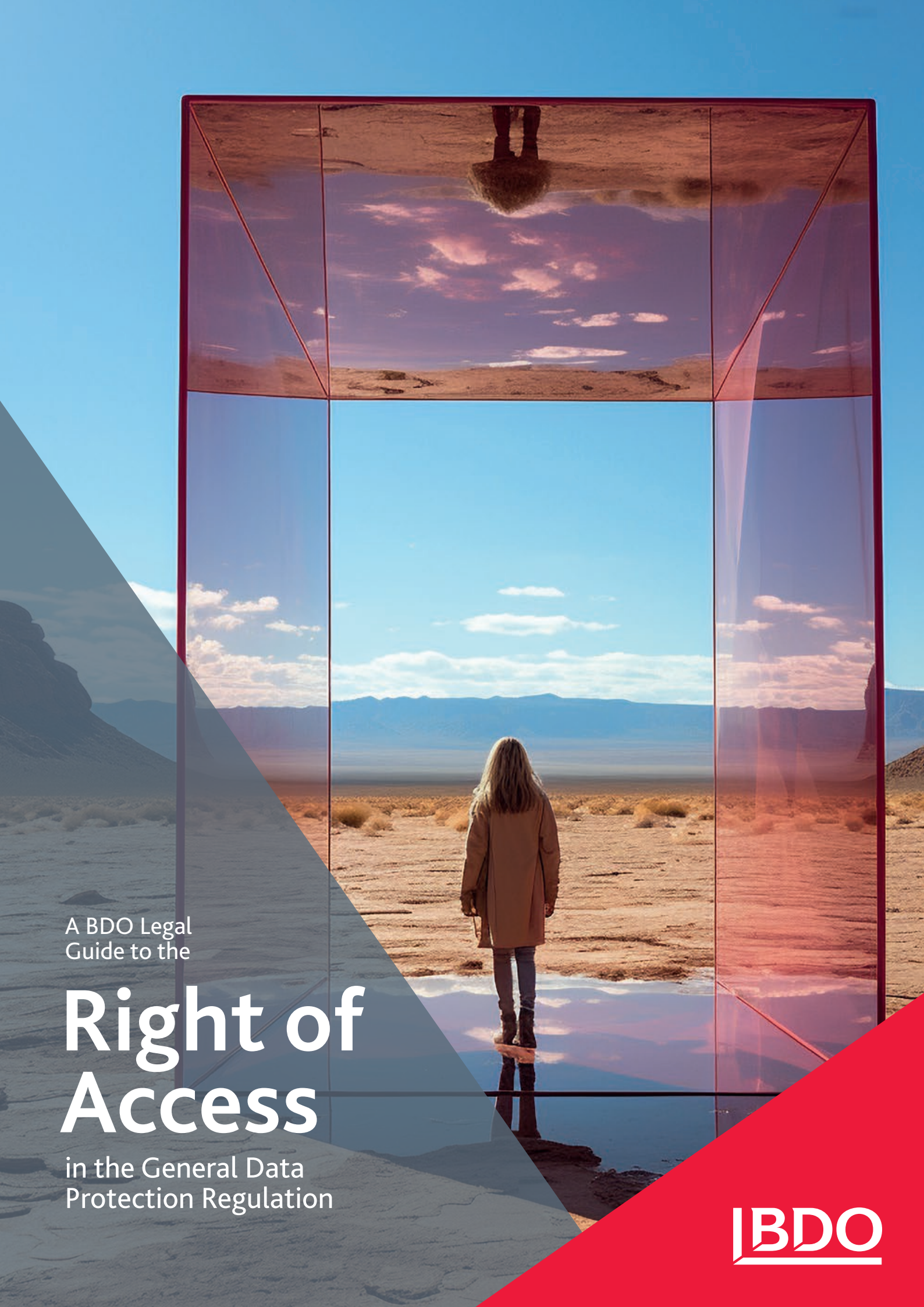


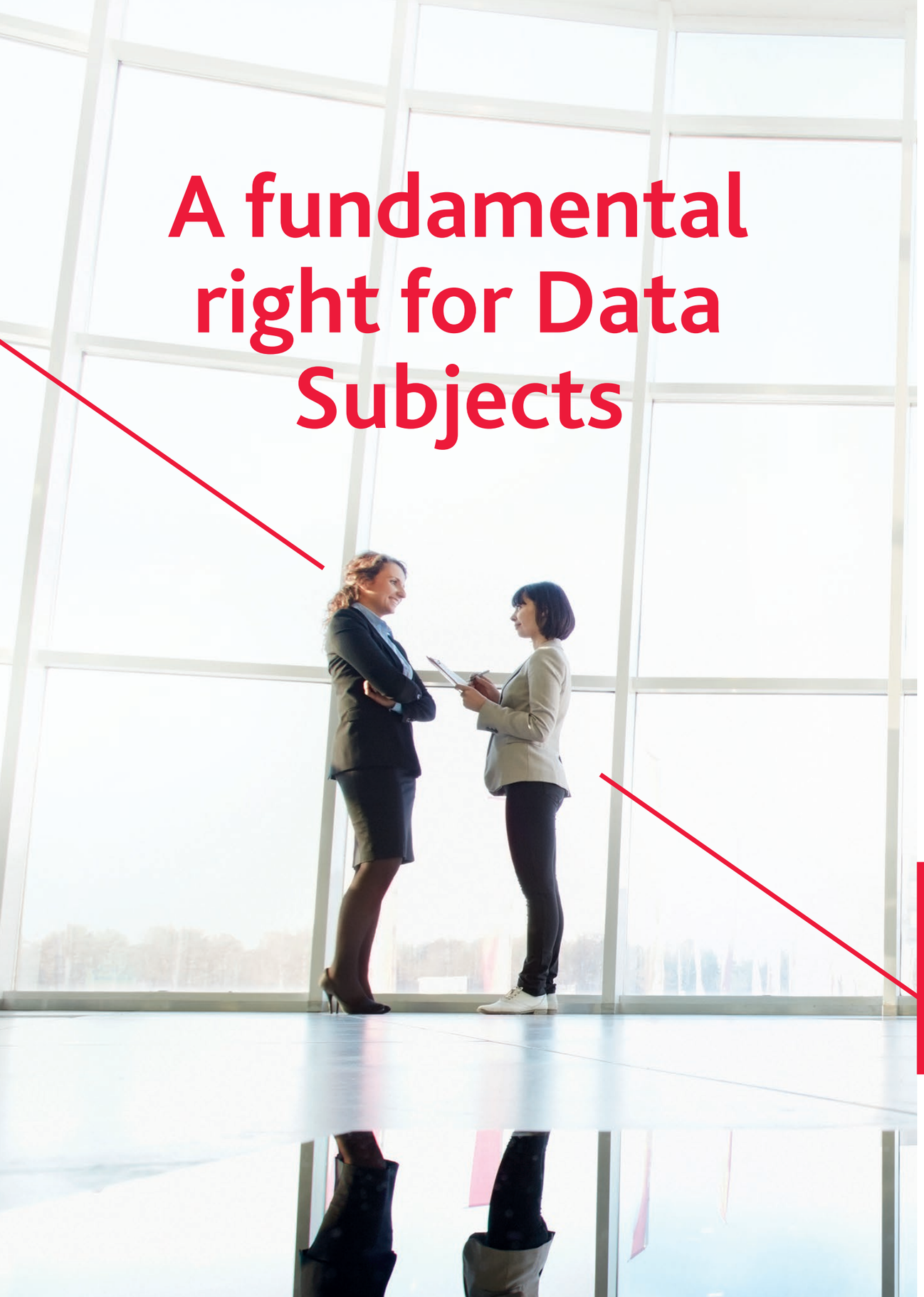
A BDO Legal Guide to the

Right of Access

in the General Data Protection Regulation

BDO

A fundamental right for Data Subjects



Understanding the Right of Access and your responsibilities under the GDPR

The General Data Protection Regulation (GDPR) establishes the Right of Access as a fundamental right for Data Subjects, allowing individuals to request access to their personal data and gain insight into its processing. For companies acting as Data Controllers, this represents a legal obligation to handle such requests efficiently, transparently, and in full compliance with GDPR principles.

For companies acting as Data Controllers, this represents a legal obligation.

WHAT CONSTITUTES PERSONAL DATA?

Under the GDPR, personal data is broadly defined as any information that identifies or can identify an individual. Anonymised data falls outside the scope of the GDPR and is not subject to Right of Access requests.

Your obligations under the Right of Access

When a Data Subject exercises their Right of Access, your company must provide:

1. Confirmation of data processing: You must confirm whether you process the individual's personal data.
2. Access to the data: A copy of all personal data related to the individual must be provided.
3. Details of processing: You are required to supply detailed information about the processing, including:
   - The purposes of processing.
   - The categories of personal data.
   - The recipients.
   - The retention period.
   - The Data Subject's rights.
   - Any safeguards in place for international data transfers.
   - The existence of automated decision-making.

How to handle Right of Access requests

To comply with the GDPR, companies should follow these steps:

1. **Receiving** the request.
2. **Verifying the identity** of the Data Subject.
3. **Processing** the request.
4. **Providing the response**: Include confirmation, data copy, and processing details in clear language.

Timelines and costs

You are required to respond to Right of Access requests within **one month** of receiving them. For **complex cases**, an extension of **two months is possible**, with notice.

First copy is free; additional copies may incur a fee.

Limitations and exceptions

- **Impact on others' rights**: Disclosing information would affect others' rights.
- **Trade secrets**: If the data includes proprietary business information, you may limit access, provided this does not obstruct the Data Subject's rights.
- **Legal exceptions**: Certain types of data processing, such as for journalistic, scientific, or historical purposes, may be exempt from full disclosure under the GDPR.

