ISSN 2794-6215

EU GDPR

Casebook 2023

Compilation of decisions by national
data protection agencies from May 2018 to May 2023

ComplyCloud

ComplyCloud

EU GDPR Casebook 2023

Highlighting selected national data protection agency decisions from 2018 to 2023 with a primary focus on Denmark, Germany, Belgium, and the Netherlands.

ComplyCloud ApS
CVR: 35813764
Borgergade 24B, 3.-4. floor
1300 Copenhagen K
Denmark

www.complycloud.com

When referencing this publication, the following source should be cited: 'ComplyCloud EU GDPR Casebook 2023'.

Welcome to ComplyCloud's EU GDPR Casebook 2023

It is with great pleasure that I present to you the EU GDPR Casebook 2023. In this edition, the ComplyCloud legal team has gathered, categorized, and analyzed a range of decisions from across the European Union, with particular focus on the Data Protection Agencies of the Netherlands, Germany, Belgium, and Denmark. The time span of these cases ranges from the inception of the GDPR in May 2018 to May 2023.

Specifically, this Casebook highlights:

- Cases resulting in the 10 largest GDPR fines from each of our three focal countries; the Netherlands, Germany, and Belgium.
- 10 intriguing cases from each of the three focal countries, handpicked due to their potential impact and unique features.
- A collection of interesting cases from Denmark, in recognition of ComplyCloud's core expertise.
- Selected compelling cases from various other EU countries, which we found to be of particular interest.

Through this comprehensive collection, we aim to paint a picture of the evolving data privacy landscape in the EU, building on the principal decisions that continually expand our understanding of the General Data Protection Regulation. Whether you are a seasoned legal professional or a newcomer to the field of data protection, we believe this Casebook will serve as a valuable resource in navigating the complexities of GDPR compliance.

The GDPR's five-year journey has been nothing short of transformative. Since its introduction in May 2018, the GDPR has given individuals greater control over their personal data and introduced new standards for businesses. It has shaped the digital transition in the EU, guiding both domestic and international approaches to data regulation.

At ComplyCloud, we have been keen observers of this development, tracking the progression and interpretation of the GDPR throughout the European Union. The ongoing evolution of GDPR, its impact, and the challenges it presents continue to be areas of focus for us. However, in compiling this Casebook, our aim goes beyond mere observation; we strive to promote transparency and provide a lens into the trends of the GDPR and changes in its enforcement. The cases presented here underline the actions taken by national data protection authorities across the EU, with over 2.5 billion EUR in fines imposed for GDPR breaches. This underscores the commitment to safeguarding data protection within the EU.

In keeping with our tradition, we supplement our legal analyses with a graphical presentation of key figures in data protection law. With our statistical overview, you will be presented with EU-wide numbers on the nature of violations, fines, sectoral trends, and more.

On behalf of everyone at ComplyCloud, we thank you for your interest and engagement with our work. As we continue to navigate the intricacies of GDPR compliance, we are committed to providing you with the most current, comprehensive, and user-friendly resources.

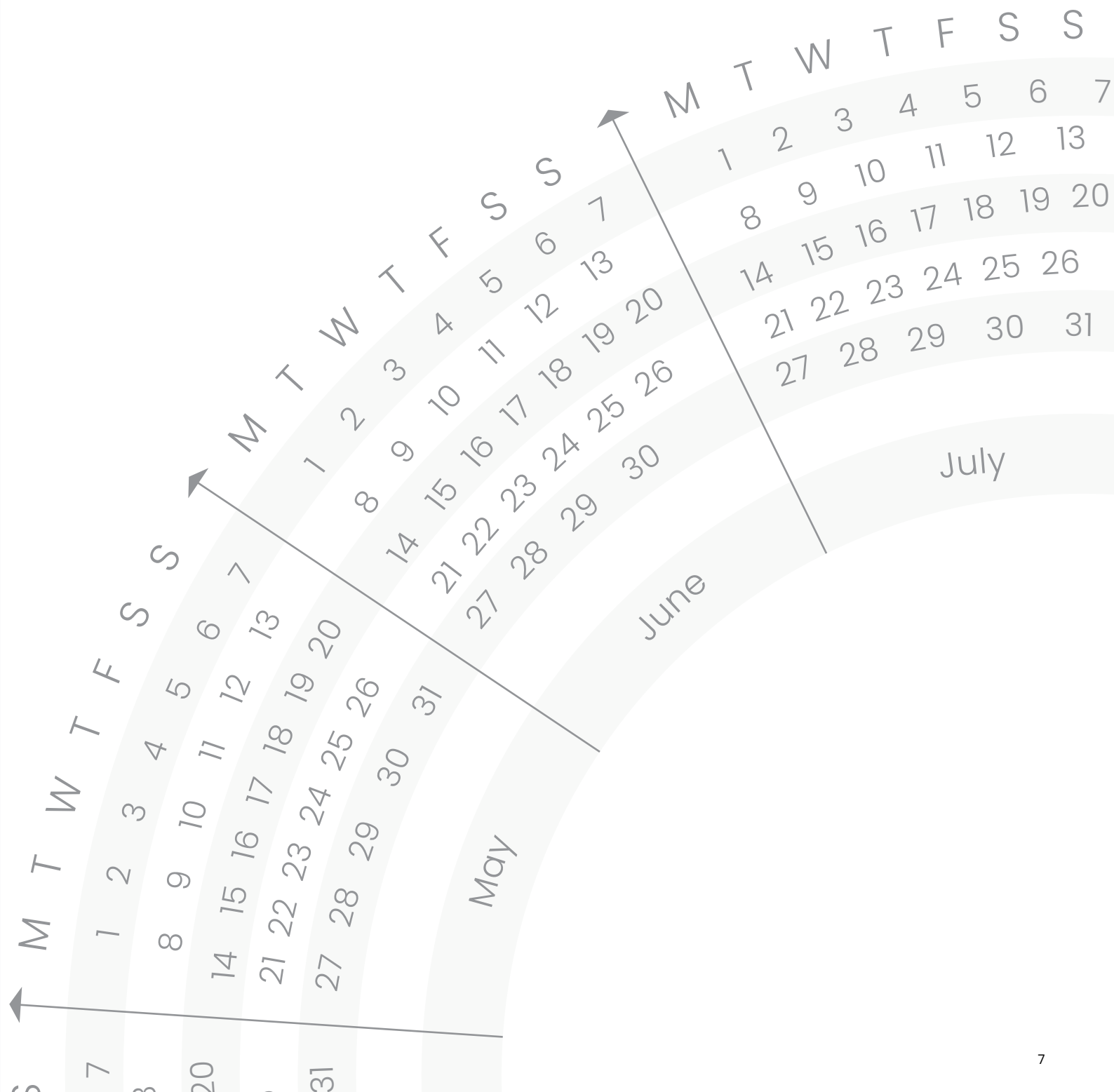
I hope you find the GDPR Casebook 2023 informative and useful. Enjoy your read!

Best regards,
Martin Folke Vasehus
CEO & IT Lawyer
ComplyCloud

Index

GDPR in numbers

Statistical Overview: A Data-Driven Analysis of EU GDPR Enforcement through Country-Specific Trends, Sectoral Differences, and Violation Types.



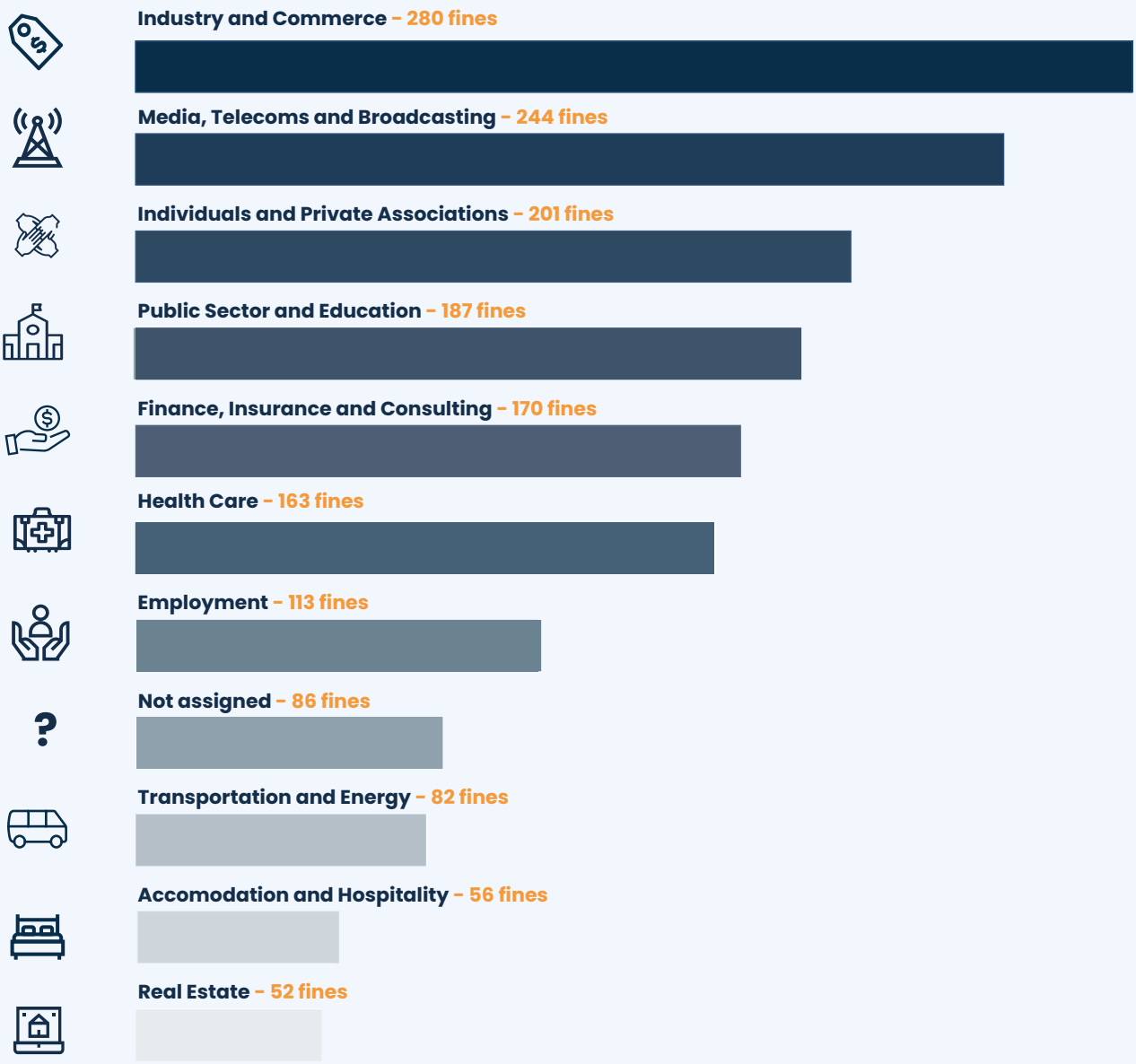
Fines based on different sectors

Cumulative EU totals of fines across different sectors (EUR)

The graph below illustrates the distribution of GDPR fines across sectors, with each bar indicating the cumulative fines for non-compliance. The stark disparity between sectors is evident, particularly the higher and more frequently imposed fines within media, telecom, broadcasting, and industry and commerce sectors. These sectors manage large amounts of personal data and often adopt new technologies, increasing their risk of data breaches. Their high public visibility and data sharing practices, particularly in relation to targeted advertising, makes these sectors more susceptible to complaints.

Number of fines across different sectors in the EU

The graph below displays the total number of GDPR fines imposed in various sectors across the European Union.

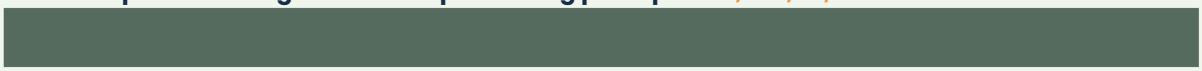


Fines based on type of violaiton

Cumulative sums of fines per violation type across the EU

The graph below depicts the cumulative sums of GDPR fines for each type of violation across the EU. Each bar represents a different violation type, providing a clear comparison of the financial impact associated with each type of GDPR violation.

