unused vacation leave, contained in the company's internal records, by publishing them online. In the remaining scope, i.e. regarding an inspection at the company's headquarters, the DPA refused to grant the request.

The facts

The company, without the plaintiff's knowing or consent, published the plaintiff's personal data including their first and last names, as well as data regarding cash payment as compensation for unused vacation leave, at publicly accessible Internet addresses. Those addresses were repeatedly published on popular online portals.

In connection with the initiation of the proceedings, the Data Protection Authority requested the company in writing to provide explanations, but the company did not reply whatsoever within the statutory timeframe. As of the date of the decision, the links redirecting to the websites were inactive.

Key findings

- ✓ On the basis of the evidence collected, the Data Protection Authority concluded that the company had failed to fulfil any of the prerequisites indicated in Articles 5(1) and 6(1) of the GDPR with regard to making the plaintiff's personal data contained in the company's internal records available online to an unlimited circle of recipients. Interestingly, in the aforementioned regard, the Data Protection Authority pointed out that the company had not complied with Article 5(1)(c) of the GDPR, i.e. with the principle of data minimization, which seems secondary to the absence of any legal basis for the processing of any of the plaintiff's data, involving the online publication of the plaintiff's personal data.

- ✓ The Authority also referred to the plaintiff's request to inspect the controller and the request to order compliance with the obligation under Article 34 of the GDPR. In both cases, according to the Authority, individual plaintiffs had no legal basis to demand that their requests be granted by the Data Protection Authority. The DPA emphasized that: '[t]he above-mentioned obligations are related to the processing of any personal data, and not to the rights of data subjects under the provisions of the GDPR. It is not possible to derive the data subject's right to demand the fulfillment of a specific obligation by the controller from those legal norms.' This last conclusion is particularly interesting from the perspective of data subjects, given that Article 34 of the GDPR is aimed directly at protecting them.

7. Claims

Obligations of an entrepreneur in connection with the processing of a debtor's data

#entrepreneur #warning #claims recovery

July 2022

The Data Protection Authority issued a warning to an entrepreneur for breaching Article 12(1) and (3) in conjunction with Article 17(1) of the GDPR by failing to respond to the plaintiff's request for erasure of their personal data. In the remaining scope, the DPA refused to grant the plaintiff's request.

The facts

The entrepreneur obtained the plaintiff's personal data from the plaintiff in connection with a text message sent by the plaintiff and in connection with the conclusion of an oral contract for the performance of work. In connection with the aforementioned contract, a claim arose from the entrepreneur against the plaintiff, and the entrepreneur instructed a company to collect the debt incurred by the plaintiff. The plaintiff requested the entrepreneur to erase their personal data, to which the entrepreneur did not respond.

Key findings

- ✓ The Data Protection Authority indicated that the acquisition and processing of the plaintiff's personal data had its legal basis in Article 6(1)(b) of the GDPR, as it was related to a contract concluded by the parties. The disclosure of the plaintiff's data by the entrepreneur for the purpose of asserting claims, in turn, was justified under Article 6(1)(f) of the GDPR. In the Authority's view, a debtor who defaults on their obligations must face the consequences under the rules governing business dealings, as the debtor's attitude must not lead to the privileging of their legal position and unjustified protection of the defaulter.

- ✓ However, under the contemplated circumstances, the Authority found that although the request for erasure of the data subject's data was not legitimate, it was appropriate to issue a warning, as the controller had failed to comply with its obligation to communicate with data subjects, i.e. it had been in breach of Article 12(1) and (3) in conjunction with Article 17 of the GDPR.

Processing of recorded image and voice for the purpose of defense against claims

#claims #image #schooling

September 2022

The Data Protection Authority ordered an educational cooperative to erase personal image and voice data captured in a recording of a meeting, processed without a legal basis.

The facts

The plaintiff, employed as a teacher at schools run by the educational cooperative, indicated that the cooperative, in breach of the law, intentionally and knowingly processed their personal data (including their disclosure). The plaintiff claimed that the cooperative processed and disclosed their image and voice captured on recordings of meetings. The Authority found that the cooperative processed the personal data of the plaintiff as a member of the cooperative and in connection with the termination of their employment. The cooperative indicated that the recording served to record the meeting and to defend against the plaintiff's possible claims resulting from the termination of the employment relationship and a conflict involving, among other things, potential breaches of the parties' personal rights. The cooperative issued a statement containing the plaintiff's personal data (first and last names, description of behavior), and sent it to nine institutions and the plaintiff in order, as it indicated, to defend its good name and to counter unlawful and unfounded allegations.

Key findings

- ✓ The cooperative was authorized to process the plaintiff's personal data under Article 23(1)(2) of the Law of 29 August 1997, until 25 May 2018, currently Article 6(1)(c) of the GDPR, in connection with the provisions of the Cooperative Law of 16 September 1982.

- ✓ However, according to the Authority the processing of the plaintiff's data from the recordings of a meeting was not necessary for the purpose of defending against or pursuing

possible claims. The cooperative failed to demonstrate that necessity and need for further processing of the plaintiff's personal data, limiting itself only to justifying the processing with unspecified claims and a contemplated action for breach of personal rights.

Processing of debtor's data versus possible investigation of the existence of a claim

#debtor #credibility #civil court #justification of claims #refusal to grant a request

April 2022

The Data Protection Authority refused to grant a complaint.

The facts

The entrepreneur refused to erase the plaintiff's personal data, indicating that the plaintiff had a debt arising from the use of a service operated by the entrepreneur. The plaintiff emphasized that they had not agreed with the additional fee charged by the entrepreneur and therefore there was no debt whatsoever. In addition, the plaintiff indicated that they did not consent to the debt being assigned to another entity.

Key findings

- ✓ The DPA, citing the case law of the administrative courts, emphasized that it had no jurisdiction to examine the existence or nonexistence of claims, or the fairness and scope of the asserted civil law claims. Those issues can only be examined by a civil court. As long as the validity of the contract has not been challenged, the contract is a document that produces certain legal effects, also under the Data Protection Law.