Ensuring secure data delivery

Use appropriate security measures (e.g., encrypted emails or secure portals). Document the process to demonstrate compliance.

Establishing best practices

To effectively manage Right of Access requests under the GDPR, your company should:

- Develop clear policies.
- Train staff.
- Maintain records of request/responses.
- Use systems that support data retrieval and security.

In summary

The Right of Access is a cornerstone of the GDPR, and fulfilling this obligation helps build trust. By demonstrating a commitment to data protection through establishing robust processes and seeking expert guidance where needed, you can fulfil your responsibilities effectively and turn compliance into a competitive advantage.

The remainder of this guide provides an overview of real examples of Right of Access cases in some key European jurisdictions. We would encourage you to reach out to our subject experts should you require any assistance in managing Right of Access requests, or indeed improving your data protection practices.

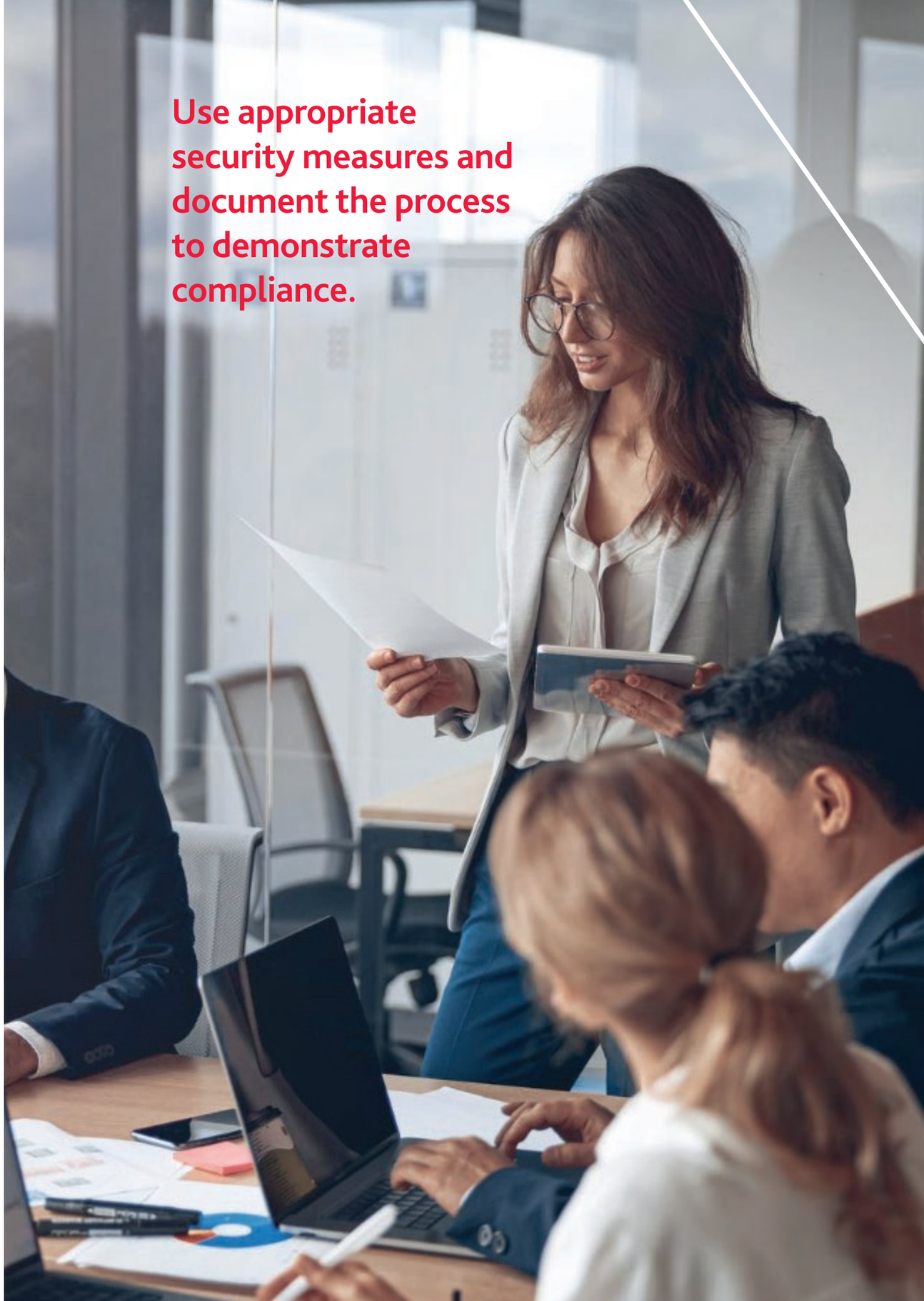
Together, we can ensure your company remains compliant in a data-driven world.

How we can assist your company

Our legal consultancy specialises in helping companies navigate the complexities of GDPR compliance. We offer support with:

- Reviewing your existing data protection policies and procedures.
- Providing training for staff on handling access requests.
- Assisting with complex or disputed requests.
- Offering practical advice to balance compliance with operational efficiency.

If you need assistance in managing Right of Access requests or improving your data protection practices, contact us today.



Belgium

Take care to verify if any personal data you obtain from a third party is legally collected.

Exercise sufficient care in verifying the identity of the requesting Data Subject.

Case One

Specific matter of Right of Access the case pertains to

Manner of communication of requested data to Data Subject.

Summary of the facts of the case

The Respondent insisted on providing the Data Subjects requested data by post although the request was made electronically, claiming that it would provide more guaranties as to the information reaching the correct Data Subject. The Respondent did not verify the identity of the Data Subjects exercising their right to access. The company also only provided categories of recipients of the personal data, although it could identify specific recipients.

Decision of the authority / court, mentioning fines

Reference: Decision 07/2024 of 16 January 2024 by the Belgian DPA.

The DPA found that the Respondent violated Article 12.3 of the GDPR by sending responses to access requests by post, even though the original requests were sent electronically. The DPA emphasises that the Respondent should facilitate the exercise of Data Subject rights and should use secure electronic means to provide information, as required by Article 12.2 and Article 15.3 of the GDPR. The Respondent's reasons for sending responses by post were not convincing. The DPA also found that the Respondent did not act with sufficient care by not verifying the identity of the requesting Data Subject. Also, the form used to exercise the right to access already contained sufficient information to check whether the email address aligned with the contact information of the Data Subject in Respondent's database.

As a result, the Respondent was found to have violated Article 12.1, Article 12.2, Article 12.3 and Article 15.3 of the GDPR, resulting in fine of EUR 41,440 specifically for breach of Articles 12 and 15 of the GDPR. In total, including breach of other articles of the GDPR, the Respondent was fined EUR 174,640 in total.

Take away / action point

Pay attention to the manner in which a response to a right to access is provided, taking into account Article 12.3 of the GDPR.

Exercise sufficient care in verifying the identity of the requesting Data Subject.

Case Two

Specific matter of Right of Access the case pertains to

Lack of timely and complete response to a request regarding the origin of the personal data processed by Respondent.

Summary of the facts of the case

The Respondent sent direct marketing to the Data Subject, using data obtained through a third party. The Data Subject, not having any previous relationship with the Respondent, requested information, based on Article 15 of the GDPR as to the origin of his personal data used to contact him. The Respondent did not answer this request as it thought that it had obtained said information legally from the third party. The Respondent only provided the necessary information when the case was brought before the national authority.

Decision of the authority / court, mentioning fines

The Respondent confirmed that it had not responded in time to the request by the Data Subject, which constitutes a violation of Article 15 of the GDPR because, even if Respondent chose not to respond to the request, it should have notified the Data Subject about its decision not to respond to the request and inform the Data Subject of the possibility to file a complaint with the national authority. The fact that the Data Subject made the request in vain twice was considered an aggravating factor, whereas the facts that the Respondent removed the data of the Data Subject from its database and that it answered the request, although too late, were considered mitigating factors.
The Respondent was fined EUR 10,000 for not respecting transparency obligations and not having treated requests for access, restriction and erasure.

Take away / action point

Take care to verify if any personal data you obtain from a third party is legally collected. Respond to a request for access, even if you do not want to provide any data, by indicating that you received the request and will not provide an answer, and that the Data Subject can lodge a complaint with the authority.