Non-compliance with general data processing principles – 1,674,711,359 EUR



Insufficient legal basis for data processing – 431,613,697 EUR

Insufficient technical and organisational measures to ensure information security – 379,851,319 EUR

Insufficient fulfilment of information obligations – 237,251,580 EUR

Insufficient fulfilment of data subjects' rights – 51,889,270 EUR

Unknown – 9,250,000 EUR

Insufficient fulfilment of data breach notification obligations – 1,778,582 EUR

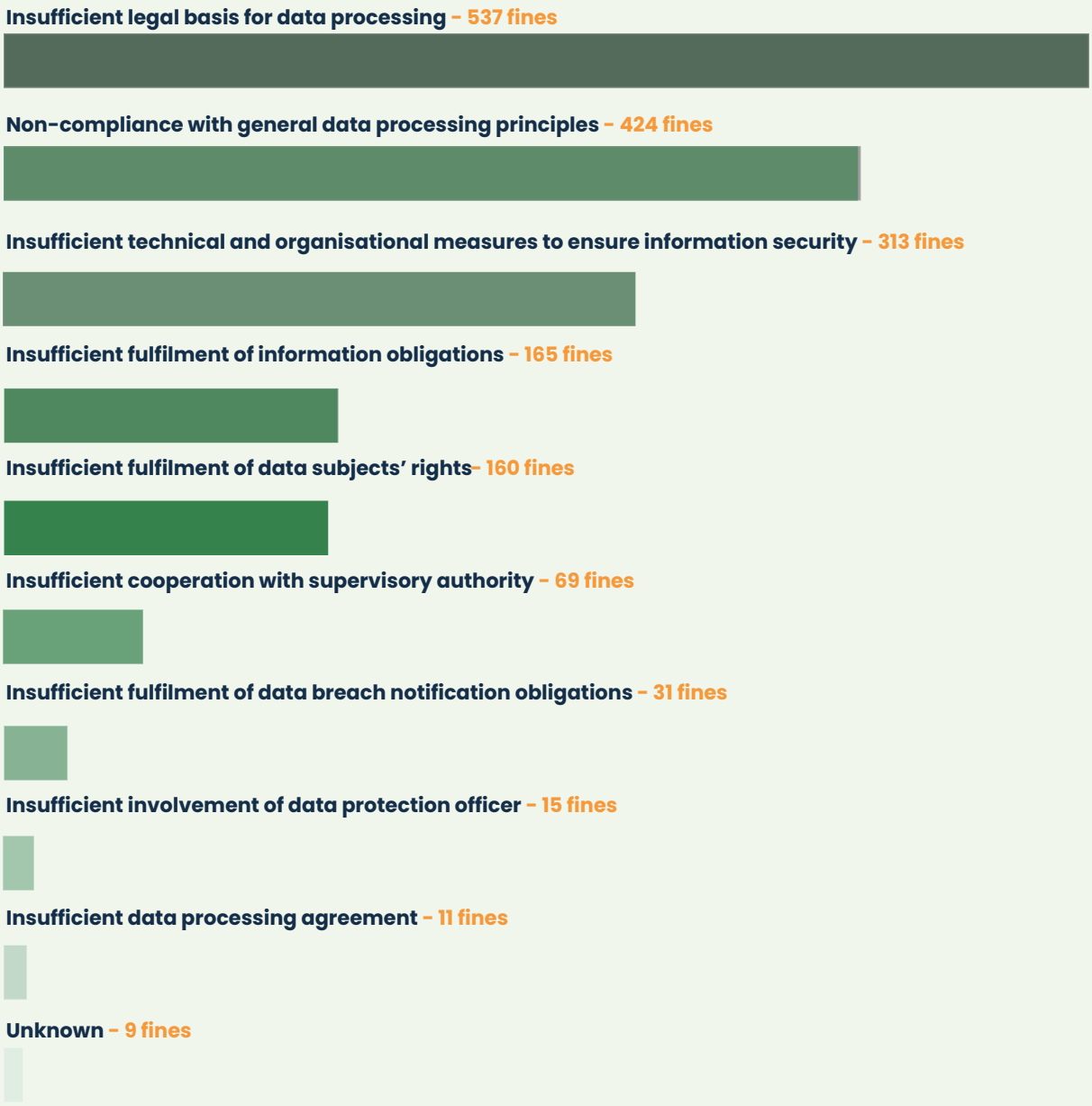
Insufficient data processing agreement – 1,057,110 EUR

Insufficient involvement of data protection officer – 919,300 EUR

Insufficient cooperation with supervisory authority – 840,529 EUR

Number of fines imposed by violation type across the EU

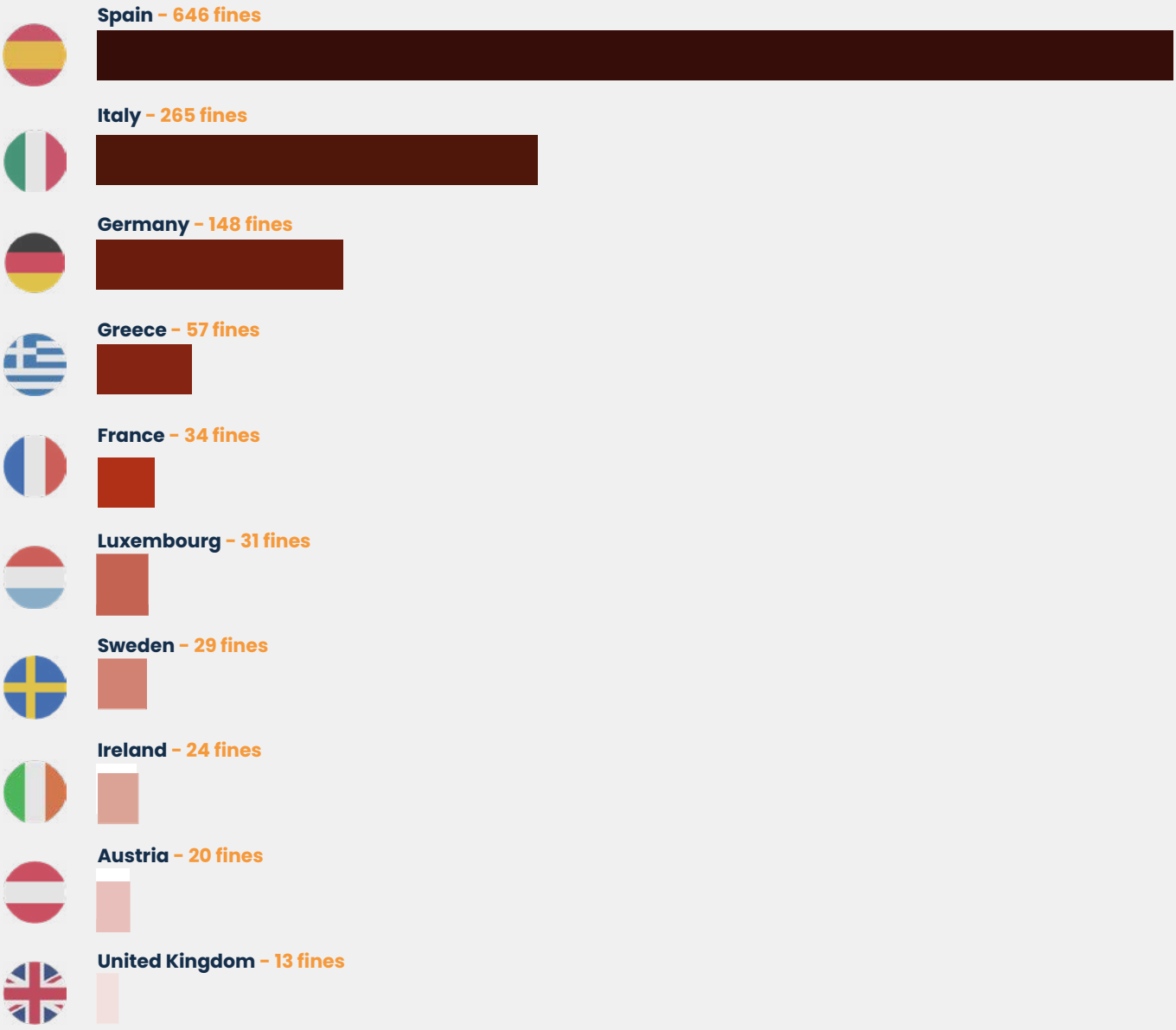
The graph on the left displays the total number of GDPR fines imposed in the EU, broken down by violation type.



Fines based on country

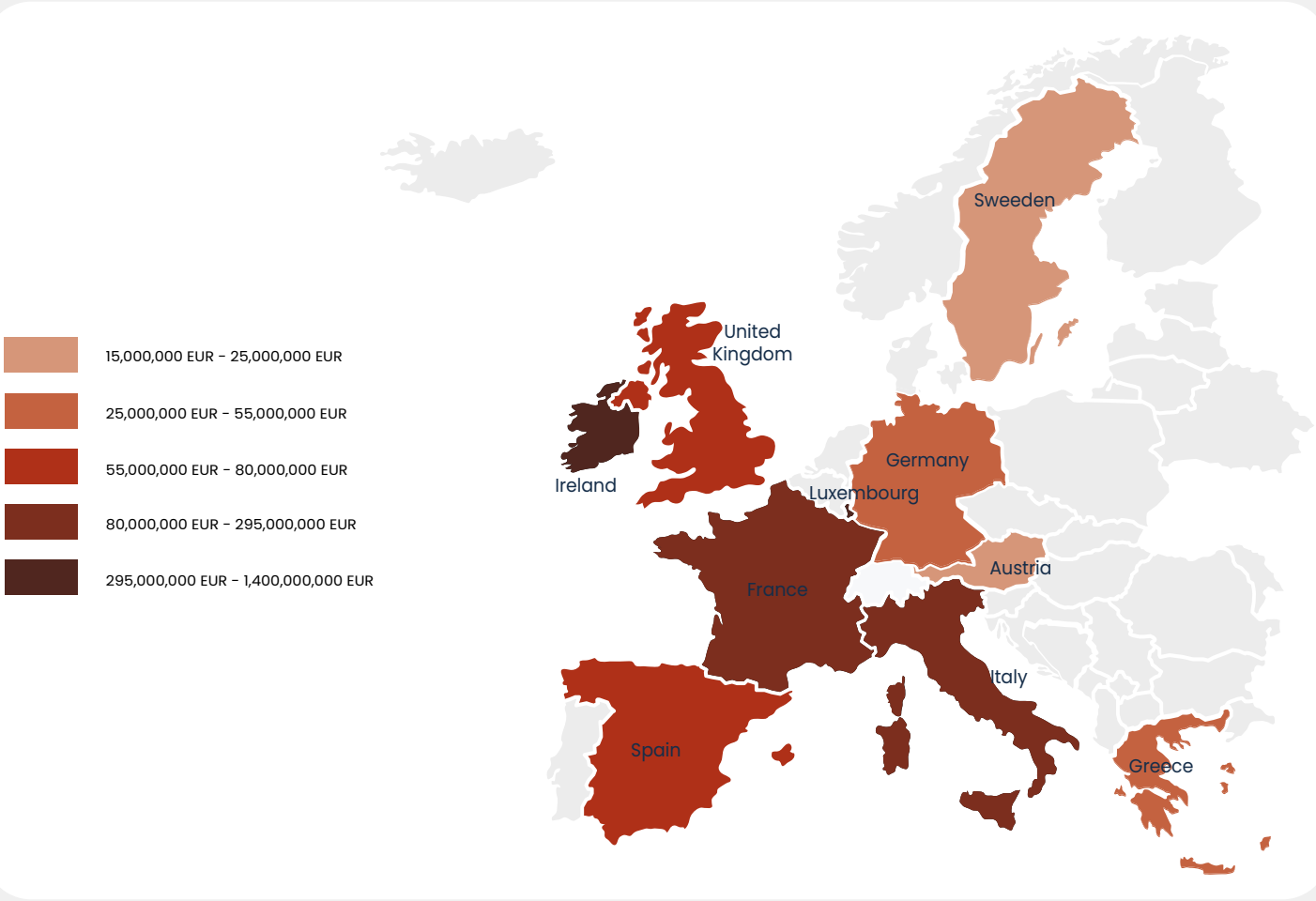
EU Countries by number of fines

The graph illustrates the count of GDPR fines among EU countries. The significant concentration of fines in Spain can be attributed to several factors, both inherent to the Spanish business landscape with a high concentration of SMEs, and the approach of the Spanish Data Protection Authority (AEPD).



Total sums of fines by country across the EU

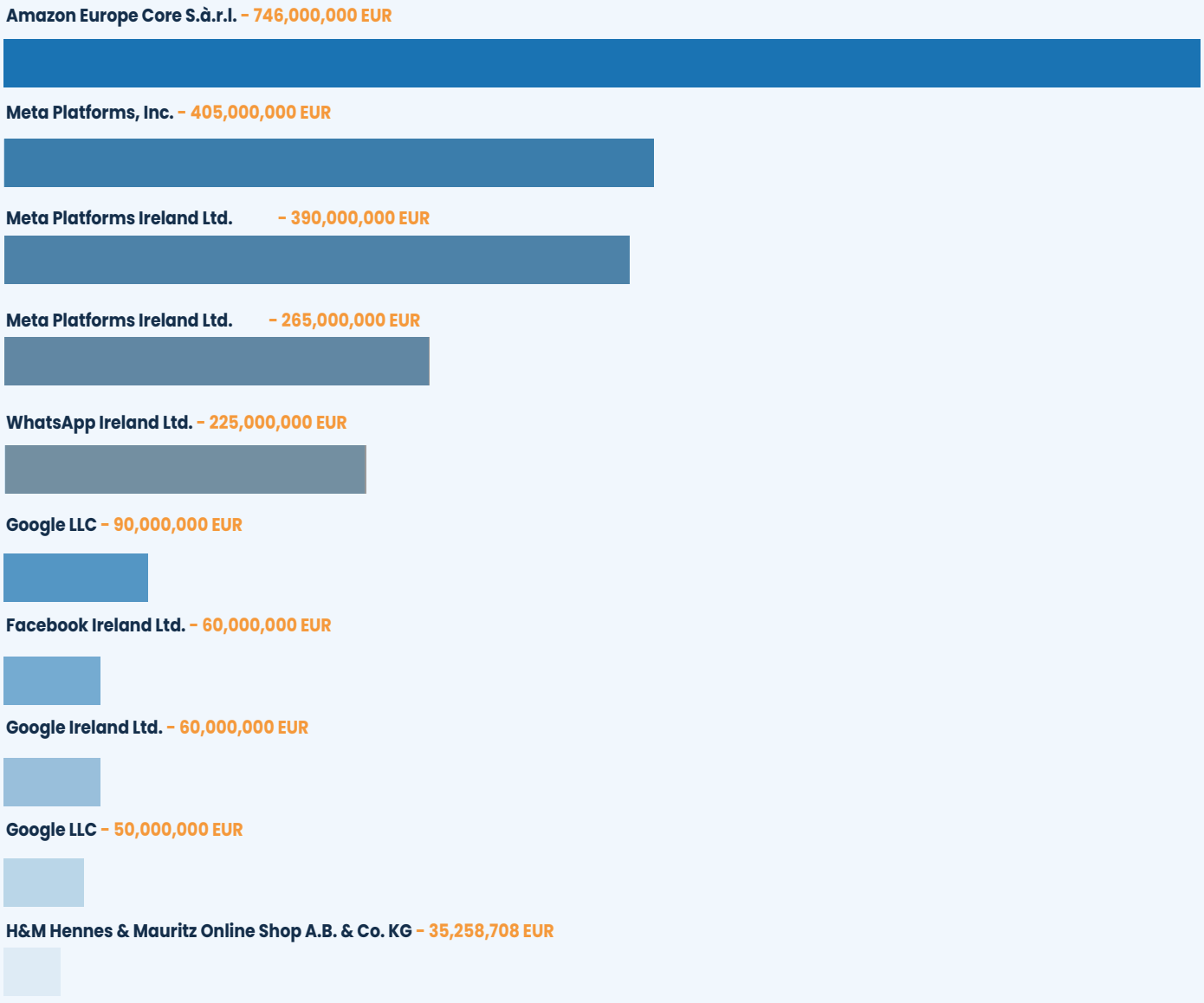
The graph presents the ten EU countries with the highest total sums of GDPR fines, illustrating where the most substantial penalties for non-compliance have been levied. Unsurprisingly, Ireland leads the chart; a consequence of its role as a European hub for many global tech giants like Google and Facebook, resulting in a high number of substantial fines.