- ✓ The Authority also pointed out that as long as the payment of the amounts due has not been effectively settled by a civil court and the court has not declared the debt assignment agreement invalid, the entrepreneur may process personal data on the basis of Article 6(1)(b) of the GDPR.

- ✓ The Data Protection Authority also argued that in the case of a sale of an online service and the related sale of the claim, it was also reasonable for the previous owner of the website to provide the plaintiff's personal data to the website buyer, which occurred pursuant to the website purchase agreement and the assignment of the claim.

Processing of data of the debtor's heir to assert claims

#finance #creditor #heir

August 2022

The Data Protection Authority ordered the erasure of personal data of a debtor's heir due to the lack of a legal basis legalizing the processing as specified in Article 6(1) of the GDPR.

The facts

The plaintiff's father entered into a loan agreement. Due to non-payment of the debt, the creditor sold the claim to a company. The company then transferred the claim to a fund. At that time, the plaintiff's father died. The fund, along with the company, as joint controllers of data regarding the claimed debt, took steps to confirm that circumstance and to determine the legal successors of the deceased debtor. In the case run by the enforcement agent, the agent identified potential heirs of the deceased, including the plaintiff.

In the opinion of the Data Protection Authority, the provisions indicated by the company, including, among others, Article 442[1] of the Civil Code in conjunction with Article 92 of the Polish Law on Personal Data Protection of 10 May 2018, in conjunction with Article 82 of the GDPR, do not constitute a premise legalizing the processing of the plaintiff's data, as the plaintiff is not and has never been a debtor to the fund or the company.

Key findings

- ✓ The Authority pointed out that it is common courts which have the jurisdiction to examine who is the heir, i.e. the person who stepped into the rights and obligations of a deceased testator. Neither the fund nor the company are entitled to determine the circle of the debtor's heirs in their own discretion. Consequently, the fund and the company have not fulfilled any of the prerequisites laid down in Article 6(1) of the GDPR, which could authorize the processing of the plaintiff's personal data for the purpose of asserting claims against them.

- ✓ The circumstance justifying the processing of personal data for the purpose of pursuing a claim is the mere fact of the existence of a claim and the intention to assert it, but not a change in the litigation rights of the defendant entity.

Direct marketing based on the purchased database

#information obligation #data access #direct marketing #data subject claims

October 2022

The Data Protection Authority issued a warning for failing to provide full information regarding the source of personal data obtained by the first controller and refused to grant the request regarding the second controller's failure to comply with the obligation referred to in Article 15(1) of the GDPR. In addition, the Authority ordered both controllers to erase the plaintiff's personal data.

The facts

The first controller sold a database containing personal data, including those of the plaintiff, to the second controller. The purchasing controller performed an information obligation to the plaintiff at their e-mail address.

The plaintiff demanded explanations from both controllers, including what data were sold, who sold it, on what basis, to whom the data were sold, the legal basis for processing the data. The plaintiff filed a complaint with the Data Protection Authority about irregularities involving the processing of their data without a legal basis, failure to comply with a request for access to the data, and failure to comply with a request to erase the data.

In the course of the proceedings before the Authority the controllers cited as the basis for processing the legitimate interest of establishing, investigating or defending against the plaintiff's claims.

Key findings

- ✓ In the opinion of the Data Protection Authority, in the case of the sale of the database, there was no reason for the data subject to expect both the acquisition and processing of their personal data for direct marketing purposes by the new controller (purchaser). This is because there was no connection between the data subject and the new controller.

- ✓ In accordance with its previous ruling practice, the Authority questioned the processing of personal data by both controllers for the purpose of establishing, asserting or defending against possible claims. As it seems, in the Authority's view, the plaintiff's filing of a complaint with the Data Protection Authority did not sufficiently justify the controllers' assumption that the plaintiff would file claims against them.

- ✓ In view of the plaintiff's objection and the Authority's exclusion of legitimate interest as the legal basis for processing, in the opinion of the Data Protection Authority, the controllers were left with no basis for processing personal data, which resulted in an order to erase the plaintiff's data. The decision may have significant practical consequences: if enforced, the controllers will be deprived, among other things, of the possibility to defend themselves in civil proceedings.

8. Video surveillance

Video surveillance versus footage showing multiple persons

#surveillance #image #data copy #refusal to grant a complaint

April 2022

The Data Protection Authority refused to grant the complaint.

The facts

A company operated a video surveillance system based on its legitimate interest in ensuring security on the premises, protecting property and preventing criminal acts. The plaintiff requested that the company provide them with a copy of their personal data.

The company refused on the grounds that there was no information to uniquely identify the plaintiff on the recording, and no indication of a legal interest entitling the plaintiff to obtain a copy of the recording, no indication of the occurrence of criminal acts on the secured recording, as well as that the recording featured many other people. The plaintiff was of the opinion that there was a data breach in connection with the use of video surveillance and objected to the processing. The company refused to comply with the data subject's right to object.

Key findings

- ✓ In the contemplated decision, the Data Protection Authority made some interesting observations. First of all, the DPA pointed out that in a situation where the plaintiff provided insufficient information to identify them as the person featured in the recording (e.g. by specifying their clothing, the way they moved), the controller was not obliged to call on them to provide additional information. According to the Authority, the initiative in this regard rested with the plaintiff.

- ✓ Further, the Authority argued that the mere recording of the image of multiple persons in a recording cannot give grounds for refusing to grant a request for a copy of the data when the request is made by one of the persons visible in the recording. In order to ensure that handing over a copy of the recording did not result in a breach of the rights and freedoms of third parties, it was the controller's duty to remove information the

disclosure of which could breach such third-party rights, for example, by anonymizing their image. Unfortunately, the Data Protection Authority did not cite more practical guidelines in this regard.

- ✓ Regarding irregularities involving inadequate security of personal data processing or the failure to appoint a data protection officer, the Authority pointed out that data processing safeguards are examined in the course of general personal data processing practices. An individual has no legal interest in the ruling issued in this regard, and therefore an inspection covering the security of data processing or the fact of appointing a data protection officer is an autonomous competence of the Data Protection Authority.