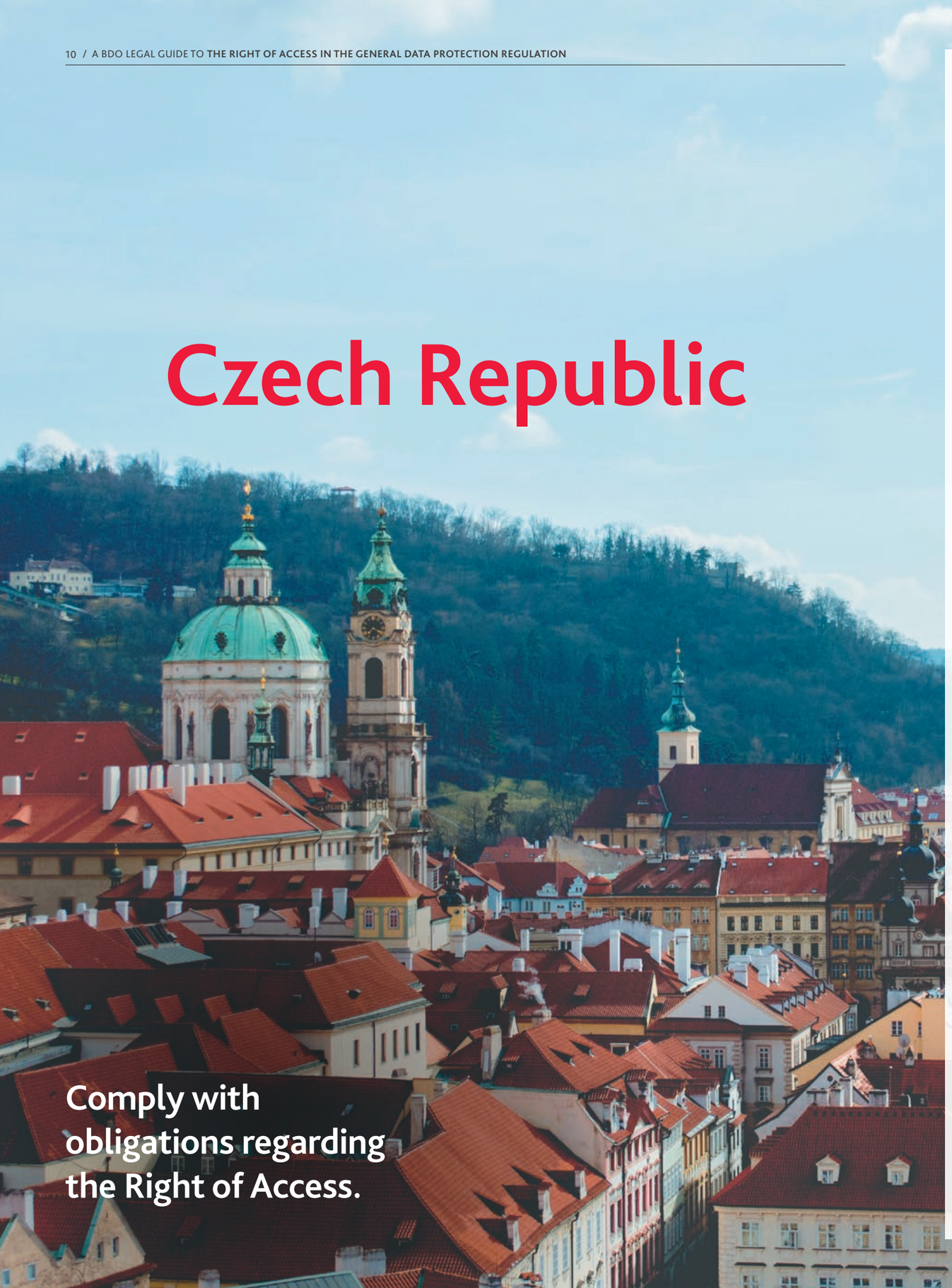
The Respondent sent direct marketing to the Data Subject, using data obtained through a third party.

For further information:

KAREN KEULEERS
BDO Legal | Belgium

karen.keuleers@bdo.be

Czech Republic



Case One

Specific matter of Right of Access the case pertains to

Incorrect email address given by Data Subject.

Summary of the facts of the case

A client collected an email address from a Data Subject, without ever checking whether the email address belonged to the Data Subject. In reality, the address belonged to a different individual and was given by the Data Subject erroneously. Commercial communications were sent to the wrong email address. The individual exercised Right of Access by post, however the client declined altogether (ignored the request), believing that no personal data of said individual is being processed.

Decision of the authority / court, mentioning fines

The Personal Data Protection Office found the client guilty on two counts, 1) ignoring the request for Right of Access, and 2) sending commercial communications to an "illegally" obtained email address, with marginal fines. We have taken over thereafter and appealed the decision in the 2nd count, pending a hearing. On the other hand, the fine for the 1st offence is obviously justified.

Take away / action point

Introduce processes to check validity of email addresses upon collection/before sending out commercial communications.

Comply with obligations regarding the Right of Access even if you believe that no data is being processed, and procure to clarify request if necessary.

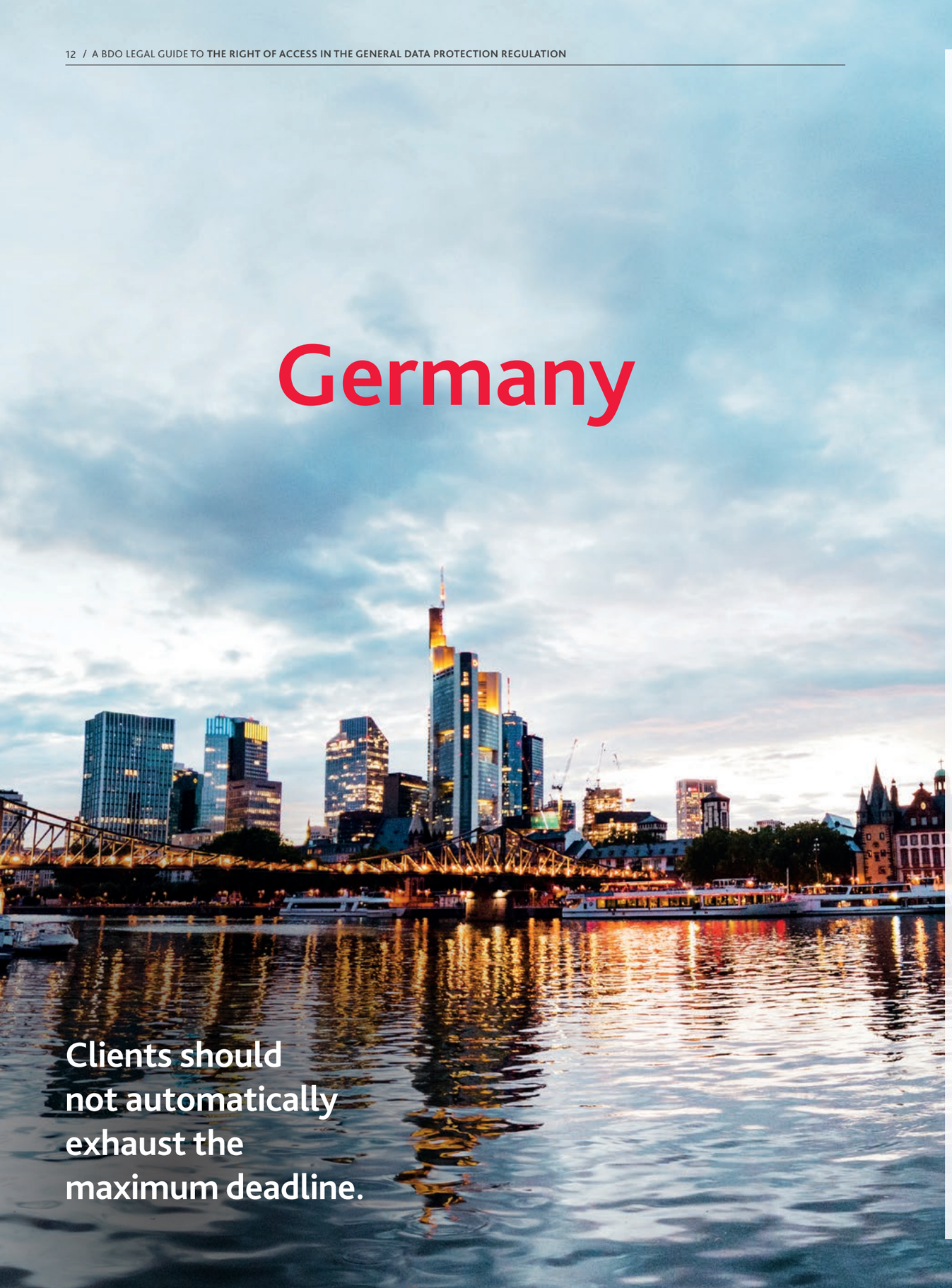
A client collected an email address from a Data Subject, without ever checking whether the email address belonged to the Data Subject.

For further information:

JIŘÍ ŠMATLÁK
BDO Legal | Czech Republic

jiri.smatlak@bdolegal.cz

Germany



Clients should not automatically exhaust the maximum deadline.

Case One

Specific matter of Right of Access the case pertains to

Provision of data without undue delay.

Summary of the facts of the case

The Data Subject applied for a position at the Defendant's company on 14 March 2017. On 18 May 2023, he requested information under Article 15 of the GDPR and set a response deadline for 2 June 2023. The Defendant did not respond until 5 June 2023, providing a negative response that claimed no data was stored about the Data Subject. Following this, the Data Subject requested compensation of EUR 1,000 for the alleged violation of his rights under Article 12 of the GDPR.

Decision of the authority / court, mentioning fines

Reference: Decision 5 Ca 877/23 of 3 November 2023 by the Duisburg Labour Court.

On 3 November 2023, the Duisburg Labour Court ruled that the Defendant must pay the Data Subject a compensation of EUR 750 plus interest. The court found that the Defendant violated Article 12.3 of the GDPR by not responding promptly. The law clearly states the duty to respond without undue delay. Although Article 12.3 sets a maximum deadline of one month, the Data Controller is still obliged to take action as soon as possible. The maximum period may not be used routinely, but only in more difficult cases. Since "without undue delay" does not mean "immediately", nor does it imply a rigid time limit, it depends on a reasonable consideration of the interests of both parties. After a period of more than one week, however, there is generally no longer any immediacy without the existence of special circumstances. In this case, there were no special circumstances that justified the longer response time beyond the set deadline. The court deemed the compensation sufficient and appropriate, considering the Defendant's first-time violation and the potential deterrent effect of the ruling.