Ten highest fines

Top ten GDPR fines in the EU

This graph presents the ten largest GDPR fines imposed across the EU. Each bar corresponds to a distinct case, with the financial penalty reflecting the severity of the GDPR violation considering the entity's annual turnover. To delve deeper into each of these cases, refer to the case commentaries in this Casebook. Our analyses provide insightful context and shed light on the justifications for these substantial fines, facilitating a deeper understanding of GDPR compliance.



Largest fines - Netherlands

01

Tax administration fined for fraud blacklist

Summary

The Dutch Tax Administration had a fraud identification facility (FSV) that contained a blacklist of data subjects registering indications of fraud.

The FSV staff were instructed to use characteristics about individuals, such as their ethnic heritage (i.e., Turkish, Moroccan, and Eastern European) as a selection criterion for further tax investigations.

In some cases, a data subject was labeled a 'fraudster' without this being subject to an adequate investigation. Even if an investigation was carried out, and there appeared to be no fraud indicators, this conclusion was often not noted, and so the suspicion of fraud remained. Furthermore, risk analyses were based on incorrect data in some cases.

Inclusion on this blacklist meant that the data subject suffered economic consequences such as having his/her application for care allowance rejected or being made ineligible for debt rescheduling etc. Around 270.000 people were on this list, and the processing took place from 2013 to 2020. Information about individuals on this list was shared with other authorities and private entities.

Furthermore, unauthorized employees of the Tax and Customs Administration were able to view personal data in FSV due to the inadequate security of FSV.

The decision of the Dutch DPA

The Dutch DPA **imposed** a combined fine of **3,700,000** EUR on the Dutch Minister of Finances for the following violations (broken down into the corresponding fines):

- The Tax administration had no statutory basis for processing personal data in the FSV: EUR 1,000,000 *(GDPR, Article 6(1))*.
- The purpose of the FSV was not specifically described in advance: 750,000 EUR *(GDPR, Article 5(1)(b))*.
- The FSV contained incorrect and obsolete information: 750,000 EUR *(GDPR, Article 5(1)(d))*.
- This particular data was stored for far too long: 250,000 EUR *(GDPR, Article 5(1)(e))*.
- The FSV was not adequately protected: 500,000 EUR *(GDPR, Article 32(1))*.
- The Tax Administration waited over a year to ask its DPO for advice about assessing the risks of using the FSV: 450,000 EUR *(GDPR, Article 32(2))*.

Our remarks

- If a processing activity relies on the legal basis of "necessary for a task carried out in the public interest", the law that the controller refers to must specifically permit the processing in question. This is also the case when the processing is within the general scope of the law. When a processing activity becomes more detailed and invasive (for example by processing special or criminal data) the requirement for clarity of the law is raised.
- When one is processing personal data, it is important to describe the processing as precisely as possible. Furthermore, the purpose of the processing activity should always be clear. This can be mapped in a Risk Assessment and eventually followed by a Data Protection Impact Assessment.
- If the controller has carried out illegal processing and is not referred to its DPO, it is an aggravating circumstance when the DPA is calculating the fine.
- If a processor has previously been found to be in violation of the GDPR, the data protection authority is inclined to issue a higher fine for the subsequent violation.

Published: 07-04-2022 **Journal number:** N/A **Tags:** 01 Legal basis and principles of processing

Tax administration fined for discriminatory processing

Summary

Between 2013 and 2019, around 26,000 parents were wrongly accused of making fraudulent childcare benefit claims, requiring them to pay back the allowances they had received in their entirety. The amount was up to ten thousand euros.

From January 2014, national legislation stipulated that if a person was of Dutch nationality, dual nationality was no longer to be recorded.

The Dutch Tax Administration continued storing data about individuals with dual nationality after the change in legislation in January 2014. In May 2018, approximately 1.4 million Dutch citizens with dual nationalities were registered in a database used by the authority.

In addition, the Administration processed the nationality of applicants to combat organized fraud. Applications submitted by dual nationals were automatically marked as a 'high risk-application' by an algorithm and would be further investigated.

Furthermore, certain nationalities were used to detect organized fraud. Data subjects with certain nationalities were more likely to be checked for fraud.

The decision of the Dutch DPA

The Dutch DPA **imposed** a total fine of **2,750,000** EUR on the Dutch Ministry of Finances for the following violations (with corresponding fines):

- Unlawful retention of data on dual nationality: 750,000 EUR *(GDPR, Articles 6(1) and 5(1)(a))*.
- Unnecessary use of dual nationality as an indicator of the risk of fraud: 1,000,000 EUR *(GDPR, Articles 6(1) and 5(1)(a))*.
- Inappropriate use of dual nationality to detect organized fraud: 1,000,000 EUR *(GDPR, Articles 6(1) and 5(1)(a))*.

Our remarks

- Governmental bodies have a heightened responsibility to perform lawful processing due to the power imbalance between the government and its citizens as the data subjects do not have a choice to have their personal data processed by the given authority.
- The less far-reaching form of processing should always be used when possible. For example, instead of using dual nationality as an indication of fraud, the Tax Administration should only check a person's nationality when there are other concrete indications of fraud.
- As a controller or processor, you should always be aware of national legislation that either prohibits or restricts certain types of processing or the processing of certain types of personal data.
- The DPA will impose a higher fine if the data subjects have suffered economic damages due to illegal processing.

Tennis association fined for selling personal data

Summary

The Dutch tennis association KNLTB sold personal data about more than 300,000 members to two sponsors for the purpose of direct marketing. The personal data was in the form of name, gender, address, and telephone numbers of members. The sponsors approached some of the KNLTB members by mail or telephone.

During the case, the Dutch DPA assessed if sharing personal data with sponsors was within the original purpose of executing the membership. Secondly, it assessed if the KNLTB could rely on the legal basis of legitimate interest when selling personal data.

The KNLTB claimed that the Dutch DPA was biased in its approach because, in a news show, the DPA had given the impression that the KNLTB had acted incorrectly while investigations were still ongoing. The Dutch DPA acknowledged this, but it did not have any legal effect on the case as the proceedings in the case took place in accordance with formal procedures.

The decision of the Dutch DPA

The Dutch DPA **imposed** a fine of **525,000** EUR on the KNLTB for the following violations:

- Selling personal data without a legal basis *(GDPR, Article 6(1))*.
- Not making it clear to their members how their personal data was processed *(GDPR, Article 5(1)(a))*.
- Processing personal data with a purpose that was incompatible with the original purpose for collection *(GDPR, Article 5(1)(b))*.

Our remarks

- A controller should be aware of how the DPA act during a case, and if they act according to formal procedures, etc.
- If the processing serves a purpose other than the one for which the personal data was originally collected, it should be assessed whether this other purpose is compatible with the purpose for which the personal data has been collected.
- In this case, the purpose of generating extra income by selling personal data to sponsors was not within the original purpose of membership. Therefore, the KNLTB should have obtained the consent of the members for this action.
- The Dutch DPA stated that any solely commercial purpose, such as interest in gaining income, could not qualify as a legitimate interest. This is quite a restrictive interpretation of the scope of legitimate interest as a legal basis.

National Credit Register (BKR) fined for personal data access

Summary

The National Credit Register (BKR) in the Netherlands offered two options for complying with a request for access from a data subject:

1. A free option where a data subject could send a manual inquiry by post once per year, or
2. a paid yearly subscription option that gave the data subject unlimited access to their personal data.

BKR argued that they were allowed to charge a fee for electronic access because when a data subject had unlimited access to their personal data, it constituted requests of a repetitive nature.

They also argued that they could set up a maximum of one free access per year because more requests than that would be repetitive. They selected that figure because the average number of consumers' requests for access to their credit status was on average once a year.

The decision of the Dutch DPA

The Dutch DPA **imposed** a fine of **830,000** EUR on the BKR for the following violations:

- Asking data subjects to pay a fee to provide them with electronic access to their personal data: 385,000* EUR *(GDPR, Article 12(5))*.
- BKR's practice discouraged data subjects to file an access request: 650,000* EUR *(GDPR, Article 12(2))*.

*The total fine was reduced by 20% due to the similarities between the two violations and so that the DPA did not violate the principle of proportionality.

Our remarks

- Providing the data subject with free postal access to personal data once per year does not entitle data controllers to charge a subsequent fee for providing an electronic copy of the personal data.
- One cannot set up a general cap restricting the number of free requests a data subject can make per year. It must be demonstrated on a case-by-case basis that the given requests are repetitive.
- The ability to view data in a digital portal for a year after payment does not constitute repetitive requests. Therefore, the data controller cannot, on a general basis, charge a fee to provide access to the data subjects.
- A data controller may never discourage data subjects to exercise the right to access their data. The Dutch data protection found that the BKR had actively discouraged the exercise of this right when communicating one free access per year in its privacy policy.

TikTok fined for violating children's privacy

Summary

TikTok is an app that allows users to create, edit and share short videos online. By the end of 2019, the app was used by 830,000 Dutch children between the ages of 12 and 18.

From 25 May 2018 to 28 July 2020 inclusive, the privacy policy of TikTok was only available in English.

In this case, TikTok believed that the Dutch DPA did not have the authority to impose a fine on TikTok as they had their main establishment in Ireland. The DPA found that TikTok had a main establishment in Ireland from 29 July 2020 and the Dutch DPA had competence until that date.

The decision of the Dutch DPA

The Dutch DPA **imposed** a fine of **750,000** EUR on TikTok for only providing their privacy policy in English to Dutch children *(GDPR, Article 12(1))*.

Our remarks

Transparent information

- When a controller is communicating with data subjects who speak a different language, they must, where possible, provide a translation of the information in a language that the data subjects understand. This is especially the case when the data subjects are children.
- It cannot be an argument for not translating e.g., a privacy policy, that the data subjects from a specific nation, in general, have a good command of English.
- A data controller should be aware of who their data subjects are. When a large amount of users of a service are children, the wording should be adapted to children when communicating with them e.g., when writing the privacy policy.

Competence of a DPA

- Where a data controller has established their primary operations across multiple EU countries, the lead supervisory authority holds the principal responsibility for taking action towards this data controller. The lead supervisory authority is identified as the governing body situated in the state where the data controller's primary operations are located.
- If a company does not have a primary establishment in Europe, any EU member state is empowered to supervise its activities. In this case, the Dutch Data Protection Authority would be authorized to take action against any violations until such time as TikTok established its primary operations in Ireland.

Company fined for processing employees' fingerprint data

Summary

An unnamed company scanned the fingerprints of employees in order to monitor attendance and absence.

The scanning machines calculated a template of the fingerprint and stored it as a text file.

The fingerprint templates were recorded at the beginning of 2017 and were still stored in 2019. This included employees that had resigned from the company.

There was no documentation of any policies or procedures relating to employee consent, either permitting or refusing the recording or storage of fingerprints.

The company argued that the supplier of the scanning system should have pointed out the GDPR violation but this argument was found to be irrelevant by the Dutch DPA.

The decision of the Dutch DPA

The Dutch DPA **imposed** a fine of **725,000** EUR on the unnamed company for processing biometric data in the form of fingerprints for the purpose of monitoring absence *(GDPR, Article 9(1))*.

Our remarks

Monitoring measures

- A consideration when implementing measures to monitor employees is that this should always be done in the least impactful manner. In this case, both attendance and absence could have been monitored by using a chip or keycard, resulting in the employer refraining from processing any sensitive data.
- The use of biometric data for access monitoring is only suitable when unauthorized access can have major negative consequences. This is, for example, the case when monitoring access to high-security facilities like nuclear power plants.

Consent as a legal basis in employment

- An employer should think twice before using consent as a legal basis for processing personal data about their employees. It is difficult to obtain consent that is freely given due to the inequality between employees and employers. In some cases, the legal basis for these processing activities can be a legitimate interest if the employer can justify the purpose of the processing.
- If an employer decides to use the consent of employees as a legal basis, policies or procedures for how the consent is obtained and recorded should be provided/readily available. To ensure that consent is freely given, it is necessary that the employee does not suffer any negative consequences by refusing to consent.

Accountability

- A data controller cannot put the responsibility on suppliers when it comes to the choice of measure to achieve a purpose. It will always be the data controller's responsibility to ensure compliance with the services they use.

Published: 30-04-2020, **Journal number:** N/A **Tags:** 01 Legal basis and principles of processing

Municipality fined for missing legal basis for Wifi-tracking

Summary

The municipality of Enschede used WiFi counting in the city center with the aim of measuring how crowded the city center was.

Sensors were placed in high streets that detected the WiFi signals from the mobile phones of passersby. Each phone was registered separately and given a unique code.

The 'counting' became 'tracking' as it was possible through data analysis to deduct information about specific persons. For example, where they worked or lived, or in some cases if they went to church, etc.

The decision of the Dutch DPA

The Dutch DPA **imposed** an administrative fine of **600,000** EUR on the Municipality of Enschede for processing personal data of owners/users of mobile devices without any legal basis *(GDPR, Articles 5(a) and 6(1))*.

Our remarks

- If a processing relies on the legal basis "necessary for a task carried out in the public interest", the law that the controller refers to must specifically allow the processing activity in question. It is not sufficient for "day-to-day administration" to legitimize the use of WIFI in such cases.
- Moreover, when collecting data for one purpose, the data controller should consider if the data could be used for other purposes. This consideration should be included in a risk assessment.
- Even if a data controller has a legal basis for monitoring citizens, this should always ensure that the processing is conducted in the most privacy-friendly way possible. For example, instead of WiFi-tracking cell phones, they could have used an automatic visitor counter. This alternative would not collect any personal data, while still serving the purpose of counting visitors.