- ✓ Finally, the Authority also clearly defined the legal basis for the processing of personal data in the case of handling requests from data subjects raised under the provisions of the GDPR: according to the DPA, the fulfillment of requests is a legal obligation of controllers, and therefore the basis for processing is Article 6(1)(c) of the GDPR.

Video surveillance of a public place using a disabled camera

#video surveillance #burden of proof #information obligation

October 2022

The Data Protection Authority ordered that the processing of the plaintiffs' personal data be discontinued and issued a warning to the controller for failing to fulfill its duty to inform the plaintiffs.

The facts

The controller installed a camera on its building, the field of view of which covered part of its property and the access road of which it was a co-owner, and which was accessed by third parties. The camera's range did not cover neighboring properties owned by the plaintiffs. The installation of the cameras was dictated by the troublesome behavior of the neighbors.

The neighbors complained to the Data Protection Authority about irregularities in the processing of their data, involving the processing of their image without a legal basis and the failure to comply with the information obligation.

The Authority found that the controller had never activated the camera, as its mere presence caused 'the problems with the troublesome neighbors to cease.'

Key findings

- ✓ The Authority stated that the fact that the surveillance covered (could cover) an access road that could be used by third parties meant that it was necessary to ensure that the processing complied with the GDPR, including compliance with the information obligation to data subjects. Following the Court of Justice of the European Union, the Data Protection Authority resolved that in this case the data processing is not of a purely personal or domestic nature.

- ✓ The DPA issued a warning for failing to fulfill the information obligation. At the same time, it did not order its fulfillment, since 'the obligation cannot be complied with in regard to data that the plaintiff will no longer process.'

- ✓ What is of particular importance, the Authority pointed out that ‘an undisputed proof that the data had not been processed by means of video surveillance would be the dismantling of such a device or directing it permanently out of the disputed surveillance area,’ thus introducing a quasi-presumption of data processing arising from the fact that the camera had been installed.

- ✓ In the course of the proceedings the Authority did not prove that the defendant processed any personal data but inferred that precisely from the fact that the defendant had installed a surveillance camera. According to the DPA, the fact that the camera was switched off during the proceedings was irrelevant as the possibility of switching on the camera and the use of surveillance were at the sole disposal of the defendant.

- ✓ The decision in question suggests that even in the absence of active surveillance of an area accessible to third parties, the mere fact of mounting a (potentially working) camera may result in the application of the GDPR provisions and the imposition of a potential sanction.

Video surveillance and litigation

#surveillance #assertion of claims #no legal basis #school #warning

March 2022

The Data Protection Authority issued a warning to a school for illegally storing personal data obtained through video surveillance for later access in case of eviction proceedings and ordered the head of the municipality to erase it.

The facts

A school installed video surveillance to ensure the safety of the school's students and staff and to protect its property. The plaintiffs' data were processed due to the fact that they were tenants of an apartment located at the school premises.

Surveillance data were provided to the police, the Municipal Police and the head of the municipality in security-threatening situations, for administrative and eviction proceedings. The plaintiff pointed out that the school's surveillance breached their privacy by, among other things, directing one of the cameras to the entrance of their apartment and continuous surveillance, and that the recordings were unfoundedly released for eviction proceedings.

Key findings

- ✓ According to the Authority, the transfer of data to the head of the municipality as evidence in eviction proceedings could not be grounded on the provisions of Article 6(1) of the GDPR and went beyond the purpose of the school surveillance, i.e. to protect the property and ensure security.

- ✓ The Data Protection Authority also found that collecting data about an individual for a future, uncertain event, the occurrence of which would only secondarily legalize the processing of such data, is a mispractice. In other words, a legal basis for data processing cannot be subsequently formulated if the initial data processing was illegal.

- ✓ The Authority emphasized that the type of the supervisory measure it used had been influenced by the breaching entity's cooperation with the Authority during the proceedings.

Result of arbitrary surveillance and voice recording

#neighbors #audio surveillance #voice recording

July 2022

The Data Protection Authority ordered the defendant to cease the processing of personal data in connection with audio surveillance, as well as to erase the data from the recordings previously made. It also issued a warning for breaching Article 13(1) and (2) of the GDPR for failure to comply with the information obligation.

The facts

The data subject filed a complaint with the Data Protection Authority, indicating that they live on a property directly bordering the property of the defendant, who had been conducting audio surveillance for a year and who had been secretly recording the plaintiff. According to the latter, the defendant justified the use of surveillance complaining about excessive noise from the plaintiff.

At the same time, the plaintiff pointed out that their neighbor did not ask them to reduce noise emissions and did not notify them of the noise level measurement being conducted. The plaintiff also suspected that the use of audio surveillance was aimed at obtaining information that was the plaintiff's business secret.

Key findings

- ✓ The Data Protection Authority referred to the qualification of voice as information constituting personal data. According to the Authority, the voice is an autonomous, unique and characteristic feature of an individual. The Data Protection Authority emphasized that another human being, no matter how they try, will not be able to emit sounds, i.e. produce vibrations, of identical intensity, and therefore a person's voice, including that recorded on a digital medium, constitutes personal data as it allows others to identify an individual.

- ✓ The Data Protection Authority also pointed out that only law enforcement and special services have the Authority to use the voice recording function, under statutory regulations

applicable to their operations, a function that was not exercised by the plaintiff.

- ✓ The Authority also noted that because the audio surveillance covered an area not owned by the defendant, the defendant was obliged to process data in accordance with the provisions of the GDPR, including the fulfillment of the information obligation.

- ✓ The Authority also argued that the audio surveillance carried out by means of a device used for, among other things, voice recording, is not appropriate and necessary to achieve the defendant's goal of measuring noise intensity. In the Authority's view, the defendant could have pursued its legitimate goal by means of other devices, less intrusive to the plaintiff's fundamental rights and freedoms, such as measuring only the sound intensity using a decibel (sound) meter. Measuring noise emissions with a device that allows simultaneous measurement and realistic recording of sound, while at the same time collecting voice data constituted, in the Authority's opinion, a redundant process that could not be considered a legally legitimate goal.