Take away / action point

Clients should not automatically exhaust the maximum deadline. It is crucial to ensure that the internal processes for managing access requests are efficient and timely to prevent violations and minimise potential damages.

Clients should not automatically exhaust the maximum deadline.

Case Two

Specific matter of Right of Access the case pertains to

Potential refusal based on the argument of disproportionate effort.

Summary of the facts of the case

The Data Subject requested access to all stored information about him from the tax authority under Article 15 of the GDPR. The tax authority provided several summaries (basic data, assessment data, e-data) in response to the request. However, the Data Subject's representative asserted that not all documents required under Article 15 were provided. The tax authority interpreted this as a request for comprehensive file inspection, which was approved. Subsequently, the Data Subject filed a lawsuit to pursue his request for information under Article 15.1, as well as for the provision of copies of his personal data under Article 15.3. During the proceedings, the tax authority sent various overviews to the Data Subject but refused to provide all files. The Data Subject requested all stored information regarding his person, which the tax authority deemed excessive.

Decision of the authority / court, mentioning fines

Reference: Decision IX R 25/22 of 14 January 2025 by the Federal Finance Court.

The court ruled in favour of the Data Subject, determining that the tax authority was not justified in refusing comprehensive information based on the argument of disproportionate effort. The court emphasised that the Right of Access under the GDPR is of high importance and that authorities must provide the requested information unless there are compelling reasons to withhold it. The court clarified that the tax authority cannot deny access simply because complying with the request would entail considerable effort. The decision also noted that no specific fines were imposed, but the tax authority was ordered to fulfil its obligation to provide the requested information.

Take away / action point

Clients should be aware of the significance of the Right of Access, which is broad and should not be limited without valid reasons. The argument of disproportionate effort cannot be classified as a valid reason.

Case Three

Specific matter of Right of Access the case pertains to

Scope of the Right of Access.

Summary of the facts of the case

The Data Subject is privately insured for health and care insurance and considers multiple contribution increases to be unlawful. She requested information on the amount of contribution adjustments and the corresponding information from the insurance policies and amendments for the years 2012 to 2020. The request included any suitable documents that included information on the amount of the premium adjustments, including naming the respective tariffs in the insurance relationship, the information provided to the plaintiff for this purpose in the form of insurance certificates and supplements to the insurance policy.

Decision of the authority/court, mentioning fines

Reference: Decision VI ZR 62/23 of 6 February 2024 by the German Federal Court.

The term "copy" in Article 15.3 of the GDPR does not refer to a document as such, but to the personal data it contains. The copy must therefore contain all personal data that is the subject of the processing. However, the reproduction of extracts from documents, entire documents or extracts from databases is only necessary in case the information is needed to comprehend the data. The documents need to be essential for ensuring the effective exercise of the rights of the Data Subject.

No specific fines were imposed, as the decision focused on the Right of Access.

Take away / action point

Although clients should ensure that they have the necessary processes and documentation in place to meet the requirements of access requests, this does not obligate the Data Controller to archive any documents but only provide access to the existing personal data.

Documents need to be essential for ensuring the effective exercise of the rights of the Data Subject.

For further information:

MATTHIAS NIEBUHR
BDO Legal | Germany

matthias.niebuhr@bdo.ge

Hungary

It is necessary to handle requests from Data Subjects taking into account the criteria set out in the GDPR.

Case One

Specific matter of Right of Access the case pertains to

Infringement of the Right of Access and restriction of processing.

Summary of the facts of the case

The Data Subject requested to a financial institution the restriction of data processing in the case of the camera recordings processed of them, and the blocking of the recordings. They also requested to see the original of certain audio recordings, camera recordings and minutes. The Data Subject also requested the deletion of their personal data where this was based on their consent.

Decision of the authority / court, mentioning fines

The Authority found that in some cases the financial institution violated the Applicant's Right of Access: it did not provide copies of the camera recordings with the third parties and certain information redacted, did not indicate the exact legal references for which it was processing their personal data, did not inform them about the processing of their personal data in the case of certain records and did not respond within a time limit of one month after receiving their requests. The financial institution thus infringed Articles 12.1, 13.2.a and 15.3 of the GDPR for which the Authority imposed a fine of approximately EUR 2,000.

Take away / action point

The Data Controller must have a clear internal procedural mechanism and accountability rules for handling Data Subject requests.

It is necessary to handle requests from Data Subjects taking into account the criteria set out in the GDPR.

Case Two

Specific matter of Right of Access the case pertains to

Infringement of the Right of Access and restriction of processing.

Summary of the facts of the case

The Applicant requested access to copies of three recorded telephone conversations, which the Data Controller ignored. According to the Respondent, the audio recordings were made for internal training purposes only, and therefore are not uniquely identified and cannot be retrieved. During the course of the case, they were able to identify the audio recordings, but it was not proven that they were available to the Applicant even after one year.

Decision of the authority / court, mentioning fines

The Authority did not consider the information provided to the callers to be adequate and therefore the consent was not lawful. The Respondent thus infringed Articles 12.1, 13.2.a and 15.3 of the GDPR for which the Authority imposed a fine of approximately EUR 13,000.

Take away / action point

The Data Controller must provide appropriate information to Data Subjects in accordance with Articles 13 and 14 of the GDPR.

For further information:

MARK SZUCS
BDO Legal | Hungary
mark.szucs@bdo.hu

Italy

Constantly check whether access requests are received.

Case One

Specific matter of Right of Access the case pertains to

Method of communication of access request by Data Subjects.

Summary of the facts of the case

The Respondent did not reply to an access request, claiming that the email address used by the Applicant to send the request, although it belonged to the same entity, was incorrect because it was used only for sending communications. The Respondent receives email communications through a different public address.

Decision of the authority / court, mentioning fines

Reference: Decision no. 218 of 17 May 2023 by the Italian DPA.

The DPA pointed out that according to Recital 63 of the GDPR, the Data Subject's Right of Access should be easily exercised. Accordingly, the Guidelines on the Right of Access No. 01/2022, adopted by the European Data Protection Board (EDPB) on 18 January 2022 at point 52, also specify that Data Subjects are not burdened with the obligation to adopt a certain format for submitting petitions to exercise their rights and that, in principle, there are no conditions that the data subject is required to comply with when choosing a communication channel through which to get in touch with the Data Controller.

In addition, the DPA stated that regardless of the manner in which the Respondent uses the PEC address (*posta elettronica certificata*), it is still established that the same is actually associated with the Respondent and it does not appear that the same has set up a specific communication channel to facilitate the exercise of rights by Data Subjects.

As a result, the DPA admonished the Respondent for failing to respond to the application and ordered them to provide feedback to the claimant's request for access.

Take away / action point

Constantly check whether access requests are received on all communication channels associated with the company, and especially public ones such as PECs. Acknowledge all access requests that are received through these channels, even if they are not the ones indicated as the main ones for sending such requests.

The Respondent had not replied to an access request, claiming that the email address used by the Applicant was incorrect.

Case Two

Specific matter of Right of Access the case pertains to

Multiple requests of access, difference between the access to data or access to the relevant documentation.

Summary of the facts of the case

The Data Controller, in arguing the reasons for the disputed failure to respond to the access request, pointed out that the Data Subject submitted a series of communications, concerning the same request for access to documentation. Specifically, the Data Controller claimed that it had failed to respond based on Article 12.5 of the GDPR which provides that "if the Data Subject's requests are manifestly unfounded or excessive, in particular because of their repetitive nature, the Data Controller may: [...] b) refuse to comply with the request."

Decision of the authority / court, mentioning fines

Reference: Decision no. 179 of 13 April 2023 by the Italian DPA.

The DPA held that the hypothesis envisaged by Article 12.5 of the GDPR cannot be considered applicable considering that the reiteration of the requests by the Data Subject pertains to the different legal institution of access to administrative documentation as they were submitted, by the Data Subject, under Law 241 of 1990, where the relevant request and two reminders, were being advanced by the Data Subject under Article 15 of the GDPR, for the first time.

The Supervisor finds that the Respondent's conduct constitutes a minor violation and, taking into account the Respondent's uncensorhip, admonishes the same without imposing sanctions.

The DPA clarified how the institution of access to personal data, provided for in Article 15, is substantiated by receiving "a copy of the personal data undergoing processing" and not, necessarily, a copy of the documents in which such data are contained (which instead constitutes access to documentation under Law No. 241/1990), noting how in the same sense the EDPB has expressed itself in points 150 and 152 of the Guidelines.

Take away / action point

Take into account the subject matter of the access request by qualifying it as an access request under the GDPR only if it concerns personal data that is being processed. Bear in mind that requests for documentation related to processing do not fall under the scope of the abovementioned provision.

Case Three

Specific matter of Right of Access the case pertains to

Denial of response to an access request due to waiting for a clarification from third parties.

Summary of the facts of the case

The Respondent stated that it did not respond to the data access request submitted by the complainant because of the need to await clarification from an Italian municipality in order to avoid providing a misleading communication.

Decision of the authority / court, mentioning fines

Reference: Decision no. 225 of 1 June 2023 by the Italian DPA.