Published: 29-04-2021, **Journal number:** N/A **Tags:** 01 Legal basis and principles of processing

Foreign office fined for poor security

Summary

Over the last three years, The Dutch Ministry of Foreign Affairs has processed approximately 530,000 visa applications per year.

To facilitate the Schengen visa process, the Ministry used the National Visa Information System (NVIS) as its digital platform. However, the security measures of the NVIS were inadequate, leading to the possibility of unauthorized access and tampering of files.

Additionally, the Ministry failed to inform visa applicants about the sharing of their personal data with third-party entities.

The decision of the Dutch DPA

The Dutch DPA **imposed** an administrative fine of **55,000** EUR on the Ministry of Foreign Affairs for inadequate security regarding visa applications *(GDPR, Article 32)*.

Our remarks

- If a controller must live up to certain security requirements due to specialist legislation, these requirements will often align with GDPR, Article 32. This is because Article 32 of the GDPR obliges the data controller to ensure appropriate security measures in light of the nature, scope, context and purposes of processing personal data.
- When the sensitivity of the personal data is high, the requirements for safety measurements also rise. When dealing with highly sensitive personal data, the requirements for safety measures also increase correspondingly.
- Within an organization, user access should always be limited in a way so that employees only have access to necessary personal data corresponding to their role. This can be achieved by implementing procedures for granting and revoking user access to different employees at different points in time.
- Logging is an effective way to ensure technical security. However if the logs contain personal data, procedures must be implemented to ensure compliance with data processing regulations.

Published: 06-04-2022, **Journal number:** N/A **Tags:** **05** Data security

DPG Media fined for unnecessary ID requests

Summary

DPG produced magazines that subscribers could receive by taking out a subscription. In order to send the magazines to subscribers, DPG collected personal data, including the subscribers' names, addresses, and financial information such as bank data.

When individuals requested access to or erasure of personal data, DPG consistently required the individual making the request to prove their identity. If the request was submitted through the online form, DPG immediately prompted the requester to provide an identity document. For requests submitted via email, DPG sent a corresponding email requesting the submission of proof of identity. DPG maintained that a request for proof of identity was necessary before processing any request.

DPG claimed that, in accordance with GDPR, Article 12(6), it had the right to confirm the identity of individuals involved by obtaining a copy of their identification documents before granting access to or deleting their personal data.

The decision of the Dutch DPA

The Dutch DPA **imposed** an administrative fine of **525,000** EUR on DPG Media Magazines BV (DPG) for hindering the right to access and erasure *(GDPR, Article 12)*.

Our remarks

- When data controllers are unsure about the identity of a data subject making a request, they can request additional information to confirm the identity of the data subject in question, as stated in GDPR, Article 12(6). However, this does not entitle the data controller to automatically request more information when receiving requests from data subjects who are exercising their rights. The assessment of uncertainty regarding identity should be done on a case-by-case basis.
- If there is any doubt about the identity of the person making a request, data controllers should only request necessary information, and refrain from collecting more sensitive personal data. Asking for copies of identification documents should only be done when strictly necessary due to the sensitive nature of the personal data contained in identity cards.
- One way to confirm the identity of a data subject could be to look at the subscriber/customer number in combination with the name and address of the requester or by e-mail verification.
- Data controllers are obliged to make it as easy as possible for data subjects to exercise their rights. Therefore, data controllers should not implement measures that make it harder for data subjects to request access or exercise their rights.

Locate Family fined for not appointing a representative

Summary

Locatefamily.com is a non-EU based organization which offers a platform enabling users to find the contact information of individuals they have lost contact with.

The Dutch DPA received several complaints about Locatefamily.com for failing to respond to requests for erasure by data subjects. Without their knowledge, the website disclosed personal data of roughly 700,000 Dutch people.

The decision of the Dutch DPA

The Dutch DPA **found** that the processing was within the scope of the GDPR and decided to impose an administrative fine of **525,000** EUR on Locatefamily.com for failing to appoint an EU representative *(GDPR, Article 27(1) Pursuant to Article 3(2)(a))*.

Our remarks

- According to GDPR, Article 3(2), a data controller not established in the EU is subject to GDPR if they offer goods or services to data subjects within the EU.
- If a controller offers services through a website aimed at European residents, they must comply with GDPR, Article 3(2) and appoint an EU representative.
- The precise criteria for determining when goods or service are "offered to data subjects in the Union" remains unclear. The mere fact of having a website or app that is available for data subjects in the EU does not necessarily trigger GDPR, Article 3(2).
- In the present case, the Dutch DPA probably found that Locatefamily fell under the GDPR because it disclosed information about a large number of European citizens and therefore should have foreseen that their service would be used by Europeans seeking to locate other Europeans.
- Factors that support the conclusion that goods and services are offered to data subjects in the EU include:
    - If the company uses marketing directed at EU citizens
    - If the company has its website in European languages other than English
    - If the company sell goods or services intended for European customers, such as travel services.

Published: 10-12-2020, **Journal number:** n/a **Tags:** 07 Scope of the GDPR

Selected interesting cases – Netherlands

02

Can commercial interest be a legitimate interest?

Summary

VoetbalTV was a platform that streamed amateur football matches in the Netherlands. The platform used cameras placed around the fields to record matches.

The VoetbalTV platform offered the ability to watch football clips, analyze matches, collect data, and share it with others. Users could access highlights and analytical tools created by the platform's editorial team, including goals and opportunities.

To process this data, VoetbalTV relied on legitimate interest as per GDPR, Article 6(1)(f).

The Dutch DPA decision

The Dutch Data Protection Authority (AP) claimed that VoetbalTV had violated the privacy rights of individuals, as they could not base the processing on legitimate interest, and instead should have obtained consent from all the people in the footage. The Dutch DPA fined VoetbalTV 575.000 EUR. VoetbalTV then appealed the case to the District Court.

Decision by the District Court

VoetbalTV argued that (1) the journalistic exception applied and therefore the processing was not covered by the GDPR and (2) commercial interest can be a legitimate interest and that they also pursued other interests.

Regarding the journalistic exception, the Court found that VoeltbalTV could not use this exemption as the broadcasting of amateur football matches did not only serve a journalistic purpose. It did not have enough news value for that, and the processing had the character of unfiltered footage, rather than journalistic content.

Regarding legitimate interest, the Court stated that one cannot exclude commercial interest from being a legitimate interest. Furthermore, VoetbalTV pursued the interests of involvement and fun of football fans, performing technical analysis and making it possible to watch matches remotely.

The District Court annulled the decision of the Dutch DPA. The decision was appealed.

Decision of the Council of State

The Data Protection Authority argued that a "legitimate interest" is an interest that **follows** from the law. Whereas VoetbalTV believed that a "legitimate interest" is any interest that does **not conflict** with the law.

The decision of the Council of State

The Council held that VoetbalTV's interest were not solely commercial in nature. The DPA should have taken into account the other interests that the platform presented during the case. Therefore, the appeal lodged by the DPA was unfounded and the judgement under appeal was upheld.

Our remarks

- While it remains unclear whether a purely commercial interest can be considered a legitimate interest, it cannot be excluded as a possibility. However, it could be argued that the Council believed it can be. For example, the Council affirmed the District Court's statement that the test for legitimate interest is to see whether it was not prohibited. A purely commercial interest would pass that test. Furthermore, GDPR, recital 47, states that processing for the purpose of direct marketing can be based on legitimate interest. This supports the notion that a purely commercial interest could be a legitimate interest.
- When a data controller wants to rely on a legitimate interest, they should ask themselves the following questions:
    1. Determine if there is a good reason for collecting and using the data.
    2. Decide if the data collection is actually needed.
    3. Weigh the benefits of collecting the data against the potential risks to people's privacy.
- The case was highly debated, and it led to the European Commission sending a **letter** to the DPA about their concerns regarding their interpretation of legitimate interest. VoetbalTV went bankrupt in September 2020, partly because of the ongoing proceedings.

Grandmother ordered to delete Facebook photos of grandchildren

Summary

A mother of three underage children sued her own mother (the grandmother of the children). She wanted the grandmother to remove pictures of the children from Facebook and Pinterest as the grandmother had not obtained consent from the mother to publish the photos.

The Dutch GDPR Implementation Act stipulates that posting photos of minors who have not turned 16 requires the consent of the children's legal representative.

In the case, the grandmother argued that the posting was not under the scope of the GDPR as the posting fell under the "household exemption" that states that the GDPR does not apply to "purely personal" or "household" processing of personal data. As one of the children had lived with the grandmother for seven years, the grandmother also argued that her special relationship with this child should allow her to post a picture of the child.

The decision of the Court of First Instance of Gelderland

- The Court **ordered** the grandmother to remove the pictures of the children on her Facebook and Pinterest accounts.
- The grandmother was required to pay **50** EUR for each day she failed to comply with the judgement, up to a maximum of **1,000** EUR.

Our remarks

- It is important to note that this is a very specific and individual interpretation, under a national GDPR related law, and that posting pictures of children on Facebook is not per se excluded from falling under the "household exemption".
- In this particular case, the Court determined that the grandmother's act of posting pictures of the children did not qualify for the "household exemption", as it could not be established that the photos would not be accessible to third parties. Thus, the posting was covered by GDPR rules. If an individual has a public profile and their pictures can be found via search engines such as Google, it suggests that user's act of posting photos is subject to the GDPR.

Legal basis for registration in Credit System

Summary

A data subject took out a loan with Hoist Finance which was registered in the Central Credit Information System (CKI) of the Credit Registration Office (BKR) with a special code "A" due to payment arrears. After the debt was settled, the data subject requested that the entry be removed from the BKR registration, but the controller did not comply.

The District Court of Amsterdam referred preliminary questions to the Dutch Supreme Court, asking whether the processing of personal data in the CKI must be assessed in accordance with GDPR, Articles 6(1)(c) and 6(1)(f), or both provisions, and whether the data subject is entitled to the right to erasure and right of objection under GDPR.

The decision of the Dutch Supreme Court

- The Supreme Court **ruled** that the processing of personal data in the CKI must be examined in accordance with the legitimate interest of the controller *(GDPR, Article 6(1)(f))*, rather than a processing necessary for complying with a legal obligation *(GDPR, Article 6(1)(c))*. It also stated that the data subject is entitled to the right to erasure and right of objection under the GDPR.

Our remarks

- Before using Article 6(1)(c) of the GDPR, it is essential to ensure that there is a legal obligation to process the personal data. This means that there must be a legal provision that explicitly requires the processing of personal data for a specific purpose.
- In this case the legal provisions did not provide clarity on which personal data could be registered in the CKI, the conditions for registration, and the time limits for the deletion of data. The CKI regulations, which were not based on a legal basis, governed these aspects. Personal data was registered in the CKI through an agreement between the BKR and credit providers.
- If the processing of data is based on GDPR, Article 6(1)(c) the data subjects do not have the right to erasure. Therefore, the legal basis relied on by the controller is important in regards to data subjects' rights.

Published: 03-12-2021 , **Journal number:** 21/00241 **Tags:** 01 Legal basis and principles of processing

Surgeon sued Google for linking to articles about her

Summary

A plastic surgeon who had been conditionally suspended in 2016 for a lack of patient aftercare requested Google to delete search results linking to articles about her suspension, pursuant to GDPR, Article 17. The disciplinary measure against the surgeon were published on a website under the title 'blacklist' due to national legislation.

Court decision

After Google rejected the request, the issue was brought before the Court which upheld the surgeons' claim. The Court considered the right to privacy to outweigh the right to freedom of expression and freedom of information as the surgeon suffered unnecessary negative impact as potential patients would find her on a "blacklist" if they googled her name.

Google argued that the surgeon was a public figure, which talked in favor of the public interest to know about her disciplinary measures. The Court did not find this leading to the right to freedom of expression overruling the right to privacy.

Court of Appeal

The surgeon argued that her request should be assessed based on GDPR, Article 10 (processing of personal data relating to criminal convictions), whereas Google had no legal basis to process criminal personal data about her. To this the Court of Appeal found that disciplinary personal data did not fall under the definition of criminal personal data under the GDPR.

The Court of Appeal found that the surgeon did not provide sufficient evidence that she was substantially hindered by the contested search results. The Court considered that the applicant is a public figure in a debate on a subject regarding her profession, and that her controversial treatments and products require easily accessible online information for patients. The Court's decision was based on the public's interest to access information, and that outweighed the applicant's right to privacy in this case.

Supreme Court

The Supreme Court found that the Court of Appeal had already considered correctly whether processing the data was strictly necessary. Therefore, they upheld the Court of Appeal's decision.

The decision of the Dutch Supreme Court

- The Dutch Supreme Court **upheld** the decision of the Court of Appeal, and thereby accepted Googles' initial rejection of the request for erasure.

Our remarks

- When an individual is subjected to disciplinary action, their personal data does not fall under the category of criminal data as per Article 10 of the GDPR. As a result, it is permissible to process personal data about disciplinary matters without having to adhere to the special requirements of Article 10 of the GDPR. Criminal data can only be processed by public authorities or individuals who have a legal basis under EU or national law.
- If an individual is in the public eye, they should anticipate heightened levels of scrutiny as they are often in positions of power, influence, or authority, and their actions can have a significant impact on society.
- The right to freedom of expression and freedom of information may outweigh the right to data protection, resulting in instances where the data controller may decline requests for erasure.

Published: 25-02-2022, **Journal number:** 20/02950 **Tags:** 03 Right to erasure and rectification

Formal warning to supermarket about facial recognition

Summary

A Dutch supermarket received a formal warning from the Dutch Data Protection Authority due to the use of facial recognition technology. Although the system was turned off in December 2019, the supermarket expressed interest in turning it back on.

The supermarket used the technology to protect its customers and staff from potential shoplifting by comparing the faces of those entering the store to a database of banned individuals. The system automatically scanned everyone who entered the store's face to do this.

The decision of the Dutch DPA

- The Dutch DPA issued a **warning** to the supermarket, **prohibiting** the use of facial recognition in the stores.