- ✓ At the same time, the Data Protection Authority pointed out that the continuous use of the audio recording function in connection with audio surveillance leads to a breach of, among other things, the right to privacy of the person being recorded and, in the case of a business entity, also to the possibility of infringing business secrets.

Obligation of the court to provide copies of personal data

#court #order #vision in surveillance footage

June 2022

The Data Protection Authority ordered the district court to comply with the plaintiff's obligation under Article 15(3) of the GDPR by providing the plaintiff with a copy of their personal data contained in the video surveillance recordings from cameras installed in the court building, in public areas of corridors and the stairwell, as requested by the plaintiff.

The facts

The court conducted video surveillance in the building to ensure the safety and public order of persons and property on the court premises. The court processed the personal data of the plaintiff legal counsel in the form of their image recorded on the video surveillance footage. The plaintiff requested that the court provide them with a copy of their personal data in the form of the recording, after anonymizing the image of other persons featured in the footage. The court refused to grant the plaintiff's request.

Key findings

- ✓ In the opinion of the Data Protection Authority, the court unjustifiably refused to provide the plaintiff with the requested copy of personal data. According to the Authority, the court should have the (technical) ability to comply with that plaintiff's right and should have foreseen that it is incumbent on the court to guarantee the data subjects the possibility of exercising their right of access in connection with the processing of personal data obtained by means of surveillance.

- ✓ In addition, in the DPA's opinion, the court's failure to implement appropriate technical measures to remove the images of other persons captured on the recordings does not constitute grounds for denying the plaintiff's right under Article 15(3) of the GDPR.

9. Personal data breach

Proper notification and irrelevant proceedings

#notification of data subjects
#irrelevant proceedings #discontinuation of proceedings

September 2022

The Data Protection Authority discontinued the proceedings for incomplete notification of data subjects under Article 34(2) of the GDPR, as there had been a new, correct notification before the decision was issued.

The facts

The controller notified the data subjects of a data breach involving their data and reported the breach to the Authority. However, the Data Protection Authority found that 'the notification did not meet the conditions set forth in Regulation 2016/679' and ordered that the data subjects be notified again. After the controller requested an extension of the statutory timeframe for complying with the information obligation, the Authority initiated administrative proceedings in the case.

In response to the initiation of the proceedings, the controller notified the data subjects again and informed the DPA of this fact, attaching the contents of the notification. The Authority concluded that the proceedings had become pointless, as the data subjects were properly notified as of the date of the decision, and there were no grounds for applying the remedial powers laid down in Article 58(2)(e) of the GDPR.

Key findings

- ✓ The Data Protection Authority resolved that the proceedings on incorrect notification of data subjects are irrelevant after the data subjects have been correctly notified before the date of the decision.

- ✓ As it seems, it may practically be less risky for controllers to communicate breach to the data subjects as per the DPA's guidelines before the Authority issues its decision, even if there is a disagreement as to the merits of the notification. This is because if the data subjects have been correctly notified, the controllers may avoid the Authority's reaching for the remedial powers the law provides it with.

Ransomware attack

#breach notification #inadequate security measures

August 2022

The Data Protection Authority issued a warning to the controller for breaching the principle of accountability, the principle of data integrity, the principles of privacy by default and by design, and the obligation to ensure the security of processing. In addition, the Authority ordered that processing operations be brought into compliance with the provisions of the GDPR by conducting a risk analysis and implementing appropriate technical and organizational measures.

The facts

As a result of a ransomware attack, the company lost access to its employees' data. Backups containing the data were also encrypted. The company filed a data breach notification indicating that 'there was no data leakage, only encryption.' The company also notified data subjects of the breach, and regained access to the data. The Authority initiated an investigation, during which it found a number of irregularities that threatened data security.

Key findings

- ✓ According to the Data Protection Authority, the aggravating factor for the controller was that although the controller had planned to implement technical security measures and had scheduled a review of the solutions in use, it had not completed the reviews, as well as failed to implement the selected measures.
- ✓ Therefore, when developing certain plans for ensuring the security of personal data, the controllers should bear in mind that the discontinuation of certain activities on their part may be negatively assessed by the Authority.
- ✓ According to the Data Protection Authority, the fact that at the time of the breach some of the equipment was secured using the operating system measures does not mean that the optimum level of processing security was ensured.

- ✓ In turn, according to the Authority, the lack of built-in and updated security features increases the risk of malware infection and attacks by exploiting security vulnerabilities.

Multiple notifications to data subjects

#lost shipment #notification #delay #warning

March 2022

The Data Protection Authority issued a warning to a Municipal Social Welfare Center for incorrectly communicating personal data breach to the data subjects.

The facts

The Municipal Social Assistance Center (‘MSAC") reported a breach involving the loss of a letter by the postal operator. The lost correspondence contained the following personal data: first and last names, address of residence or domicile, PESEL number, description of evidence to determine the alimony debtor and remission of the decision. The MSAC notified the data subjects of the breach several times, but only in the last notification were all the prerequisites of Article 34 of the GDPR fulfilled. In the opinion of the Data Protection Authority, the communication of a correct and adequate description of the possible consequences of the breach to data subjects therefore occurred only after the fourth notice had been sent to them.

Key findings

- ✓ The Authority once again emphasized that in the case of the loss of personal data such as the PESEL personal identification number, when pointing out the possible consequences of a data protection breach, it is not enough to point out only the risk of impersonation to extort additional information or the use of data to register a prepaid phone card that can be used for criminal purposes.

- ✓ Prompt notification of all possible consequences to the individuals affected by the breach is crucial to their ability to counter its negative effects. A delay in proper notification of any possible consequences deprives the aforementioned individuals of guidance on the actions they can take to effectively counter the negative consequences of the breach.

- ✓ The Data Protection Authority is of the opinion that if it is necessary to communicate data breach to the individuals on several occasions, the application of supervisory measures by the Authority is necessary due to the indisputable nature

of the breach and the need to prevent future incompliance in communicating data breaches to the individuals.