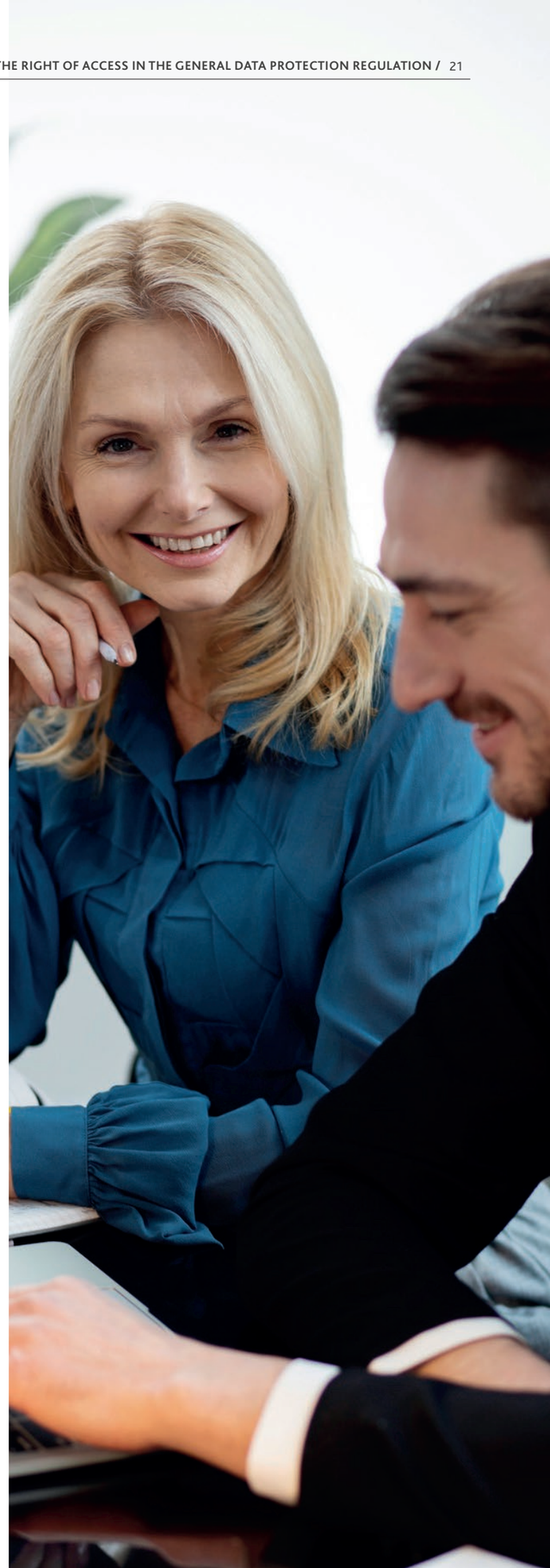
The DPA notes how Article 12.3 of the GDPR stipulates that the Data Controller must respond - even if negatively - to the Data Subject's request without undue delay and, in any case, no later than one month after receipt of the request. Where it fails to comply with the Data Subject's request, it must, in any event, inform the Data Subject without undue delay, and at the latest within one month of receipt of the request, of the reasons for non-compliance and of the possibility of lodging a complaint with a supervisory authority and seeking judicial redress.

The DPA notes how this did not happen in this case, declaring such behaviour unlawful, and admonishing the Respondent without imposing sanctions.

Take away / action point

Take into account the subject matter of the access request by qualifying it as an access request under the GDPR only if it concerns personal data that is being processed. Bear in mind that requests for documentation related to processing do not fall under the scope of the abovementioned provision.

Take into account the subject matter of the access request.

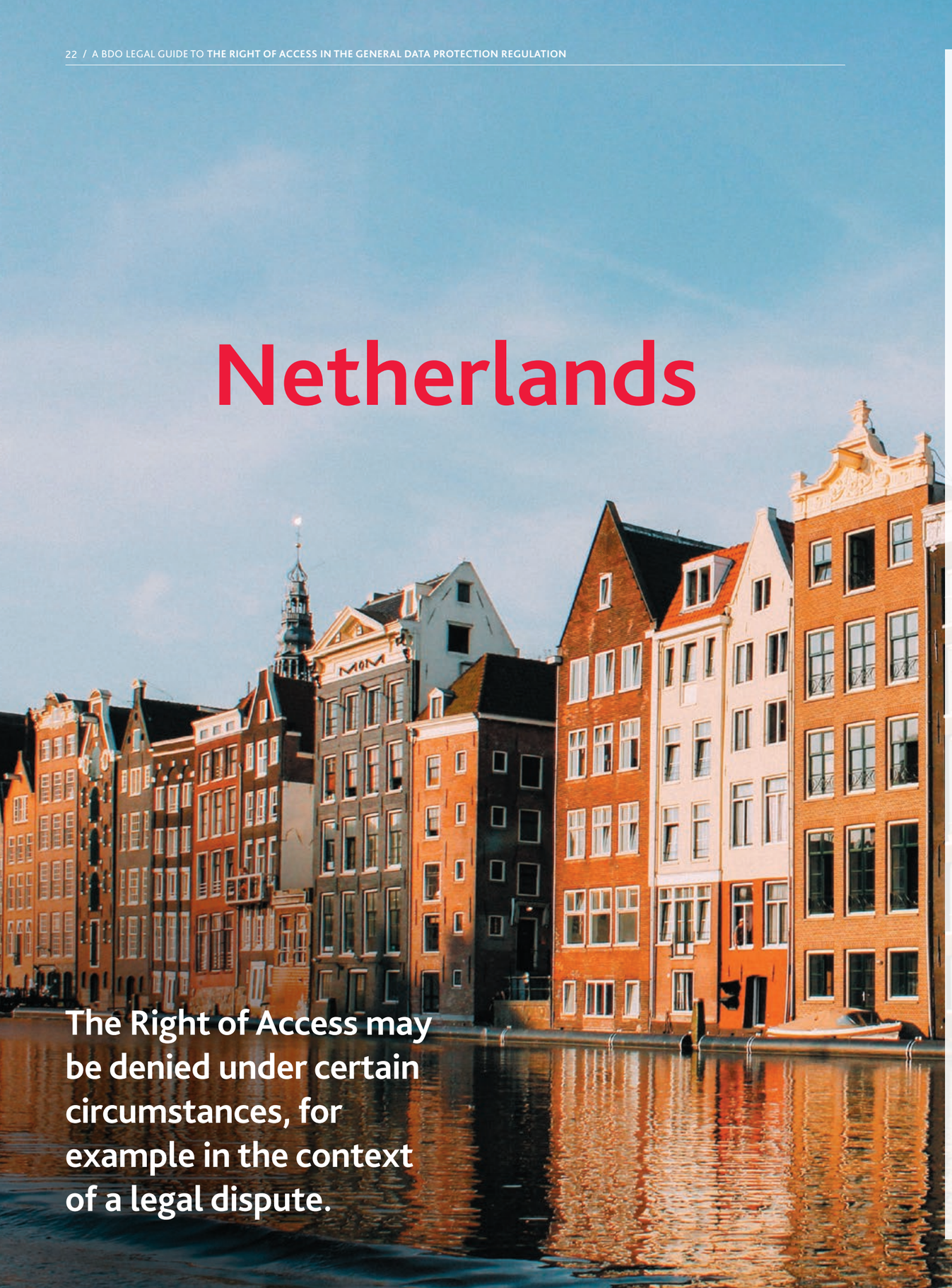


For further information:

GABRIELE FERRANTE
BDO Legal | Italy
gabriele.ferrante@bdo.it

ROBERTO CAMILLI
BDO Legal | Italy
roberto.camilli@bdo.it

Netherlands



The Right of Access may be denied under certain circumstances, for example in the context of a legal dispute.

Case One

Specific matter of Right of Access the case pertains to

Companies may provide an overview of personal data instead of a copies of documents containing those data.

Summary of the facts of the case

The Respondent had not replied to an access request claiming that the email address used by the Applicant to send the access request, although belonging to the same, was incorrect because it was used only for sending communications, while the public address through which the Respondent receives email communications is another.

Decision of the authority / court, mentioning fines

The court ruled that the claimant had not provided sufficient evidence that the chief of police did not give a faithful and understandable reproduction of his personal data in the overview. In addition, the claimant had not provided sufficient evidence that complete copies were indispensable to exercise his rights under the GDPR.

Take away / action point

The obligation to provide a copy of the personal data does not mean that an company is obliged to always provide copies of the documents containing that personal data. The company can also choose another form in which to provide the copy of personal data, as long as it is a faithful and understandable reproduction of all this personal data.

Case Two

Specific matter of Right of Access the case pertains to

The Right of Access may be limited or denied for certain information.

Summary of the facts of the case

This case concerns a conclusion of the Advocate General at the Supreme Court of the Netherlands.

The Applicant worked as a court lawyer at the North Holland court. She left the job after a labour dispute. In order to find out if her colleagues had spoken negatively about her, she submitted a request for access to her personal data to the Council for the Judiciary. The request for access was only denied to the extent that it related to a request for advice from the North Holland court to the Council for the Judiciary in connection with the labour dispute and the Council's advice.

The court lawyer then submitted a subsequent request which was rejected. This was followed by appeal.

Decision of the authority / court, mentioning fines

The Advocate General considers, among other things, that the North Holland court and the Council for the Judiciary have a justified interest in refusing access to the request for advice and the advice.

The fact that these documents contain a subjective interpretation of the labour dispute is inherent in a position determination in the context of a legal dispute, and justifies why these documents can be excluded from access and not, as the Applicant seems to argue, a reason to provide access to them because those evaluations relate to her.