Our remarks

- As facial recognition processes biometric data, one needs to be able to use one of the exceptions in GDPR, Article 9(2). Pursuant to GDPR, Article 9(2)(a), explicit consent can be an exception to the prohibition of processing sensitive personal data. Walking into a store cannot count as explicit consent itself, as there is no active action from the data subject regarding the consent.
- In the opinion of the Dutch DPA, facial recognition can also be used for ensuring authentication or security. But there is a high threshold for when the need for it is serious enough. In their opinion, it is appropriate to use facial recognition for ensuring security at nuclear power plants, but the purpose of avoiding shoplifting is not enough to justify facial recognition.
- This is a bit of a strict interpretation. For example, in Denmark, it has been accepted to use facial recognition for identifying banned football fans outside football stadiums.
- Nevertheless, if one wants to use facial recognition one must carefully assess the processing before taking the system into use. This can be done by doing a risk assessment, where it should be evaluated which other purposes the data collected can be used for, for example, profiling, surveillance, etc.

Published: 15-12-2020, **Journal number:** N/A **Tags:** 01 Legal basis and principles of processing

Compensation for non-material damage

Summary

A person filed multiple requests under the Freedom of Information Act and data protection law, after their personal data was shared on an online forum without their consent.

The individual claimed non-material damages resulting from the loss of control over their personal data and delays in receiving information about the forum messages. However, the State Council rejected the claim, stating that a GDPR violation does not automatically warrant compensation for damages, and that the individual must demonstrate real and certain harm, which they failed to do in this case.

The State Council's decision

The State Council **rejected** the claim for damages.

Our remarks

- According to GDPR, Article 82(1) *(right to material or non-material damage)*, a data subject has the right to receive compensation if they have suffered material or non-material damage as a result of a GDPR violation.
- Non-material damage in GDPR encompasses harm that is not monetary, including emotional distress or reputational harm caused by a violation of their data protection rights.
- It is important to note that mere discomfort or inconvenience resulting from a breach of the GDPR is not sufficient to warrant compensation. The damage caused must be real and certain. The data subject must prove that they have suffered actual and provable harm as a result of a specific breach of the GDPR.

Published: 01-04-2020, **Journal number:** 201902699/1/A **2 Tags:** 08 Compensation for non-material damages

Right to access bank documents

Summary

A data subject made a request to their former bank for all documents containing their personal data that had been processed.

The data subject specifically sought information about potential EVA registration (a Dutch fraud prevention system) and the bank's security affairs department's report.

However, the bank stated that it no longer had these documents due to exceeding retention periods. The bank did, however, offer to conduct an internal investigation.

District Court

The District Court rejected the data subject's request but allowed the bank to conduct an investigation and provide a report to the data subject. The data subject filed an appeal claiming that under GDPR, Article 15 they had the right to access complete copies of documentation containing their personal data, and that the bank had conducted multiple investigations into their activities. The bank argued that it no longer had the data as the retention period had lapsed.

The decision of the Court of Appeal

The Court of Appeal **rejected** the access request.

Our remarks

- Under Article 15 of the GDPR, individuals have the right to access their personal data, but this does not mean that they can demand full copies of all documentation containing their personal data, including underlying documents and personal notes made by others.
- Furthermore, a request for access may be rejected if it is deemed manifestly unfounded or excessive. This could be the case if the data subject submits requests for access every other week to harass or annoy an organization.
- If the organization chooses not to comply with a request, it must be able to demonstrate why the request is unfounded or excessive, and must still respond to the individual within one month of receiving the request. The organization must also explain the reasons for not complying with the request and inform the individual of their right to complain to the relevant supervisory authority and to seek a judicial remedy.

Does the right to access also extend to exams and comments?

Summary

A student who had studied at The IHE Delft Institute for Water Education from 2011 to 2013, and failed several exams, was informed by the institute that he could no longer successfully complete the degree. The student requested access to view his exams and was told that payment was required for copies of the exams.

The student then took the case to court and demanded that IHE granted access to the documents of 16 exams, including the examiner's written comments on answers to these examinations.

During the preliminary relief hearing, the judge informed both parties that the exams requested by the applicant, along with the examiner's comments on their answers, should be considered personal data under GDPR, Article 4(1).

The decision of the Court

The preliminary relief judge **ordered** that IHE must provide the student with copies of the 16 requested examinations and the examiner's written comments within three days of the date of the decision.

Our remarks

- Exams and comments from examiners can be regarded as personal data if it is possible to identify the data subjects involved.
- Data controllers cannot charge a fee for providing information requested by data subjects, unless the request is manifestly unfounded or excessive. An example of this is if the data subject requests access to an enormous amount of information.
- If the organization believes a request is excessive they may attempt to clarify the scope of the request with the individual to see if it can be narrowed down.

Mother's right to rectification regarding opinion on child's safety

Summary

Veilig Thuis, a public organization responsible for dealing with cases or suspicions of domestic violence or child abuse, received reports from a school about an 11-year-old with frequent absences. Veilig Thuis sent an email to the child's mother, stating that they had made an agreement with the obligatory education officer to be notified if the child's safety was jeopardized again or continued to be so. The mother requested that the word "again" be removed from the email and for the entire file to be erased. Veilig Thuis rejected both requests, leading the mother to bring the matter to court.

District Court

The District Court rejected the mother's appeal, stating that Veilig Thuis had a reasonable basis to judge that the child's substantial interest required the organization to save the data. The Court further stated that this substantial interest of saving the data outweighed the mother's interest in erasing it.

Appeal Court

Both the mother and Veilig Thuis appealed this decision. The Court of Appeal rejected the appeal, stating that Veilig Thuis processes personal data and carries out a task in the public interest and for reasons of public health. Therefore, the deletion request must be assessed on the basis of the Dutch Social Support Act 2015.

The decision of the Court of Appeal

The Court **confirmed** the District Court's decision, stating that the substantial interest of Veilig Thuis and the child outweighed the mother's interest.*

* the case is pending before the Dutch Supreme Court.

Our remarks

- Public organizations, such as Veilig Thuis, that deal with cases or suspicions of domestic violence or child abuse may process personal data and carry out tasks in the public interest and for reasons of public health. Therefore, the rules governing the processing of personal data, such as the GDPR, must be considered in conjunction with the applicable legislation.

- The right to erasure under the GDPR is not absolute, and the interests of the data subject must be balanced against the interests of the controller. In this specific case, the Court of Appeal found that the substantial interest of Veilig Thuis in maintaining the data outweighed the interest of the mother in having it erased. Therefore, it is important to understand that the right to erasure is not always applicable and must be balanced against the interests of all the parties involved.

- Additionally, the right to rectification under the GDPR does not extend to correcting or removing impressions, opinions, research results, and conclusions with which the data subject does not agree. This means that controllers may still hold personal data that is accurate and reflects their assessments and opinions, even if the data subject does not agree with them.

- Lastly, it is essential to consider the best interests of the child when making decisions that affect them, particularly in cases involving child welfare and protection. In some cases, the interests of the child's legal representative, such as a parent or guardian, may not align with the best interests of the child. Therefore, it is crucial to prioritize the welfare of the child when making decisions that could impact their safety and well-being.

Uber, right to access and data portability

Summary

In 2018, a group of Uber drivers from the United Kingdom submitted requests to access their data to Uber.

The drivers were affiliated with the App Drivers & Couriers Union (ADCU), a trade union representing the interests of private hire drivers and couriers in the UK. ADCU was affiliated with the International Alliance of App Transport Workers (IAATW), which sought to establish a database to ensure the trustworthiness of data for gig workers.

However, Uber denied to provide the full information about the drivers, which led them to sue Uber in the District Court of Amsterdam, where Uber had its headquarters.

Uber argued, in its defense, that the drivers were abusing the law within the Dutch Civil Code by requesting access to the data. Uber claimed that the applicant would misuse the right to access to establish a database containing data from drivers, and that the database would serve as unlawful means of retaliation in the case against Uber.

Request for access

Overall, the drivers wanted to know how Uber used their personal data and how the company's algorithms made decisions about their work. This included an assessment of eight different types of data.

Automated decision

Based on their request for access, the drivers wanted to establish that they were subjected to automated decisions within the meaning of GDPR, Article 22, so that they would be entitled to receive information about how the automated decision was made.

Uber used automated data processing to allocate available rides through the "batch matching system". The system grouped the nearest drivers and passengers in a batch and determined the optimal match within that group between a driver and a passenger.

Right to data portability

The drivers required Uber to provide the personal data specifically in a CVS file.

In summary, the Court had to decide on the following:

- If different types of information were personal data. If so, whether Uber had to grant access to this information
- Whether Uber had properly complied with the requests for data portability
- If the processing of personal data about the drivers carried out by Uber constituted an automated decision within the meaning of GDPR, Article 22

The decision of the Court of Amsterdam

Request for access (GDPR, Article 15)

The Court of Amsterdam ordered Uber to provide access to the drivers in accordance with the findings in the case. The specific data were evaluated as follows:

- **Driver's profile:** Uber's internal referrals and reports to customer service employees did not qualify as "profiles" under GDPR, Article 4(4) and did not contain verifiable personal data, thus not subject to GDPR access requests.
- **Tags:** The Court defined a tag as a description used by Uber to assess driver behavior that cannot be verified by the data subject and, therefore, is not subject to access requests.
- **Passenger feedback reports:** The Court deemed these as personal data but required anonymization to protect the rights of others under GDPR, Article 15(4), and Uber did not have to provide further access to the passengers' details based on the contractual relationship.
- **Start and end location of a trip:** The Court found Uber's overviews of journey times and locations sufficient for access requests, preventing potential privacy rights infringements.

- **Individual ratings:** Uber was ordered provide an anonymized overview of individual ratings.
- **Driving behavior and use of phone during trips:** The drivers' requests were too vague, and their claim was incomprehensible due to a lack of information.

- **Upfront pricing system:** Only one plaintiff was subjected to this new system, so the others could not request information about it under GDPR, Article 15.

- **Automated decision-making and profiling:** The Court agreed with Uber's argument that the company does not use automated decision-making under Article 22, even though Uber uses automated decisions. Therefore, the Court rejected the request for further information under Article 15(1)(h). See also "Automated decision making" in this section.

- **Request for additional information:** As Uber provided further information on processing purposes, categories of data, recipients of data, retention periods, and appropriate safeguards in its defense, the Court considered the question already resolved.

Right to data portability (GDPR, Article 20)

The Court **ordered** Uber to provide the data covered by the request for data portability in another format than PDF. However, it did not have to be a CVS file.

Automated decision-making (GDPR, Article 22)

The Court found that their anti-fraud process did not constitute automated decision-making as there was human intervention.

The automatic decision that happened in the "batch matching system" was an automated decision, but did not impose on the drivers any legal consequences or significant effect. Therefore, it was not covered by GPDR, Article 22(2) and Uber did not have to provide the information mentioned in 15(1)(h).

Our remarks

Request for access

- A data subject does not have to provide a reason or justification for submitting an access request under the GDPR. In this case, the Uber drivers did not need to specify a particular interest or state the purpose they wished to achieve with the inspection. The mere fact that personal data was being processed was sufficient.

- A data controller is on the other hand entitled to ask for specifications on the type of personal data that the data subject requests access to. This is especially the case if the data subject has submitted a general request for access.

- When providing access, the data controller also has to observe the rights to privacy of others than the data subject submitting the request. For example, when providing access, Uber was required to anonymize the reports based on feedback from passengers in order to respect the rights and freedoms of the passengers.

Data portability

- The right to data portability means that the data subject has the right to receive a copy of their personal data from a company and transfer it to another company in a format that can be easily read by machines. It is normally viewed as being useful for customers, for example, if they want to change bank or telephone operator, but the case shows that it also can be relevant in employment based relationships.

- If there are no specific common formats within a certain industry, then there is no obligation for the data controller to provide the data in a certain type of file, as long as they provide the data in any commonly used public formats like XML, JSON, CSV.

- Providing personal data in PDF-files is not a way of complying with the right to data portability as the personal data in such a file is not structured or descriptive enough for the reuse of the data.

Automated decision-making

- It is important for data subjects to know if they have been subject to automated decision-making under GDPR, Article 22, because such decisions can have significant legal or other effects on individuals. Data subjects have the right to be informed about the logic involved in any automated decision-making process, as well as the significance and consequences of such processing. Furthermore, they have the right not to be subject to a solely automated decision.
- If there is any kind of human interference within a process, the processing will never be an automated decision within the meaning of GDPR, Article 22.
- If an automated decision has no legal consequence, it should be assessed if it has a "similarly significant" effect. Even though the "batched matching system" did have a certain effect on the performance of the agreement between Uber and the driver, meaning the possibility of the driver to earn money, it was found that the batch making system did not have a "similarly significant" effect on the data subject.
- This must be viewed as an edge case, and maybe it was ruled like this as the automated process was about the drivers in groups, and therefore the automated process was not deemed so intrusive for the rights of the driver as an individual.

Largest fines - Germany

03

H&M fined for insufficient legal basis for processing sensitive personal data

Summary

Several hundred employees of an H&M Service Center in Nuremberg had since 2014 been subject to extensive recording of information regarding their private lives, including symptoms of illness, diagnoses, romantic relationships and religious beliefs.

The data was collected through a 'Welcome Back Talk' for all employees returning from vacation or illness, and through office gossip. The data was permanently stored on a local network, which was accessible by up to 50 managers of the company.

The data was, in some cases, continuously updated and used to evaluate the performance of the workers and ultimately in employment decisions.

The affected individuals were unaware of the systemic recording of their personal data until it was discovered due to a technical error in October 2019. The technical error made the information available company-wide for hours. As a result of the incident, protective measures were introduced, and the company explicitly apologized to the affected employees. The DPA suggested offering monetary compensation which was accepted and actioned by H&M.

The decision of The Hamburg Commissioner for Data Protection and Freedom of Information

The DPA **fined** H&M **35,300,000** EUR for the following violations:

- Not having a legal basis for the recording of special categories of personal data
- Not adhering to the principles of data minimization and storage limitation

Additionally, the DPA suggested remedial actions towards the affected employees.