- ✓ At the same time, despite a significant similarity of the facts pertinent to the contemplated decision to a decision in which the President of the Office of Competition and Consumer Protection imposed an administrative fine on a bank due to, among other things, the fact that the notification of data subjects did not contain all the mandatory elements referred to in Article 34 of the GDPR, in the case at hand the Authority resolved that the purpose of the proceedings could be achieved by applying a measure of a lesser nature, and the warning would be an appropriate manifestation of the implementation of the principle of proportionality.

Disclosure of personal data via Messenger

#Messenger #warning #scan #breach #no basis for processing

September 2022

The Data Protection Authority issued a warning to a city mayor for breaching Article 6(1) of the GDPR by disclosing the plaintiff's personal data to an unauthorized person without a legal basis.

The facts

The data subject submitted an e-mail request for public information to the city hall. The request contained the plaintiff's personal data.

The mayor mistakenly sent a scan of the aforementioned request via Messenger to an unauthorized person. After the mistake was discovered, the scan was immediately removed from the Messenger conversation, and the breach was described in the city hall's record of breaches and reported to the DPA.

In addition, the plaintiff claimed in the complaint that the city mayor had not informed the Data Protection Authority within the prescribed timeframe about the possibility of a personal data breach.

Key findings

- ✓ Although the operative part of the decision indicates that the warning was issued in connection with the disclosure of personal data via Messenger, in the substantiation for the decision the Data Protection Authority did not address the meaning of using Messenger in the incident.

- ✓ In particular, the Authority found that personal data had been erased from the chat app, without examining the way the application works, i.e. the circumstance that although the sender of the message erased it, the recipient could still be in possession of the message. The lack of analysis in the aforementioned regard is surprising in light of the position

presented by the Data Protection Authority, in which it indicates that the mere fact that the unauthorized recipient of the message committed to erase it does not mean that there had been no data breach or that it did not have further consequences for the data subjects.

- ✓ With regard to the plaintiff's allegation that the city mayor did not inform the Authority of the possible data breach within the statutory timeframe, the DPA replied the Authority was verifying the controller's actions *ex officio*. According to the DPA, only the controller can be a party to the proceedings concerning the notification of a data breach, and in the plaintiff's individual case there was no legal basis for investigating the allegation raised by the data subject.

- ✓ The above statement seems to contradict the high-profile decision of the Data Protection Authority, in which it imposed an administrative fine on a controller in connection with the controller's failure to report a personal data breach to the Authority and incorrect notification of the breach to data subjects. Unlike the decision at hand, in the above case the Authority initiated administrative proceedings *ex officio*, but the parties to the proceedings were the data subjects whose data were affected by the breach, and who had approached the Authority with a complaint about irregularities in the processing of their personal data.

10. Miscellaneous

Distinction between professional and personal activity

#public person #access #erasure order

September 2022

The Data Protection Authority ordered the erasure of a plaintiff's personal data regarding their first and last names, nickname and bank account number, which had been made available online.

The facts

The plaintiff, who is a public figure, complained about an online disclosure of their data including their nickname and bank account number. The plaintiff provided the data to the defendant to enable a money transfer in connection with a contract for participation in a martial arts gala. The personal data were disclosed on the plaintiff's public profiles to prove that the defendant had paid their dues under the contract. The data were disclosed as a result of a conflict between the parties over the terms and conditions of the contract.

Key findings

- ✓ The Data Protection Authority pointed out that although the defendant had an actual interest in addressing the plaintiff's allegations in the public sphere, there was no legal basis for them to disclose the plaintiff's data.

- ✓ What is noteworthy is the Authority's assessment of professional activities. The Data Protection Authority pointed out that the exemption in Article 2(2)(c) of the GDPR did not apply in this case, since the defendant's publication was posted in the context of their professional activity, and therefore it was not of a purely personal or domestic nature. The basis of the relation between the plaintiff and the defendant was a contract between the former and the entity responsible for the organization of the sports gala. In settling the accounts with the plaintiff, the defendant acted on behalf of the said entity.

- ✓ Also, the defendant's representation indicates that they posted that information in the context of their professional activity (including for the purpose of demonstrating that they

did settle accounts for contracts entered into as part of those activities), so it was not purely personal in nature.

Disclosure of personal data at a municipal council session and their publication

#government #transmission #public sector

September 2022

The Data Protection Authority ordered the mayor of a municipality to remove the plaintiff's personal data including their last name and home address from recordings of the municipal council sessions made available online.

The facts

At a municipal council session, during the presentation of a report on the activities of the committee on complaints, motions and petitions, the chairwoman of the aforementioned committee gave the plaintiff's personal data in the form of their last name and home address in connection with a complaint filed by a third party against the mayor, also concerning the plaintiff.

Subsequently, the data were made public online in connection with the publication of the broadcast and recording of the council session. in addition, the justification for the adopted resolution of the council and the minutes of the commission meeting were posted on the public information bulletin.

The plaintiff was not a public official, nor did they waive their right to privacy.

Key findings

- ✓ The Data Protection Authority did not find legal grounds for making the plaintiff's personal data public when presenting a third-party complaint at a session of the municipal council, the content of which included the plaintiff's personal data, as it was not, in the Authority's opinion, necessary for the consideration of the complaint filed.

- ✓ As the entity responsible for the content published in the information bulletin on the municipality's website, or in any other customary manner, the mayor is obliged, pursuant to Article 5(2) of the Access to Public Information Law, to anonymize the published data so as not to breach the provisions on data protection (Article 6(1) GDPR, Article 5(1)(c) GDPR).

Inadvertent failure to cooperate with the Authority

#controller's responsibilities in the proceedings
#obstruction of proceedings

June 2022

The Data Protection Authority issued a warning for inadvertently failing to cooperate with the Authority and failing to provide access to data and information in the proceedings.

The facts

As a result of a data subject's complaint about irregularities in data processing, the Authority sent questions to the company, demanding that it respond to the complaint and provide explanations. The company did not respond to the correspondence.