Take away / action point

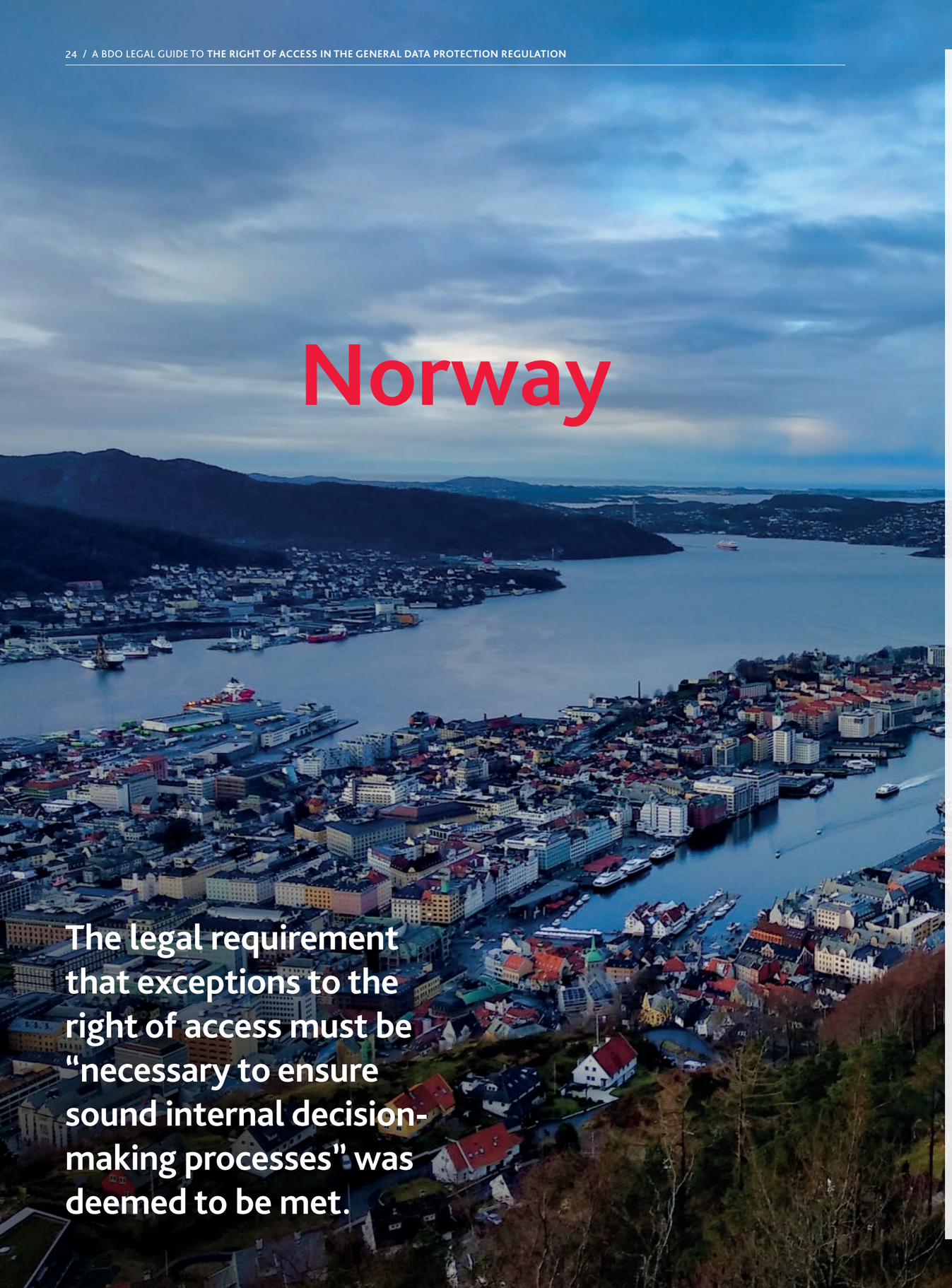
The Right of Access may be denied under certain circumstances, for example in the context of a legal dispute.

For further information:

FEMKE SCHEMKES
BDO Legal | Netherlands

femke.schemkes@bdo.nl

Norway



Case One

Specific matter of Right of Access the case pertains to

Request for access to internal documents, as well as questions about the valid legal basis for processing personal data in an employee case.

Summary of the facts of the case

The case concerns a complaint from an Applicant regarding the Norwegian Data Protection Authority's decision, where the authority concluded that the employer had not violated the Norwegian Personal Data Act. After a personnel case in which a termination agreement was reached, a dispute arose between the parties regarding access to the Applicant's personnel file. The Applicant was granted partial access to the personnel file but was denied access to an internal memo prepared by the employer in connection with the employee case. The Norwegian Data Protection Appeals Board assumed that the request for access concerned information contained in documents prepared for internal case preparation and not disclosed to others. The legal requirement that exceptions to the Right of Access must be "necessary to ensure sound internal decision-making processes" was deemed to be met.

Decision of the authority / court, mentioning fines

Reference: Decision PVN-2023-12 of 12 May 2023 by The Norwegian Data Protection Appeals Board.

The appeal board agreed with the Data Protection Authority that the Norwegian Personal Data Act did not provide the right to further access, under Article 15 of the GDPR in conjunction with the Norwegian Personal Data Act § 16, first paragraph, letter e. The appeal board also agreed with the authority that the employer had a legal basis for using the private emails in the employee case under Article 6.1.c of the GDPR in conjunction with subsection 3, with supplementary legal grounds in the Norwegian Working Environment Act § 2-2. The Data Protection Authority's decision was upheld.

Take away / action point

- Limited Right to Access Internal Documents: Employees may not have the right to access all documents related to them, especially those prepared for internal decision-making processes. The right to access can be legally restricted if it is necessary to ensure sound internal decision-making.
- Legal Basis for Processing Personal Data: Employers must have a valid legal basis for processing personal data in employment-related matters. In this case, the employer was found to have a legitimate basis under Article 6.1.c of the GDPR and the Norwegian Working Environment Act.
- Confidentiality of Internal Memos: Internal memos or documents prepared by the employer that are not shared with third parties can be protected from disclosure. This reinforces the employer's ability to maintain confidentiality in sensitive personnel matters.
- Upholding of Data Protection Authority Decisions: The Privacy Appeals Board upheld the Data Protection Authority's decision, indicating that the authority's interpretation of data protection laws is robust and likely to be supported in appeals.
- Importance of Proper Documentation: Employers should ensure that their documentation, especially in personnel cases, is thorough and complies with legal standards, as these documents may be subject to scrutiny in disputes.

For further information:

ELISABETH ASPAAS RUNSJØ
BDO Legal | Norway
elisabeth.aspaas.runsjo@bdo.no

Romania

The Data Controller should respond to the Data Subject's request.

The Data Controller should adopt appropriate measures for facilitating the exercise of Data Subjects' rights.

Case One

Specific matter of Right of Access the case pertains to

The personal data that the Data Controller must provide to comply with the Data Subject's request to exercise their Right of Access.

Summary of the facts of the case

The investigation commenced following a complaint that reported the Data Controller's refusal to fully comply with the Data Subject's request to exercise their Right of Access, and the omission of providing certain information to them, particularly a video recording concerning the Data Subject.

Decision of the authority / court, mentioning fines

Reference: Decision of the Romanian DPA of 11 May 2023.

The DPA found that the Data Controller did not provide a full answer to the Data Subject's request to exercise their Right of Access, thus violating the provisions of Article 15.1 and 15.2 of the GDPR. Specifically, the Data Controller did not provide a copy of all the personal data processed concerning the Data Subject. Additionally, the Data Controller did not send the response to the postal address specified in the contract, as requested by the Data Subject, as such violating Article 15.3 of the GDPR.

Furthermore, the DPA concluded that the provisions of Article 12.4 corroborated with Article 15.3 of the GDPR were violated because the response sent to the Data Subject via email did not include information regarding the possibility of filing a complaint with the supervisory authority and pursuing a judicial remedy for the refusal to provide a copy of the requested video recording.

The DPA observed that the Data Controller did not provide evidence showing that it had implemented measures to facilitate the exercise of the Data Subjects' Right of Access to copies of video recordings concerning them, an aspect that affected how the Data Subject's request to the DPA was addressed. Concerning this aspect, the DPA found that the Respondent did not comply with the provisions of Articles 12.2, 15.3 and 15.4 of the GDPR.

Consequently, the Data Controller was sanctioned with a fine of RON 4,940 (equivalent to EUR 1,000) for violating Articles 12.4 and 15.3 of the GDPR, and a fine of RON 49,405 (equivalent to EUR 10,000) for violating Article 12.2 corroborated with Article 15.3 and 15.4 of the GDPR.

Additionally, the DPA imposed corrective measures.

Take away / action point

- The Data Controller should respond to the Data Subject's request by providing all the information stipulated in Article 15.1 and 15.2 of the GDPR and a copy of the personal data as specified in Article 15.3 of the GDPR, adapted to the specific situation of the petitioner, in the format requested by them, by post to the correspondence address they provided;
- The Data Controller should adopt appropriate measures for facilitating the exercise of Data Subjects' rights, particularly the Right of Access to a copy of their personal data that are being processed, including through the use of software that allows for the editing of information that could infringe upon the rights and freedoms of others.

Case Two

Specific matter of Right of Access the case pertains to

The need to observe the 30-day response period imposed by the GDPR.

Summary of the facts of the case

The investigation commenced following a complaint which reported that the Data Controller violated the Data Subject's Right of Access by refusing to provide certain recordings of their conversations via the call centre.

Decision of the authority / court, mentioning fines

Reference: Decision of the Romanian DPA of 21 June 2023.

During the investigation, the DPA concluded that the Data Controller failed to prove that it responded to the Data Subject's request filed in respect of their Right of Access within the required 30-day period, thus infringing Article 15.3 of the GDPR.

Article 15.3 states that the Data Controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the Data Subject, the Data Controller may charge a reasonable fee based on administrative costs. Where the Data Subject submits the request electronically, and unless otherwise requested by the Data Subject, the information shall be provided in a commonly used electronic format.