Our remarks

- If a data controller wants to record employee data, they should ensure that they have an appropriate legal basis. This could, for example, be the performance of a contract between the employer and employee, or compliance with a legal obligation. If data processing is not covered by these grounds, another legal basis, such as consent or legitimate interests, must be established.
- When collecting personal data about employees it is important to limit any processing of special categories of personal data to a minimum. The data controller should ensure that they fulfill one of the requirements in GDPR, Article 9(2). Recording personal data about employees' diagnoses or romantic relationships qualifies as processing of special categories of personal data.
- When processing and storing data concerning employees, it is essential to adhere to the principles of data minimization and storage limitation, as well as the principles of lawfulness, fairness and transparency. Before processing employee data, the employer should consider which data is necessary for the legitimate purpose of the processing, or for the fulfillment or performance of a contract to which the employer is a party. This can for example be ensured by having internal guidelines for the collection of personal data, erasure policies and so forth.
- The Hamburg Commissioner did not specifically mention compensation under GDPR, Article 82. H&M's voluntary remedial actions in response demonstrate a growing awareness of corporate responsibility regarding employee privacy. Similarly, the size of the fine highlights the employer's extensive responsibility in ensuring employee privacy.

Published: 01-10-2020 **Journal number:** N/A **Tags:** 01 Legal basis and principles of processing, 03 Right to erasure and rectification

Notebooksbilliger.de fined for lack of legal basis for video surveillance

Summary

For at least two years, the company Notebooksbilliger.de monitored both customers and employees in a range of areas, including sales, warehouses, and common spaces. The company claimed that the purpose of the monitoring was to prevent and resolve criminal activities such as theft, as well as tracking the flow of goods in the warehouses.

The monitoring was not limited to a specific timeframe or to specific conditions. In many cases, the records were stored for 60 days. Additionally, the Lower Saxony DPA (LfD Lower Saxony) noted that the monitoring was not based on suspicion towards specific individuals.

The DPA also found that some cameras were positioned to observe seating areas in the salesroom. Since seating areas typically encourage customers to get comfortable and stay for extended periods, such as when testing devices on offer, it could also potentially result in the observation and analysis of a person's entire behavior.

The decision of the State Commissioner for Data Protection Lower Saxony

The DPA **imposed** a fine of **10,400,000** EUR to Notebooksbilliger.de AG for the following violations:

- Monitoring their employees and customers without sufficient legal basis for doing so *(GDPR, Article 6(1))*.
- Not adhering to the principles of data minimization, storage limitation and proportionality.

Additionally, the DPA suggested remedial actions towards the affected employees.

Our remarks

- When an employer considers video monitoring of the workplace, they should consider what legal basis the data processing should rely on:
  - The inherent power imbalance between employers and employees means that consent is unlikely to be freely given. Therefore, employers should avoid using consent as a legal basis for processing personal data about employees.
  - Instead, legitimate interests would likely be a more appropriate legal basis for video surveillance of employees. If the legitimate interest is to prove a criminal act, there must be a well-documented reasonable suspicion against specific persons (e.g., recent criminal offence). General suspicion is not enough.
  - If you are considering monitoring workplace areas that are accessible to customers, a separate legitimate interest must apply. If the legitimate interest is to prove a criminal act by visitors or customers, there must be a real and current threat, such as a recent act of vandalism of neighboring shop or statistical proof of heightened crime risk in the area.
  - Such practices, both regarding employees and customers, should be reviewed at regular intervals to ensure the continuous necessity and proportionality of the processing.

Published: 08-01-2021, **Journal number:** n/a **Tags:** 01 Legal basis and principles of processing

- Video surveillance is considered a particularly intrusive form of data processing, as it potentially allows for observance and analysis of a person's entire behavior. Therefore, the employer should carefully ensure to respect the principles of fairness, transparency and proportionality.
    - When balancing the interests in question, the employer must ensure that the data processing is necessary and proportionate to the concerns raised. If a less intrusive method can achieve the same goal, the less intrusive method must be used. Consider other methods of risk mitigation than video surveillance (e.g., random bag checks).
- Finally, employers must consider the principle of data minimization by storing personal data for the minimum amount of time necessary and with a specified retention period. In the case in question, the DPA stated that 60 days was significantly longer than necessary.
- For further reading on processing personal data of employees, see A29WP Opinion 2/2017 on data processing at work or EDPB guidelines 3/2019 on processing of personal data by video devices.

1&1 Telecom GmBH fined for insufficient security measures

Summary

The federal DPA of Germany (BfDI) discovered that 1&1 Telecom's authentication practice allowed any caller who claimed to be a family member of a customer, and who could provide the customer's date of birth, to gain access to a range of personal data. Additionally, callers were able to change the customer's personal data, such as bank details.

As a result of this practice, an individual gained access to their previous partners' new telephone number. The person whose number was compromised had deliberately changed his phone number to avoid contact from their ex-partner. After notifying the police, the DPA was informed of the breach.

The authentication practice was not assessed for compliance with GDPR.

The decision of The Hamburg Commissioner for Data Protection and Freedom of Information

The DPA initially ruled that the authentication procedure violated the obligation to take appropriate technical and organizational measures to systemically protect the processing of personal data (GDPR, Article 32).

The District Court of LG Bonn **reduced the fine** from **9,550,000** EUR to **900,000** EUR for the following reasons:

- The District Court of LG Bonn upheld the DPA's decision that the calculation model, which considers turnover as an essential factor in determining the appropriate level of penalties, is appropriate for medium data protection violations under the GDPR.
- However, when it comes to a minor GDPR violation by companies with large turnovers (at group level or otherwise), the model would lead to disproportionately high fines, whilst conversely resulting in disproportionately low fines for severe GDPR violations by companies with low turnovers. The District Court states that the strong focus on annual turnover is problematic, especially in cases where the data breach was minor.

Our remarks

To prevent data breaches, it is important to implement appropriate organizational and technical measures. In the case at hand, a personal 'Service Pin' was introduced to provide an extra layer of security, that was sufficient for customer authentication.

- The data controller should assess the appropriateness of a safety measure by considering the state of the art and the costs of implementation, balanced against the risk and severity of potential impacts on the rights and freedoms of the individuals whose data is being processed *(GDPR, Article 32)*.
- When assessing the risks to the data subject's rights and freedoms, consider the possible negative consequences of a data breach, including unlawful access, alteration, or deletion of personal data. Special categories of personal data, such as ethnicity or political beliefs, generally imply a higher risk than ordinary personal data, such as customer number or e-mail address. However, some cases might infer high risks even to ordinary personal data, depending on the type and severity of the breach in conjunction with the type and context of the data processed.
- Taking effective actions to mitigate the damage of a breach will possibly affect the fine size positively.
- Notify the appropriate DPA about the nature of the breach, and if possible, the categories and amount of personal data and number of data subjects concerned. This notification should be done without undue delay.

If the data breach is likely to result in a high risk to the rights and freedoms of natural persons, the data subjects should be notified about the breach without undue delay. Effective cooperation with supervisory authorities may also have a positive impact on the size of the fine.

Brebau GmbH fined for for lack of legal basis and transparency

Summary

The housing and residential association Brebau GmbH processed sensitive data of over 9500 potential tenants. In more than half of the cases, the data collected included information about skin color, ethnic origin, religious beliefs, sexual orientation, health status of the data subjects and even physical appearance such as hairstyle and body odor.

In multiple cases, Brebau GmbH prevented data subjects from accessing their personal data and obtaining insight into how their data was processed.

The Decision of the State Commissioner for Data Protection Bremen

The DPA **fined** Brebau GmbH **1,900,000** EUR for the violation, stating that the extraordinarily severe nature of the violation allowed for an even higher fine than the one imposed. Brebau was fined for the following violations:

- Processing categories of personal data that were not necessary for the fulfillment of the contract.
- Not complying with the right to access *(GDPR, Article 15)* and principle of transparency *(GDPR, Article 5(1)(a))*

However, as Brebau GmbH cooperated willingly by mitigating the damage, clarifying the facts and ensuring that no such violations would be repeated, the DPA reduced the amount of the fine.

Our remarks

The processing of special categories of personal data such as skin color, ethnic origin, etc. is not necessary for fulfilling rental agreements and therefore, such processing is considered unlawful. Assessing which personal data categories are necessary for processing ensures compliance with GDPR regulations. As a data controller, it is essential to implement efficient and accessible transparency practices to uphold the data subjects' right to access. The data subject must upon request be able to access information on *(see GDPR, Article 15 for an exhaustive list)*:

- The purposes of the processing,
- The categories of personal data concerned,
- Third party recipients or categories of recipients of personal data,
- The existence of the right to rectification and the right to erasure, and the right to complaint with a DPA.

Published: 03-03-2022 **Journal number:** n/a
Tags: 01 Legal Basis and principles of processing, 02 right to access and obligation to provide information

AOK Baden-Württemberg fined for failing to security of processing

Summary

The health insurance company AOK Baden-Württemberg hosted competitions on various occasions between 2015 and 2019, where personal data such as contact information and health insurance affiliation was collected. AOK wanted to use this information for advertising purposes if the participants had consented accordingly.

For this purpose, AOK implemented various technical and organizational measures including internal guidelines and data protection training to ensure that only those who had given their valid consent to the processing received advertisement material. However, the measures taken were not sufficient, resulting in over 500 raffle participants' personal data being used for advertising purposes. No insurance data was concerned.

As soon as the allegations came to light, AOK immediately discontinued all sales activities.

The Decision of the DPA

The DPA (LfDI) **fined** AOK Baden-Wuerttemberg **1,200,000** EUR for not meeting the requirements for technical and organizational measures to ensure secure data processing *(GDPR, Article 32)*.

During the investigation, AOK conducted comprehensive internal reviews and adjusted their technical and organizational measures. Their cooperation with the DPA also resulted in a reduction in the amount of the fine.

Our remarks

- Ensure that internal data protection guidelines and training include the principle of integrity and confidentiality, as well as the legal requirements as stated in GDPR, Article 32.
- When doing so, assess the level of risk to the data subjects' rights and freedoms in the processing of personal data to ensure a level of security appropriate to this risk.
- Appropriate measures to ensure security of processing personal data include, but are not limited to (see GDPR, Article 32 for exhaustive list):
  - Pseudonymization and encryption of personal data.
  - Ensuring ongoing confidentiality, integrity and resilience of processing systems.
  - The ability to restore availability and access in a timely manner in case of incidents.
  - A process of testing, assessing and evaluating the effectiveness of these technical and organizational measures.

Volkswagen fined for not providing data subjects sufficient information about the data processing

Summary

The police stopped a vehicle for a traffic check near Salzburg (Austria), as the police officers noticed unusual attachments to the vehicle that turned out to be cameras. The vehicle was part of a research program that tested and trained a driver assistance system in order to further avoid traffic accidents.

Among other things, the vehicle recorded the surrounding traffic for error analysis. The research trip was carried out by a service provider on behalf of Volkswagen. Due to an accident, the vehicle was missing magnetic signs that were meant to inform other road users about the recording.

Even though the data processing took place in Austria, The State Commissioner for Data Protection (LfD) in Lower Saxony handled the case as Volkswagen, the controller of the processing of personal data, is primarily situated in Germany.

The Decision of the State Commissioner for Data Protection (LfD) Lower Saxony

The DPA **imposed** a fine of **1,1 mio** EUR for the following violations:

- Not providing the other road users sufficient information about the processing *(GDPR, Article 13)*.
- Not concluding a data processing agreement with the company that carried out the testing *(GDPR, Article 28)*.
- Not maintaining a record of processing activities *(GDPR, Article 30)*.
- Not carrying out a data protection impact assessment (GDPR, Article 35).

All four violations were 'low severity'. Additionally, the DPA took into account that the processing served to optimize the driving assistant system, thus improving road safety.

Our remarks

- When collecting data from the data subject through capturing video, make sure to properly inform the data subject of the nature and purpose of the processing as well as their rights. This ensures fair and transparent processing. In the case in question, a sign on the car containing a camera symbol as well as the mandatory information is likely to be adequate.
    - Note: This practice differs from Danish DPA decisions, in which personal data collected through video surveillance is regulated through GDPR, Article 14, thereby allowing for the exemption from the obligation to inform the data subject, if doing so proves impossible or involves a disproportionate effort. This would likely be the case when the data subjects are road users.
- Any processing of personal data carried out on the behalf of a controller must rely on a data processing agreement. The processor must prove appropriate technical and organizational measures to ensure compliance with the GDPR, and the data processing agreement must be clear and comprehensive.
- Make sure to keep record of all processing activities containing the purpose of the processing, a description of categories of personal data, the categories of third-party disclosures, third country transfers, envisaged time limits for erasure and, where possible, a general description of technical and organizational security measures.
- When processing is likely to result in a high risk to the rights and freedoms of the data subjects, performing a data protection impact assessment (DPIA) is required. While the case in question does not specify why the data processing was 'likely to result in a high risk to the rights and freedoms of natural persons', the use of new technologies (e.g., the use of new technologies in innovative ways or the use of new technologies in combination) is generally an indicator that a DPIA would be necessary. A DPIA should at least contain:
    - A description of the envisaged processing operations including purposes and, where applicable, legitimate interests,
    - An assessment of the necessity and proportionality,
    - An assessment of the risks of the rights and freedoms of data subjects,
    - The measures envisaged to address these risks.
- Seek advice with your designated Data Protection Authority when performing a DPIA.

Bank fined for creating costumer profiles without a legal basis

Summary

A commercial bank*, acting as the controller, used personal data of both current and former customers to identify those with a preference for digital media usage. The customer profiles were created to target them with intense electronic communications for commercial purposes, in the form of advertisements.

To carry out this analysis, a service provider was hired to analyze digital usage behavior including app-store purchases, frequency of bank statement printers' usage, and online banking transfers. This data was compared to offline usage at local branch offices and further enriched with data from a commercial credit reporting agency. Although most customers were notified in advance, the controller did not obtain consent from the data subjects.

The bank relied on legitimate interests, in the form of direct marketing, as the basis for the processing of data, analysis, and creation of customer profiles.