In the absence of a response to the summons, the DPA initiated administrative proceedings for the imposition of an administrative fine. The letter initiating the proceedings was effectively served upon the company. The company then replied that the lack of response to previous correspondence was due to the illness of the company's president, the only person authorized to represent the company.

The Authority found that the company's actions clearly breached Articles 31 and 58(1)(a) and (e) of the GDPR, but was unintentional, nonetheless.

Key findings

- ✓ The Data Protection Authority stated that the controller should promptly report any obstacles preventing it from timely compliance with its obligations to the Authority. However, undertaking cooperation with the Authority already in the ongoing proceedings for non-cooperation will be taken into account and may alleviate the remedial measures applied by the DPA.

- ✓ Despite the lack of willfulness in the company's actions, the Authority did not refrain from imposing a warning. At the same time, the DPA emphasized that in the event of a similar occurrence in the future, any warning issued by the DPA

against the company will be taken into account when evaluating the prerequisites for the possible imposition of an administrative penalty.

Proceedings for publication of a student's data

#higher education #thesis

September 2022

The Data Protection Authority ordered a technical university to erase a graduate's personal data regarding their phone number and issued a warning for breaching data provisions by disclosing their data online (in a curriculum management system, USOS) without a legal basis.

The facts

A technical university graduate challenged the content of a form which included mandatory consent to make their thesis available on the university's website. The plaintiff did not consent to the publication of their thesis or personal data. The plaintiff alleged that despite that statement, the university processed and disclosed their personal data. In the course of the investigation, the Data Protection Authority found that the plaintiff's thesis had not been published, unlike the metadata relating to it, including: their first and last names, their rank, the year of the thesis exam. However, the investigation revealed other irregularities in the university's data processing, including the processing of data outside the catalog allowed for the purpose of documenting the course of study (like telephone number), or the fact that there was no basis for making the plaintiff's personal data including their first and last names, their rank and the year of the thesis exam available to an unlimited circle of recipients online.

Key findings

- ✓ The student's phone number was processed in the USOS without a legal basis. As pointed out by the DPA, the scope of that information did not fall within the catalog of data referred to in sections 3 and 4 of the regulation of 14 September 2011 on the documentation of the course of studies.

- ✓ Of particular relevance to all controllers, the Authority highlighted that the scope of proceedings before the DPA may go beyond that originally defined in the complaint and cover other issues related to the processing of personal data.

Order to release IP address for the assertion of claims regarding personal rights

#web service #personal #IP address.

September 2022

The Data Protection Authority ordered a company operating a website to disclose the IP address of the authors of posts for the purpose of asserting personal rights claims.

The facts

The plaintiffs asked the company to disclose the IP address of a user posting under a certain nickname. The plaintiffs pointed out that entries had been posted by one of the users on a website operated by the company, which were untrue and of an offensive and demeaning nature. The plaintiffs explained that the entries in question infringe their personal rights and they intend to file a civil lawsuit to hold the infringing person liable.

The Company explained that it was forced to refuse to comply with the request to release the data of the authors of the posts until it received an appropriate request from the competent authorities, citing Article 18(6) of the Polish Law on the Provision of Electronic Services. The decision was issued based on the provisions of the Polish Law on the Protection of Personal Data of 29 August 1997, but the Authority pointed out that the reasoning remains valid under currently applicable regulations as well.

Key findings

- ✓ In the opinion of the Data Protection Authority, the controller unjustifiably refused to provide the plaintiffs with the requested personal data of the authors of the challenged posts, including the IP number, thus preventing them from taking further action to identify the authors in this manner.

- ✓ The Authority considered the basis for such action to be the necessity of processing the data to fulfil a legitimate interest (Article 6(1)(f) of the GDPR). It also argued that the provisions of the Polish Law on the Provision of Electronic Services, which provide for the necessary disclosure of data to state authorities, do not exclude the same to the user.

Leaving a delivery note in a publicly accessible place

#delivery note #address #indirect identification #warning

March 2022

The Data Protection Authority issued a warning for a public disclosure of the plaintiff's address without a legal basis by leaving a delivery note containing the plaintiff's address in a publicly accessible place.

The facts

An entrepreneur's employee left a delivery note by the intercom in front of a stairwell. The delivery note contained the exact address of the plaintiff (including the apartment number) and the time of the attempted delivery. However, the plaintiff was not the addressee of the delivery, and the delivery note did not contain their name. The address indicated on the delivery note was the delivery address for the plaintiff and other recipients as well.

Key findings

- ✓ The same personal data in terms of address may apply to more than one person. However, each of those persons will be affected independently. Each person is free to provide their address for service. The fact that the same address pertains to more than one person does not deprive such information of the value of one plaintiff's personal data.

- ✓ Despite the fact that no first and last names were given on the delivery note, the mere leaving of the same with an address on it in a publicly accessible place constitutes a breach. The Authority supports this claim by way of reference to life experience which shows that residents of the same staircase know who lives in a particular apartment indicated on the delivery note. That makes allows unauthorized persons to indirectly identify the addressee of the delivery note without excessive effort or cost.

- ✓ The ruling in question can be considered disputable. After all, the Authority found a breach in the present case, where the data were disclosed to the plaintiff's neighbors (who were already in possession of the data) and to third parties, who

could not, in principle, identify the plaintiff without access to other plaintiff's data.

Disclosure of data by a housing cooperative on the intercom box

#housing cooperative #warning #intercom.

June 2022

The Data Protection Authority issued a warning to a housing cooperative for breaching Article 6(1) of the GDPR, in connection with disclosing the plaintiffs' data including their last names on the building's intercom box without a legal basis.

The facts

The cooperative processed the plaintiffs' personal data in connection with their membership in the cooperative, including their last names, which appeared on the intercom box even before the GDPR came into effect.

The plaintiffs did not request the cooperative to remove their last names from the intercom box, nor did they respond to letters addressed to them by the cooperative on the matter. Despite the fact that the plaintiffs' data were removed from the intercom box, the plaintiffs complained to the DPA.

Key findings

- ✓ The Data Protection Authority found that the plaintiffs' personal data in the form of their last names had been disclosed on the intercom's box, as the box could be accessed by members of the cooperative and members of the public.