In respect of the conclusion of the investigation, the DPA sanctioned the Data Controller with a fine of RON 4,961, equivalent to EUR 1,000.

Additionally, the Data Controller was required to implement technical and organisational measures to ensure effective compliance with requests concerning the rights of Data Subjects as provided by Regulation (EU) 679/2016, including the Right of Access under Article 15.

Take away / action point

The Data Controller should implement the necessary mechanisms to ensure that the Data Subjects receive an answer to their requests within the 30-day period provided by the GDPR.

Case Three

Specific matter of Right of Access the case pertains to

Types of personal data which must be provided to the Data Subject.

Summary of the facts of the case

The investigation was initiated following a complaint by a Data Subject who alleged that the Data Controller failed to provide a complete copy of a video recording for a specific period during which the Data Subject was present on the Data Controller's premises.

Decision of the authority / court, mentioning fines

Reference: Decision of the Romanian DPA of 20 January 2022.

The DPA concluded that the Data Controller must provide video recordings containing images of the Data Subject following their exercise of the Right of Access. The Data Controller can fulfil this obligation by obscuring (blurring) any images that might infringe on the rights and freedoms of other individuals, if necessary. As a consequence, the Data Controller must implement technical and organisational measures to ensure the full exercise of the Data Subject's Right of Access while also respecting the rights of other individuals.

As a result, the DPA determined that the Data Controller failed to provide the complete video recordings requested, thus violating Article 15.3 of the GDPR.

Consequently, the Data Controller was sanctioned with a fine of RON 14,846 (equivalent to EUR 3,000) for violating Article 15.3 of the GDPR.

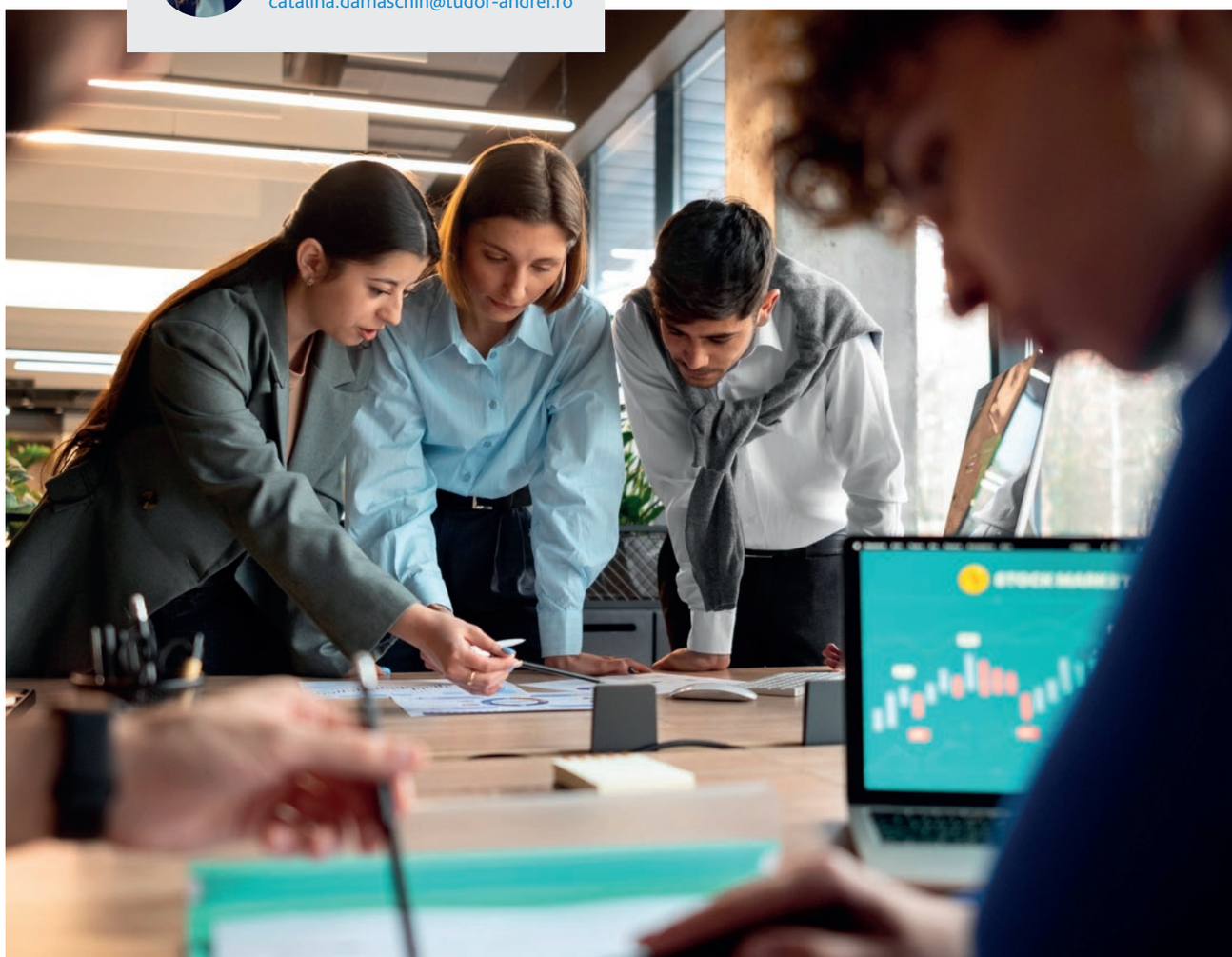
Take away / action point

- The Data Controller must provide the Data Subject with all personal data processed, including video recordings.
- The Data Controller must ensure that the rights and freedoms of third parties are protected.

Data Subjects should receive an answer to their requests within the 30-day period provided by the GDPR.

For further information:

CATALINA DAMASCHIN
BDO Legal | Romania
catalina.damaschin@tudor-andrei.ro



Slovakia

The DPA imposed a fine to the Data Controller for violation of Article 12.3 of the GDPR for not responding to the Data Subject on time.

Case One

Specific matter of Right of Access the case pertains to

Content of request for restriction of processing personal data (substance over form).

Summary of the facts of the case

The Data Controller did not review the entire content of the request to exercise the right to restriction of processing personal data pursuant to Article 18 of the GDPR, and rejected the request based only on its form and document name. The Data Controller stated that the request for exercising the Data Subject's right was not obvious from the form of the delivered document and as the respective request for exercising the Data Subject's right was only mentioned at the end of the document, it allegedly remained unnoticed by the Data Controller by mistake. The Data Controller also did not deal with the request within the required time period of one month from receipt of the request.

Decision of the authority / court, mentioning fines

Reference: Decision of the Slovak DPA published on no-name basis in the annual report of DPA from 2022 (exact decisions of Slovak DPA with case number and date of decision are not publicly available).

The DPA started proceedings on the protection of personal data on the basis of a submission in which the Data Subject stated that it had exercised to the Data Controller the right to restriction of processing the personal data according to Article 18 of the GDPR, which was rejected. The DPA stated that the Data Controller is obliged to review the entire request received from the Data Subject and to analyse it based on its content and not just form (substance over form). It was clear from the part of the document (request) delivered by the Data Subject to the Data Controller that the Data Subject was exercising its right to restriction of processing under Article 18 of the GDPR, notwithstanding the primary purpose and form of the document (request) was not exercising the Data Subject rights. Moreover, the Data Controller is also obliged to process the request of the Data Subject for exercising its rights and to provide the Data Subject with information on action taken on its request within a period of one month from the delivery of the request.

As a result, the DPA imposed a fine to the Data Controller for violation of Article 12.3 of the GDPR for not responding to the Data Subject on time, however the Data Controller subsequently took action on the request of the Data Subject.

Take away / action point

- Exercise sufficient care in reviewing any request of the Data Subject and focus on its substance, taking into account Article 12.3 of the GDPR.
- Respond to the request of Data Subject within the time period prescribed by the GDPR.

The Data Controller also did not deal with the request within the required time period of one month from receipt of the request.

Case Two

Specific matter of Right of Access the case pertains to

Manner of request for Rights of Access by the Data Subject.

Summary of the facts of the case

When exercising the right to access personal data, the Data Controller (the operator providing financial services) referred the Data Subject to a standardised form "Request for exercising the rights of the Data Subject under the GDPR". The Data Controller requested the Data Subject for notarial/official verification of its signature on the standardised form of request for exercising its rights.

Decision of the authority / court, mentioning fines

Reference: Decision of the Slovak DPA published on no-name basis in the annual report of DPA from 2021 (exact decisions of Slovak DPA with case number and date of decision are not publicly available).

The DPA declared that the Data Controller's requirement for a verified signature on the request for Right of Access to personal data is not compliant with Article 12.5 of the GDPR. Requesting a verified signature is an unreasonable condition and is undoubtedly linked to financial considerations (costs of a verified signature). In contrary to Recital 59 and 63 of the GDPR, the Data Controller therefore hindered the Data Subject's rights to access their personal data. The DPA emphasised that the Data Controller should facilitate the Data Subject's rights, and the same should have the Right of Access to personal data without any unreasonable conditions, such as including a verified signature on the request.

Given the Data Controller withdrew the condition of a verified signature during proceedings on the protection of personal data before the DPA, they were not imposed with any fines or measures to remove identified deficiencies.

Take away / action point

Ensure to not impose any unreasonable conditions on the rights of the Data Subject. The Data Controller should not request the verified signature of the Data Subject on the request for exercising their rights.

Case Three

Specific matter of Right of Access the case pertains to

Content of response to request for erasure of personal data.