*Possibly Hannoversche Volksbank. This is not confirmed by the DPA.

The Decision of the DPA

The LfD Lower Saxony **fined** the bank **900,000** EUR for the following violations:

- The bank's analysis of large amounts of data to create customer profiles could not be based on legitimate interests as it did not properly balance its interests with the fundamental rights and freedoms of the data subject *(GDPR, Article 6(1)(f))*.

- The data subject could not reasonably expect their personal data to be analyzed on such a large scale for targeted advertising. The bank could not invoke a weighing of interests and should have obtained consent for the processing.

- The use of third-party data enrichment, such as data from a commercial credit reporting agency to create precise profiles, weighs heavily in favor of the rights and freedoms of the data subject in a balancing of interests. Thus, consent should have been obtained.

Note: The DPA press release states that the decision is not final. However, as no appeal was made within the two-week appeal period, the decision is now considered final.

Our remarks

- When basing the data processing on a legitimate interest such as direct marketing, perform a balancing test to weigh the legitimate interest of the data processing against the fundamental rights and freedoms of the data subjects.

    - While it might not be obvious what the specific interests of the data subject are, it's crucial to consider their reasonable expectations. Do these reasonable expectations align with your legitimate interests? In the case in question, third-party enrichments to create precise profiles and the use of large databases for advertisement purposes both exceeded what could be considered reasonable expectations.

- Ensure that any third-party data enrichment is based on a legal basis. In the case in question, consent should have been obtained. As third-party enrichments allow for collection of data from different areas of life, potentially creating very precise profiles, it's important to carefully consider the implications of the data processing and choose a legal basis accordingly. Also keep in mind the principles of data minimization and transparency.

Vatenfall Europe Sales GmbH fined for not fulfilling transparency obligations

Summary

Vattenfall Europe Sales GmbH offered its customers especially beneficial contracts that involved a payout to customers. To avoid making these deals unprofitable, the company conducted routine reviews of contract inquiries for "behavior conspicuous for switching". To do so, Vattenfall utilized invoices from around 500,000 previous customers, effectively cross-referencing this information with the data obtained from the inquiries. However, the company did not inform new or existing customers about this data reconciliation process or its purpose.

The company cooperated extensively with the DPA throughout the investigation process.

The Decision of the DPA

The DPA's investigation focused solely on the matter of information obligations and did not assess whether the data reconciliation itself was permissible.

The DPA **fined** Vattenfall Europe **900,000** EUR for the following violations:

- Not providing data subjects information about their rights as data subjects in relation to the data processing *(GDPR, Article 12)*.
- Not providing data subjects with information about the nature of the processing of their personal data or the purpose of the processing *(GDPR, Article 13)*.

The fine was significantly reduced due to Vattenfall's extensive and immediate cooperation with the DPA.

Our remarks

- When processing personal data, make sure to inform your data subjects of their rights under the GDPR, including:
  - The right to be informed,
  - The right to access,
  - The right to rectification and erasure,
  - The right to restriction of processing,
  - The right to data portability,
  - The right to object,
  - The right to not be subject to automated decision-making, including profiling.
- In accordance with the right to be informed, data controllers should inform the data subject about the data processing itself, including:
  - The identity and contact details of the data controller and the DPO (if applicable),
  - The purpose of the processing and the legal basis for the processing,
  - The categories of data being processed, as well as the purposes of the processing,
  - The recipients or categories of recipients who will have access to the personal data,
  - Where processing is based on consent, the right to withdraw the consent.
- When the data is collected from the data subject, the data subject should, when possible, be informed at the time of the collection.

Published: 24-09-2021 **Journal number:** N/A **Tags:** 02 Right to access and obligation to provide information.

Berlin e-commerce group fined for DPO conflict of interest

Summary

A Berlin-based e-commerce retail group appointed a Data Protection Officer (DPO) who also served as the managing director of two service companies that processed data on behalf of the controller. The two service companies were part of the same group and were responsible for customer service and order fulfillment.

As part of their legal obligations, the DPO was responsible for ensuring compliance with data protection laws by the service companies and making managerial decisions within them.

In 2021, the German DPA issued a warning to the controller for violating data protection laws. Despite a subsequent inspection, it was found that the violation persisted.

The Decision of the DPA*

The BlnBDI (DPA) **fined** the e-commerce retail group **525,000** EUR for the following violation:

- Failing to ensure that the tasks assigned to the DPO did not result in a conflict of interest *(GDPR, Article 37(6)).*

When imposing the fine, the DPA considered the controller's high turnover in the previous financial year, the DPO's role as the point of contact for both employees and customers, and the controller's deliberate continuation of the violation despite warnings. However, the controller cooperated fully with the DPA and stopped the violation during the ongoing fine proceedings, resulting in a reduced overall fine.

*The decision is not yet final.

Published: 20-09-2022 **Journal number:** N/A **Tags:** 01 Legal basis and principles of processing

Our remarks

- The independence of the DPO is critical in ensuring compliance. Monitoring one's own decisions is incompatible with the role of a DPO, who must act independently of the controller or processor. To avoid risking a conflict of interest when appointing or instructing a Data Protection Officer, and to generally ensure a compliant DPO practice, consider the following:
    - The DPO cannot be responsible for the processing activities of the data controller or processor, as this would not fulfill the requirement for independence. Therefore, a DPO typically cannot hold the position of the top IT or HR executive in an organization. Instead, an employee who does not have ultimate responsibility for these areas may be appointed as DPO.
    - Although a DPO may fulfill other tasks and duties beyond those of the DPO role, the controller must ensure that these additional tasks do not lead to a conflict of interest for the DPO.
    - The tasks and duties of the DPO should be regularly reviewed to ensure they remain independent and not in conflict with other responsibilities within the organization.
    - Data controllers should establish a reporting mechanism that allows employees to report any concerns about the DPO's independence or conflicts of interest.
    - The DPO should have direct access to the highest management level and should not receive any instructions regarding the exercise of their tasks.
    - The controller should ensure that the DPO is properly involved and informed in a timely manner about all issues which relate to the protection of personal data.
    - The DPO should be provided with adequate resources to enable them to perform their tasks effectively and independently.

VfB Stuttgart fined for neglecting the accountability principle

Summary

Between 2016 and 2017, VfB Stuttgart 1893 e.V., a registered association under German law, transferred tens of thousands of personal data records belonging to club members to an external service provider. The purpose of this transfer was to enable the spin-off of the professional soccer department into a stock corporation named "VfB Stuttgart 1893 AG". The data included information on underage members who would have turned 18 at the time of a general meeting where the spin-off decision was made.

Furthermore, after the GDPR came into effect, the soccer club shared an Excel spreadsheet containing over 100,000 data records with the service provider.

VfB Stuttgart did not provide a contractual basis for their partnership with the service provider. They had not documented who initially commissioned the service provider, the specific powers it held within VfB Stuttgart, or the extent of its access to the personal data of members and employees.

The Decision of the DPA

The LfDI (DPA) limited the proceedings to a violation of the principle of accountability and provisionally terminated any further proceedings concerning potential other violations of the GDPR. The DPA **fined** VfB Stuttgart 1893 **300,000** EUR for the following violation:

- Lack of a contractual relationship with the external service provider and its authority within the club. Consequently, the legitimacy of the data processing activities could not be adequately verified or proven, which was a breach of the principle of accountability *(GDPR, Article 5(2))*.

Our remarks

- Compliance with the GDPR's accountability principle is important to keep in mind when processing personal data. You must be able to provide evidence of compliance upon request by the relevant supervisory authority. Make sure that you can provide the Data Protection Authority with the following:
  - Detailed and up-to-date documentation of your data processing activities, including the legal basis for processing, the purposes of processing, the categories of data subjects and personal data processed, the recipients of personal data, the retention period, and the security measures employed.
  - Appropriate policies, procedures, and where applicable, codes of conduct to demonstrate compliance with the GDPR's principles, including data minimization, accuracy, integrity, and confidentiality. This may involve conducting regular data protection impact assessments, reviewing and updating data processing agreements with third-party service providers, and ensuring that employees are adequately trained on GDPR compliance.
  - Documentation of which appropriate technical and organizational measures to ensure the security of personal data and prevent unauthorized access or disclosure. This includes maintaining confidentiality and integrity of data, providing regular training to staff members, and conducting regular audits of data protection processes.

Published: 10-03-2021 **Journal number:** 0623.1-2/3 **Tags:** 01 Legal Basis and principles of data processing, 04 Data processing agreements and supervision of data processors and sub-processors.

Selected interesting cases – Germany

04

Scalable Capital ordered to compensate data subject for non-material damages

Summary

Upon registration as a customer at Scalable Capital, individuals provided a range of personal data that was later compromised in a data breach. Attackers were able to gain access to Scalable Capital's entire IT system by acquiring access information from the firm's former IT service provider, CodeShip Inc. As a result, the attackers gained access to a range of personal data, including the data subjects' first and last name, title, address, email address, mobile phone number, nationality, marital status, tax residence and tax ID, IBAN, copy of identity card, and portrait photo. These third parties accessed the data on three separate occasions between April and October 2020, stealing a total of 389,000 records from 33,200 affected individuals.

Although CodeShip Inc. had ceased providing IT services to Scalable Capital in late 2015, the access data to Scalable Capital's system had never been changed. The stolen personal data was subsequently used to obtain loans and was also offered for sale on the dark web.

The Decision of the Court of LG Bonn

The Court of LG Bonn **ordered the controller to pay 2,500 EUR** to the data subject for the following violations:

- The controller failed to implement organizational measures to ensure an appropriate level of data protection by not excluding CodeShip from access to their digital document archives immediately after the termination of their business relationship *(GPDR, Articles 31(1) and 5(1)(f))*.
- The Court found that the data breach had caused non-material damage to the affected individuals, such as feelings of uncertainty, loss of trust, and anxiety about potential misuse of their personal data.

Therefore, the Court ordered compensation for non-material damage *(GDPR, Article 82(1))*.

Our remarks

- The case signifies that the German Court applies a broad interpretation of the right to compensation for non-material damages. A data controller could be held liable for such damages that might result from a data breach within its responsibility.
- When doing a risk assessment, take into account the nature and severity of a possible infringement.
- In this case, even though there was no evidence of existing fraud or misuse of the personal data, the personal data involved in the breach was so comprehensive that the risk for future material damage was taken into account.
- To avoid being held liable for inflicting non-material damages or the risk of future material damages as a result of a data breach, it is important to ensure adequacy of technical and organizational security measures:
    - Make sure that only current third-party business relations have access to your systems. Conduct regular security assessments and penetration testing to identify vulnerabilities in your system and organization (including partners) and implement adequate measures to address them.
    - Monitor access to personal data, limit it to authorized personnel (internally as well as regarding third parties), and revoke access for those who no longer require access.

Company ordered to cover repair costs for customer

Summary

A German company used Mailchimp as a newsletter tool. A data subject claimed that transferring email addresses of the company's newsletter subscribers to Mailchimp, which is a US-based company, constituted an unlawful third-country transfer pursuant to the GPPR.

The Decision of the Bavarian State Office for Data Protection Supervision (BayLDA)

As the company informed the DPA that it had used Mailchimp only twice and confirmed that it would stop using the service with immediate effect, and as the final EDPB guidelines on the supplementary measures for transfers of personal data to third countries were not yet finalized, the DPA **did not impose a fine or take any other enforcement actions.**

Our remarks

- When using services that require transfers to third countries, first see if the country in question has received an adequacy decision from the European Commission. Data transfer to these countries is expressly permitted. The countries that have received adequacy decisions are:
    - Andorra, Argentina, Canada (only commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, Japan, the United Kingdom and South Korea.
- When transferring data to unsecure third countries, conduct a Transfer Impact Assessment (TIA) to assess the adequacy of the data protection level of the data importer to ensure EU level protection of personal data. Data controllers must take the wording of the SCCs (Standard Contractual Clauses) and the legal system of the third country into account, in particular with regards to access to the transferred data by public authorities (such as intelligence services) in the third country.
- Depending on the outcome of this assessment, the data exporter and the data importer may be required to implement and prove adequate supplementary measures in order to safeguard the data.
- For this purpose, if the data importer does not require 'data in the clear', you can implement effective encryption as a supplementary measure. (See ComplyCloud Transfer Roadmap for an exhaustive overview)
    - Data must be subject to transfer encryption prior to transfer on the 'data layer'.
    - The encryption must be 'state-of-the-art'.
    - The encryption keys must be reliably managed (must be kept under the sole control of trusted parties in the EEA or a country which offers an essentially equivalent protection).
    - 'Backdoors' must be excluded.
- If the importer needs the data in the clear, you must demonstrate and document that you have no reason to believe that relevant and problematic legislation will be applied in practice.
    - To rely on a 'no reason to believe'-assessment, you must be able to demonstrate and document that the law is not interpreted and/or applied in practice to cover your transferred data and importer (for a list of possible sources of information, see EDPB recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data paragraphs 44-47).
- At appropriate intervals, evaluate the level of protection afforded to the personal data you transfer to third countries and monitor if there have been or there will be any legal developments that may affect it.

Published: 15-3-2021 **Journal number:** LDA-1085.1-12159/20-IDV **Tags:** 06 Transfers to third countries

- To ensure compliant third country transfers, and to further your understanding of the European data transfer regime after Schrems II, see the ComplyCloud **Transfer Roadmap whitepaper** on our webpage under 'academy' -> 'downloads'-> Transfer Roadmap.

Please note that this decision was made prior to the EU Commission's adoption of the EU-U.S. Data Privacy Framework. The framework solves the challenges of the SCHREMS II case and thereby ensures that entities in the EU can transfer personal data to entities in the US that comply with the framework without conducting a TIA. However, general considerations concerning the transfer of personal data to other unsafe third countries still apply.

Insurance company ordered to cover the cost of repairs for a customer

Summary

A customer of a health insurance company experienced an increase in his premiums. Subsequently, after paying the premium for a period, he requested a refund, as well as access to all supplementary documents related to the insurance policy and notification letters sent to him during the contractual relationship.