- ✓ The Authority pointed out that the cooperative had failed to demonstrate the legal basis for the legality (right or obligation) of providing access to the plaintiffs' personal data, including, among other things, failing to obtain their consent to provide the data.

Leaving the initials alone does not always mean that the document has been anonymized

#anonymization #school #unauthorized data disclosure

July 2022

The President of the Office of Data Protection issued a warning to a school complex for the disclosure of personal data contained in the data subject's complaint filed via the electronic diary.

The facts

The teacher sent a complaint to the district council against their employer: the school headmaster. The complaint included information about the teacher's health condition.

The school's headmaster received the anonymized complaint and then made it available in the electronic diary to all members of the teachers' board, disclosing the date it was filed and the teacher's initials, in order to allow the board members to comment on the issues raised in the complaint. As a result, the plaintiff reported a breach of their personal data. Referring to the complaint, the school's headmaster stated that there was no breach, as the document was anonymized and was only shared as part of the teachers' board internal communication, within a secure computer system. The complaint was removed from the electronic diary after the relevant committee of the district council completed its work on the complaint.

Key findings

- ✓ The decision shows that 'anonymizing' a document by leaving only the initials is not always sufficient. The circumstances of the case at hand clearly demonstrate that the persons to whom the complaint was made available could recognize its author, as they knew the plaintiff and knew of the events involving them, as described in the complaint.
- ✓ The Data Protection Authority further highlighted that it was inadequate to disclose the entire complaint to the members of the teachers' board given the purpose, i.e. defending the school against the allegations made. In the DPA's view, it would have been appropriate to disclose only the relevant

parts of the complaint to the teachers affected by the allegations or to those who were witnesses in the case then contemplated.

The importance of granting consent

#university #warning #consent

September 2022

The Data Protection Authority issued a warning for breaching Articles 6(1) and 5(1)(c) of the GDPR in connection with the disclosure of a student's personal data regarding their exam score by an academic to third parties.

The facts

As part of the online exam an academic lecturer conducted via MS Teams in the presence of other students taking the exam, they indicated that the student had failed the exam and needed to retake it.

The disclosure of the results of the plaintiff's exam was preceded by the lecturer's indication that, provided none of the students objected, they would announce the exam results orally for practical reasons. The academy indicated in this regard that the legal basis for the oral communication of the student's exam result in the presence of other students taking the exam was the consent.

The student replied that they had never consented in any form or to any extent to the disclosure of information about their exam score, and consequently complained to the Data Protection Authority.

Key findings

- ✓ The DPA emphasized that a consent must be actively granted by the data subject. Silence, implicitly checking the consent box or failing to take action cannot be considered a clear affirmative action. The procedure for obtaining consent used by the lecturer therefore lacked the 'student's active action' characteristic.

- ✓ In other words, the Authority said that no objection to the proposed method of providing information about the exam results cannot automatically mean that the student consented to sharing their personal data with other students.

Refusal to provide copies of personal data contained in call recordings

#company #order #data copy #information obligation

April 2022

The Data Protection Authority ordered that a company provide a copy of the personal data recorded in the recordings of phone calls made by the plaintiff with the company's employee. In the remaining scope, the DPA refused to grant the request.

The facts

The company obtained personal data directly from a purchaser in connection with the latter's order placed with a third party via a platform operated by the company. The company offers an additional service to protect users of its sales platform, which the purchaser signed up for.

The purchaser requested that the company send a copy of their personal data processed by the company and to send a full information clause about the processing of their personal data in connection with their signing up with the purchaser protection program.

The company provided a copy of the personal data excluding the data contained in the phone call recordings, referring to the duty to protect third-party privacy. At the same time, the company sent three separate documents that contained information on the processing of the plaintiff's personal data. According to the data subject, their request had been fulfilled in breach of the GDPR provisions, which justified their complaint to the Authority.

Key findings

- ✓ The Data Protection Authority challenged the correctness of the company's position, according to which it refused to provide copies of the data recorded in the telephone call recordings to comply with the data protection regulations and the protection of the rights of its hotline operators. According to the Authority, the company did not prove the excessive nature of the plaintiff's request, nor did it prove that the request was 'manifestly unfounded'.

- ✓ The above indicates that controllers processing personal data via hotlines will need to put in place mechanisms to simultaneously provide copies of such data to data subjects and ensure the protection of the hotline operators' personal data.

- ✓ With regard to the assessment of the controller's fulfillment of the information obligation, the Authority argued that the fact that the necessary information was placed in different documents does not preclude that the obligation had been fulfilled in breach of the provisions of the GDPR. In the opinion of the Data Protection Authority, unifying information obligations so that they can refer to the controller's several services at the same time is a manifestation of a concise and transparent form of the fulfillment thereof, and not of their negation. A separate information obligation, on the other hand, should be applied in situations where data processing is clearly different in kind, or is related to the company's similar tasks, such as in relation to data collected during the recruitment of new employees.

- ✓ What is of particular importance is that the DPA pointed out that the plaintiff had not indicated what they did not understand or what they considered unclear information. Therefore, the DPA moved the burden of proof regarding the inadequacy of performance of the obligation under the GDPR regulations to the data subject.

Authors

Anna Kobylańska

advocate, partner

Anna specializes in legal counselling in the field of personal data protection, including legal issues related to the provisions of the EU General Data Protection Regulation. She has many years of experience in advising on the new technologies law, e-commerce and intellectual property protection. She has authored publications on data protection law and protection against trademark infringement online. Lecturer at H. Grotius Center for Intellectual Property, she was acknowledged six times by the *Chambers and Partners: Europe* ranking, in consecutive years from 2012 to 2017, in the Telecommunications, Media, New Technologies – Personal Data category.