Summary of the facts of the case

The Data Controller (a public authority) processed personal data of the Data Subject for the purposes of an employment selection procedure based on the explicit consent of Data Subject. The Data Subject objected to the processing of their personal data and requested that the Data Controller erase its personal data from part of a video recording and its presentation from the record to the municipal council meeting at the end of the selection procedure. The Data Controller did not comply with the request, with the justification that they need the personal data for the purposes of public interest and for the fulfilment of its legal obligations.

Decision of the authority / court, mentioning fines

Reference: Decision of Slovak DPA of 26 February 2024 (exact decisions of Slovak DPA with case number and date of decision are not publicly available).

Among other violations by the Data Controller (they should not have requested consent from the Data Subject on the processing personal data for the purposes of an employment selection procedure), the DPA found that in the rejection of the request from the Data Subject, the Data Controller had referred to Article 17.3.e of the GDPR (the establishment, exercise or defence of legal claims), which was incorrect, as the Data Controller should have referred to Article 17.3.b (legal obligation), with this being considered a breach of the transparency principle and Article 12.3. Moreover, the Data Controller responded to the request after the required time period of one month from receipt of the request, without requesting an extension of the time period.

The DPA imposed a fine of EUR 1,000 on the Data Controller, applying the absorption principle, and considering the non-transparent provision of information to the Data Subject (requesting consent of the Data Subject for the processing of personal data) to be the most serious violation by the Data Controller.

Take away / action point

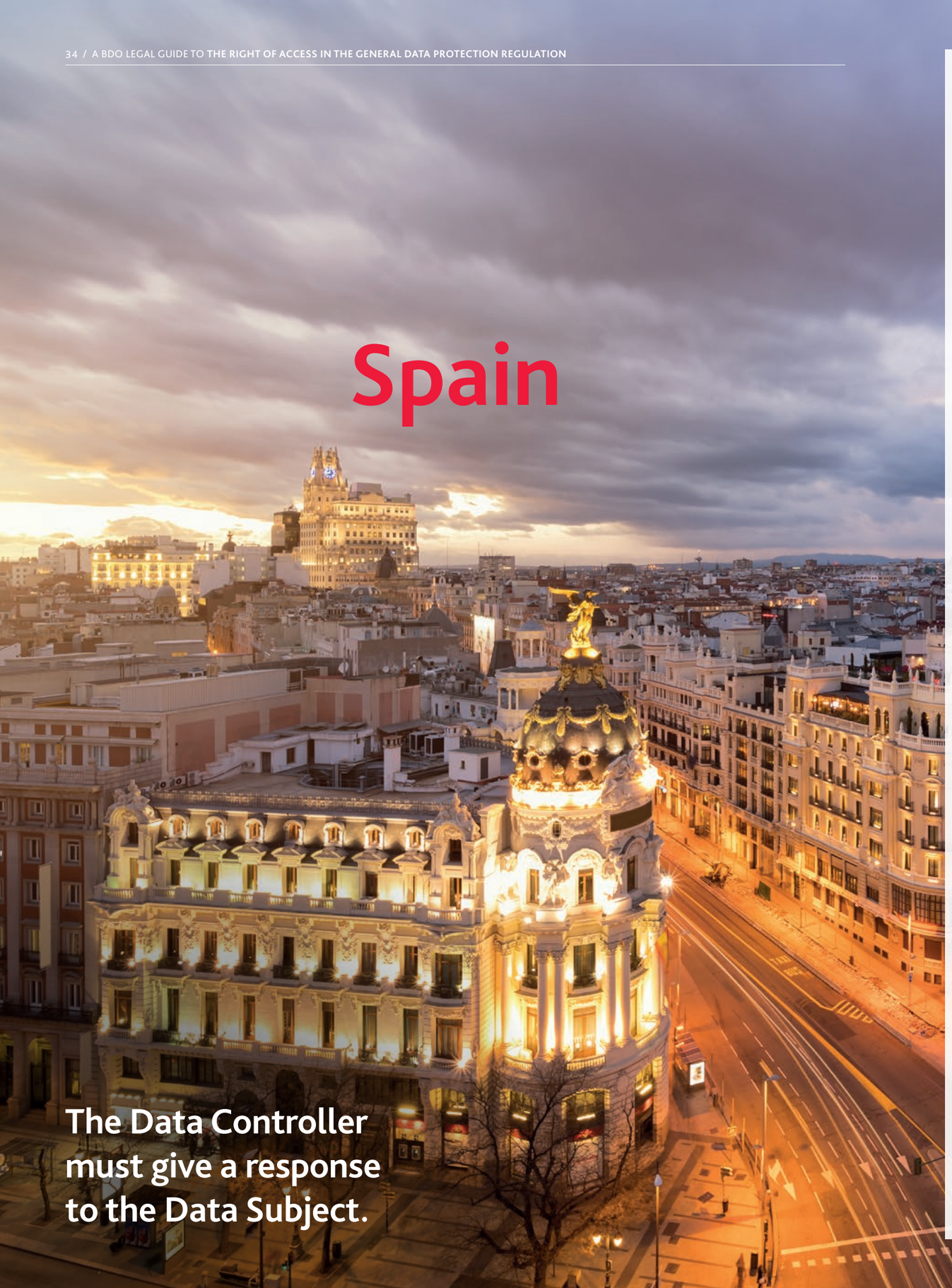
- Rejection of a request from a Data Subject must be justified by the exact provision of the GDPR or respective legislation.
- Responses to requests from Data Subjects must be within the time period prescribed by the GDPR.

For further information:

MAREK PRIESOL
BDO Legal | Slovakia
priesol@bdoslovakia.com

PATRÍCIA KMEŤOVÁ
BDO Legal | Slovakia
kmetova@bdoslovakia.com

Spain



The Data Controller must give a response to the Data Subject.

Case One

Specific matter of Right of Access the case pertains to

Exercising the Right of Access through the customer service department.

Summary of the facts of the case

The Applicant requested the Right of Access to their personal data through a leading Spanish airline's customer service department on numerous occasions. The Respondent, in the face of these repeated requests, did not comply with the Right of Access and consequently the Applicant was unable to access their personal data.

Decision of the authority / court, mentioning fines

For infringement of Article 15 of the GDPR, the Spanish airline was fined EUR 50,000. The decision added an aggravating circumstance of having committed the same infringement previously.

Take away / action point

The Data Controller must give a response to the Data Subject. Not providing a response to an Applicant's request may also be an aggravating factor for future cases.

Case Two

Specific matter of Right of Access the case pertains to

Access to multiple phone call recordings without having to bear the burden of proof.

Summary of the facts of the case

The Applicant exercised their Right of Access when requesting access to the recordings of telephone conversations made by a leading Spanish bank's customer service department, and by the companies it had subcontracted. In response to this request, the bank replied that it needed more information in order to retrieve the recordings. The Applicant asserted that retrieving additional information was the responsibility of the bank.

Decision of the authority / court, mentioning fines

The inadequate management of the Right of Access request by the Respondent led to the infringement of Article 15 of the GDPR, therefore the Spanish Data Protection Agency imposed a penalty of EUR 70,000.

Take away / action point

Although it is legitimate for the Data Controller to request further information, this does not entitle them to impose the burden of the process upon the Data Subject.

Although it is legitimate for the Data Controller to request further information, this does not entitle them to impose the burden of the process upon the Data Subject.

For further information:

ALBERT CASTELLANOS
BDO Legal | Spain
albert.castellanos@bdo.es

MARINA FONTCUBERTA
BDO Legal | Spain
marina.fontcuberta@bdo.es

Switzerland

The new Swiss Data Protection Act entered into force on 1 September 2023. The Swiss rules relating to Data Access Rights may be more restrictive than the GDPR. However, no court decisions were taken in the first year relating to Data Access Rights.

For further information:

KLAUS KROHMANN
BDO Legal | Switzerland

klaus.krohmann@bdo.ch

FOR MORE INFORMATION:

CAROLINE MACDONALD
COORDINATOR | LEGAL SERVICES
BDO GLOBAL OFFICE

+34 686 339 922
caroline.macdonald@bdo.global

This publication has been carefully prepared, but it has been written in general terms and should be seen as broad guidance only. The publication cannot be relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained herein without obtaining specific professional advice. Please contact the appropriate BDO Member Firm to discuss these matters in the context of your particular circumstances. Neither the BDO network, nor the BDO Member Firms or their partners, employees or agents accept or assume any liability or duty of care for any loss arising from any action taken or not taken by anyone in reliance on the information in this publication or for any decision based on it.

The provision of professional services under the BDO brand is the sole preserve of each of the BDO Member Firms in their own country. For legal, regulatory or strategic reasons, not all BDO Member Firms provide legal services. Neither BDO LLP (UK) nor BDO USA LLP (USA) provide legal advice. Where BDO does not provide legal services, we work closely with "best friend" external law firms.

BDO is an international network of professional services firms, the BDO Member Firms, which operate under the name of BDO. Each BDO Member Firm is a member of BDO International Limited, a UK company limited by guarantee that is the governing entity of the international BDO network. Service provision within the BDO network is coordinated by Brussels Worldwide Services BVBA, a limited liability company incorporated in Belgium with its statutory seat in Zaventem.

Each of BDO International Limited, Brussels Worldwide Services BVBA and the member firms of the BDO network is a separate legal entity and has no liability for another such entity's acts or omissions. Nothing in the arrangements or rules of the BDO network shall constitute or imply an agency relationship or a partnership between BDO International Limited, Brussels Worldwide Services BVBA and/or the member firms of the BDO network.

BDO is the brand name for the BDO network and for each of the BDO Member Firms.

© BDO, July 2025.