Marcin Lewoszewski

legal counsel, partner

Marcin has many years of experience in data protection and the new technologies law. On a daily basis, he provides legal services to clients from various sectors of the economy, especially to those whose business involves new technologies. He teaches postgraduate courses on Information Security Management and Application of Cloud Computing Technology in Business Modeling, organized by the Warsaw School of Economics. Acknowledged by the *Chambers and Partners: Europe* ranking in consecutive years from 2013 to 2017, in the Telecommunications, Media, New Technologies – Personal Data category. Marcin was also among the winners of the 2015 Rising Stars ranking: the most promising lawyers in Poland before the age of 35, organized by the *Dziennik Gazeta Prawna (DGP)*. He is the first Pole to sit the Chair of IAPP KnowledgeNET, the International Association of Privacy Professionals, an association of privacy lawyers. In 2022, he was appointed an expert on new technologies to the European Data Protection Board.

Dr. Arwid Mednis

legal counsel

Arwid area of expertise covers the law of new technologies, including telecommunications law and personal data protection. He also specializes in cyber-security, information protection and access to public information. His experience covers administrative law, particularly local government law and public and private partnership. From 1991 to 2000, he represented Poland in the Committee for the Protection of Personal Data at the Council of Europe in Strasbourg and was its chairperson from 1998 to 2000. Member of the Scientific Council at the former General Inspector for Data Protection, Arwid drafted and co-drafted laws on personal data protection and economic information exchange. He represents clients in regulatory matters and in judicial and administrative proceedings. He works at the Faculty of Law and Administration at the University of Warsaw, where he teaches courses on, among other things, access to public information, personal data protection and electronic communications law. Arwid has authored numerous publications on telecommunications law, personal data protection, e-business and administrative law.

Ewelina Kęciek

advocate

Ewelina specializes with data protection law and regulations governing the e-commerce industry. Her experience involves the implementation of GDPR requirements and data protection compliance audits. She was a member of the Data Protection Officer team. Ewelina participates in inspection and administrative proceedings conducted by the Data Protection Authority and in proceedings before administrative courts. She graduated from postgraduate studies in personal data protection and modern technology law organized by the Kozminski University.

Robert Brodzik

advocate

Robert's area of specialization covers personal data protection and the new technologies law. He graduated from the Faculty of Law and Administration at the University of Warsaw and the School of American Law at the Lehrstuhl für US-amerikanisches Recht at the Faculty of Law of the University of Cologne. He has implemented the requirements of the EU Data Protection Regulation (GDPR) in more than thirty companies from different areas and sectors of economy, including e-commerce, banking, pharmaceuticals, automotive, FMCG and marketing. In a similar capacity, he has conducted more than a dozen audits for compliance with data protection and information security law requirements. He has advised clients on security incidents and data protection breaches, as well as proceedings before the Data Protection Authority. He also negotiated data processing agreements. He has served as a Data Protection Officer and conducted training courses on data protection and information security law. He has authored publications and articles on data protection issues, including co-authoring a commentary on the Personal Data Protection Law.

Mikołaj Ostoja-Ciemny

trainee advocate

He specializes in advising on data protection, privacy and the new technologies law, including IT contracts and telecommunications law. He has participated in numerous proceedings before the Data Protection Authority and administrative courts. His extensive experience covers advising entities in the banking sector and e-commerce industry. He has participated in IT implementations in regulated sectors (including cloud computing) and GDPR implementations. Mikołaj has conducted workshops on copyright law and agile project management and gained professional experience in the digital transformation, the new technologies law and data protection teams at a renowned Polish law firm. He graduated with honors in law from the University of Warsaw and also studied at the University of Lisbon.

Anna Stępień

trainee advocate

She graduated from the Faculty of Law and Administration at the University of Warsaw and completed postgraduate studies at the H. Grotius Center for Intellectual Property Rights. Before joining Kobylańska Lewoszewski Mednis sp. j., she gained experience in the litigation departments of the most prestigious international and Polish law firms. Her litigation experience was also polished when she took part in international moot court competitions and she also provided legal advice at the University of Warsaw Law Clinic. Anna provides comprehensive legal services in the field of administrative, court-administrative, civil, criminal and arbitration proceedings and has performed legal analyses for the largest companies operating on the Polish market from various sectors of the economy, including State Treasury companies and public entities. Regarding civil proceedings, Anna has mainly dealt with tort liability, liability for non-performance or improper performance of a contract and corporate disputes. In the field of criminal proceedings, she deals with business criminal law. Anna has also advised companies on matters related to the COVID-19 pandemic.

Filip Starzec

trainee advocate

Filip is a law graduate from the University of Warsaw. He also completed the one-year course of the Center for American Law organized by the Faculty of Law and Administration of the University of Warsaw in cooperation with Georgia State University College of Law and Emory University School of Law. Prior to joining KLM LAW, Filip gained experience in alternative dispute resolution and pharmaceutical and banking law at Polish and international law firms.

Filip shares his expert knowledge of cyber-security issues and the new technologies law in the area of personal data protection, regulation of professional secrets and the applicability of the blockchain technology. He is one of the co-founders of the Scientific Circle of the New Technologies Law at the University of Warsaw and an honorary member of the Scientific Circle of Mediation, Negotiation and Arbitration.

Małgorzata Giemza

A fifth-year law student at the University of Warsaw and an LL.M. student at the UC Berkeley School of Law with a specialization in Law & Technology. Małgorzata also studied at Nova School of Law in Lisbon. She has built her experience in corporate law and M&A transactions and was also active in counselling at the University of Warsaw Law Clinic, providing pro bono legal help to victims of violence and discrimination. Małgorzata is a member of numerous scientific circles and student organizations dealing with, among others, the new technologies law, art and law, and the practical application of law.

Izabela Sienicka

A fifth-year law student at the University of Warsaw, Izabela gained her first professional experience as an intern at a law firm, where she addressed issues relating to personal data protection. Her interests include the new technologies law, criminal law and data protection law.

Contact details

Anna Kobylańska

advocate

e: anna.kobylanska@klmlaw.pl

m: +48 (0) 515 975 705

Marcin Lewoszewski

legal counsel

e: marcin.lewoszewski@klmlaw.pl

m: +48 (0) 604 817 352

Dr. Arwid Mednis

legal counsel

e: arwid.mednis@klmlaw.pl

m: +48 (0) 510 087 786