The Regional Court of Aachen ruled in favor of the data subject in the initial hearing. However, the controller (the insurance company) appealed the decision, arguing that GDPR, Article 15 only requires transparency of processed data and does not grant access to documents. The controller further contended that granting access to such a wide range of documents would be an impermissible discovery of evidence, contrary to the principle of civil procedural law. Lastly, the controller claimed that the data subject's request was excessive under GDPR, Article 12(5) as it was meant to verify the validity of premium increases, not the lawfulness of the processing.

The Decision of the Higher Regional Court of Köln (OLG Köln)

OLG Köln rejected the controller's arguments, **ordering them to pay and cover the cost of repairs to the data subject (~2000 EUR) as well as providing access to the documents in question** with the following holdings:

- The Court found that the right to a copy is independent from the right to access and gives the data subject a right to a copy of the data in its raw form *(GDPR, Articles 15(1) and 15(3))*.
- The Court rejected the controller's arguments that the request was excessive under German Civil Code or *GDPR, Article 12(5)*. It reasoned that the overall purpose of the GDPR is to protect all rights and freedoms of the individual against harm and risks arising from the processing of personal data, not just those enshrined in data protection law.
- The Court concluded that the data subject has a legitimate interest in using GDPR, Article 15(3) to reduce an asymmetric level of information between themselves and the controller to protect their rights. Moreover, the Court noted that the right to access must not depend on an unverifiable assertion about the inner motivation of a data subject.

Our remarks

- The right to access is independent of the right to a copy of the data and should be construed extensively to provide individuals with a complete picture of how their data is being used.
- Controllers cannot reject a request for access unless it is excessive or unfounded and must provide access to any supplementary information related to the data. Be aware that the burden of proof that a request is excessive lies with you as the controller.
- Data controllers must not restrict or limit the right to access based on the motivation or purpose of the request and must consider the overall purpose of the GDPR to protect the rights and freedoms of individuals in relation to their personal data.
    - Be aware, however, that even though this case is conclusive and persuasive, it differs from other cases. For example, the Danish DPA has, in a similar case, ruled that a father could not gain access to the data processed about his daughter at a sports club, since his motivation was not to secure the lawfulness of the data processing, but to gain access to his daughters dancing class schedule. Link to article.

Data subject awarded reparation after unlawful transfer of IP addresses

Summary

The controller, an unnamed German company, incorporated Google Fonts into their website, resulting in the automatic transmission of the data subject's dynamic IP address to Google's servers located in the United States.

The Decision of LG Munich

LG Munich **awarded the data subject 100 EUR in reparations**, as it found the data controller in breach of the following violations:

- The Court found that a **dynamic IP address was to be considered as personal data** as the controller had an abstract opportunity to identify the data subject *(GDPR, Article 4(1)).*
- The Court found the transfer of the IP address to Google without the consent of the data subject to be unlawful *(GDPR, Article 6(1)(a))*.
- The Court also held that the infringement is not justified as necessary for the purpose of the legitimate interests pursued by the controller, since Google Fonts could be used without having a connection to Google's servers *(GDPR, Article 6(1)(f)*.
- The Court held that the term 'damages' in *GDPR, Article 82(1)* is to be understood broadly, including to prevent future violations in cases of risk of repetition.

Our remarks

- The transfer of personal data, including IP addresses to third-party services such as Google Fonts should only be done with the explicit and informed consent of the data subject.
    - Don't forget to conduct a TIA (See Mailchimp case and our Transfer Roadmap whitepaper).
- Controllers should take into consideration the broad interpretation of the term "damages" in GDPR, Article 82(1), which aims to sanction data protection violations and prevent future ones.
- The risk of repetition is factually presumed when a violation of rights has been established, and controllers should take active measures to prevent further violations from occurring.

Please note that this decision was made prior to the EU Commission's adoption of the EU-U.S. Data Privacy Framework. The framework solves the challenges of the SCHREMS II case and thereby ensures that entities in the EU can transfer personal data to entities in the US that comply with the framework without conducting a TIA. However, general considerations concerning the transfer of personal data to other unsafe third countries still apply.

Data subject awarded damages for unauthorized criminal background check

Summary

The data subject sought membership in an association, and the association's managing director instructed a background check to be carried out on the individual. The investigation uncovered information on the individual's past criminal convictions, which was then relayed to the association's executive board. Subsequently, the association rejected the individual's membership application. The data subject argued that the controller had breached GDPR, Article 10, since the processing of their personal data related to criminal convictions did not occur under official supervision. Consequently, they demanded compensation for pain and suffering.

The Decision of the Higher Regional Court of Dresden

The Higher Regional Court upheld the decision of the Regional Court of Dresden, **awarding the data subject damages in the amount of 5,000 EUR** for the following violations:

- The processing was deemed unnecessary because the controller could have used less intrusive alternatives like self-disclosure or police clearance certificates.
- In terms of liability, the Court found that the managing director was to be considered a controller alongside the company *(GDPR, Article 4(7))*.
- When assessing the non-material damages under GDPR, Article 82, the Court considered the nature, gravity, duration, degree of fault and measures taken to mitigate harm, previous breaches, and categories of personal data. In this instance, the Court found that the breach exceeded the *de minimis* threshold despite it being a one-time event. The sensitive nature of the personal data collected and disclosed affected the interests of the data subject, which was why the damages already awarded in the amount of 5.000 were deemed appropriate.

Our remarks

- Personal liability can apply to managing directors. The case shows that managing directors can be held personally liable for breaches of GDPR if they are found to have acted intentionally or negligently in violation of the GDPR.
- Personal data relating to criminal convictions must be processed under official supervision. Collection must happen under official supervision, as required by GDPR, Article 10. This supervision may be provided by a public authority or by a person or body authorized by EU or Member State law.

Published: 30-11-2022 **Journal number:** N/A **Tags:** 07 Compensation for non-material damages

Data Processor's promises regarding third-country transfer were valid

Summary

A Europe-wide invitation to tender for the procurement of a digital healthcare patient discharge management software system included a criterion that any data processing had to be conducted in a data center situated in the EEA, and that no subcontractor should be located in third countries. The tender was won by Company A, which had an EU subsidiary serving as a subcontractor (data processor) and was incorporated in the US as a parent entity. The complainant, Company B, which was also a part of the tender process, argued that company A should be excluded from the procurement as its subcontractor posed a potential risk, in that US governmental bodies could gain access to the personal data on the EU servers.

The Baden-Württemberg Public Procurement Chamber agreed with the complainant, arguing that the use of the subcontractor, and its inherent risk, constituted a transfer within the meaning of GDPR, Article 44.

The decision was appealed. Additionally, the Baden-Württemberg DPA criticized the decision, noting that the decision did not factor in the possibility for parties to implement technical and organizational measures to reduce or eliminate risks, such as using encryption technology, and that equating the risk of access with actual transmission to be legally questionable.

The Decision Karlsruhe Higher Regional Court (OLG Karlsruhe)

The OLG Karlsruhe **overturned** the decision of the Public Procurement Chamber, holding that:

- Merely being a subsidiary of a US-based company did not require the respondents to doubt the fulfilment of the promise of performance. The respondents did not have to assume that the US parent company would give instructions that violated the law and the contract or that the European subsidiary would follow instructions from the US parent company that violated the law.
- Since the respondents did not have to assume that the personal health data would be transferred to a third country, there was no need to conduct a transfer impact assessment.
- Promises of organizational and technical measures to ensure compliance with GDPR provisions when transferring data to the US are irrelevant in terms of the agreement to process the data exclusively in Germany.

Our remarks

- The mere fact that a subsidiary is owned by a US-based parent company does not necessarily mean that the subsidiary would violate GDPR provisions. However, controllers must ensure that the third-party processors they engage with, regardless of their ownership structure, can fulfill GDPR requirements. In this case, it would be sufficient to implement organizational and technical measures to prevent unauthorized third country access.
- To assess whether you need to conduct a transfer impact assessment, and to further your understanding of the European data transfer regime after Schrems II, see the ComplyCloud Transfer Roadmap whitepaper on our webpage under 'academy' -> 'downloads'-> Transfer Roadmap.

Please note that this decision was made prior to the EU Commission's adoption of the EU-U.S. Data Privacy Framework. The framework solves the challenges of the SCHREMS II case and thereby ensures that entities in the EU can transfer personal data to entities in the US that comply with the framework without conducting a TIA. However, general considerations concerning the transfer of personal data to other unsafe third countries still apply.

Published: 07-09-2022 **Journal number:** Az. 1 VK 23/22 **Tags:** 06 Transfer to third countries

Claim of non-material damages rejected by Court

Summary

Following the expiration of a fixed-term employment contract, a photograph of the data subject, along with his name, was still available on the Internet in connection with the former employer's (controller) company. In a letter dated 12 September 2018, the data subject requested the plaintiff to delete these entries. During an internet search on 10 and 11 October 2018, the data subject found entries by the former employer with his name and photo via Google.

The data subject further argued that the unauthorized publication of his photo and his name in connection with the controller's company put him at a noticeable disadvantage in his work as a freelance real estate agent. The data subject argued that several potential business partners would have refused to work with him because of the former employer's bad reputation in the real estate industry. He was of the opinion that the immaterial damage he had suffered because of this should amount to at least 25.000 EUR and declared the offsetting of this claim as compensation.

The Decision of the Higher Regional Court of Brandenburg (OLG Brandenburg)

OLG Brandenburg **rejected the claim** for damages for the following reasons:

A claim for damages can only arise from GDPR, Article 82, if concrete damage has been fully presented. The Court stated that such a claim had no material prospect of success in this case. A mere breach is not sufficient for claiming non-material damages.

Our remarks

- Even though the German Court applies a broad interpretation of the right to compensation for non-material damages, there must be indicators that the data subject has been significantly affected by the infringement. The threshold at which the severity of the infringement needs to be evaluated varies on a case-by-case basis and requires individual consideration.
- When doing a risk assessment, take into account the nature and severity of a possible infringement.
    - Examples of recognized non-material damages include feelings of uncertainty, loss of trust and anxiety about (potential) misuse of personal data. These risks need to be assessed in conjunction with the severity of the infringement.
- To avoid being held liable for inflicting non-material damages or the risk of future material damages because of a data breach, ensure adequacy of technical and organizational security measures:
    - Ensure that only current third-party business relations have access to your systems. Conduct regular security assessments and penetration testing to identify vulnerabilities in your system and organization (including partners) and implement adequate measures to address them.
    - Monitor access to personal data, limit it to authorized personnel (internally as well as third parties), and revoke access for those who no longer require access.

Copyright law prioritized artistic freedom over personality rights

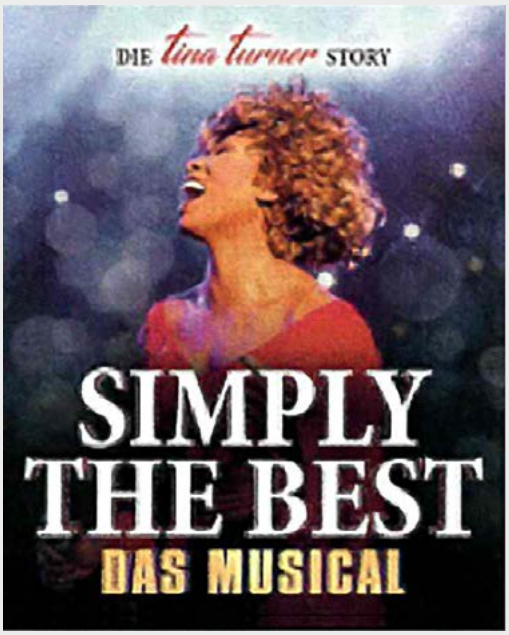
Summary

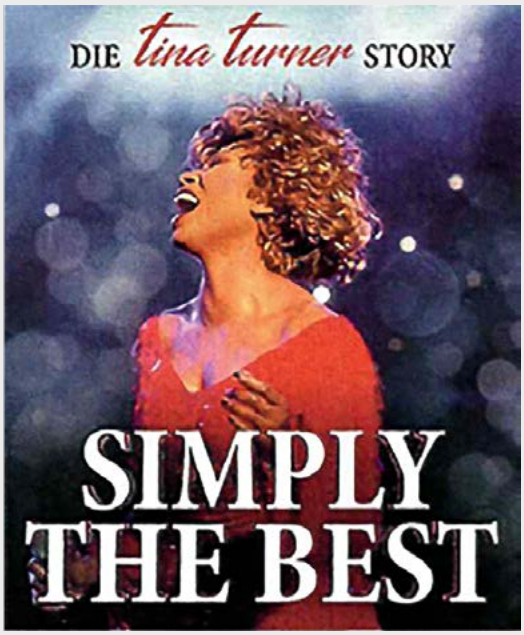
Tina Turner brought a lawsuit against the organizers of a tribute show titled "Simply the Best - Die Tina Turner Story," seeking injunctive relief. She claimed that the show's name and promotional materials created the impression that she would be performing or endorsing the production.

At issue was whether the Tina Turner impersonator in the show closely resembled the original performer, and whether the advertising posters featuring her photo and the title "Simply The Best - The Tina Turner Story" suggested that the superstar was directly involved in the production.

The dispute regarded whether the artistic freedom according to German copyright law of the Tina Turner lookalike outweighed the real Tina Turner's personality rights to the use of her image.

Even though the dispute mainly was assessed under articles in the German Civil Code, the Court specifically stated that the evaluation of the interests of the parties in the case is the same as the one made after *GDPR, Article 6(1)(f)*.





The photo of Tina Turner used on the posters

The Decision of the German Supreme Court

The German Supreme Court denied Tina Turner's claim for injunctive relief as the impersonator's artistic freedom **outweighed** the personality rights of Tina Turner, according to German copyright law. This decision was made after a balancing exercise, similar to that required by legitimate interests as legal basis *(GDPR, Article 6(1)(f))*.

Our remarks

- In some cases, other fundamental rights like the right to freedom of expression or artistic freedom can exceed a data subject's rights under the GDPR.
- In the specific case, the Court found that Tina Turner's right to images was exceeded as there was no risk of confusion between the cover artist and the real Tina Turner. As Tina Turner was 80 years old and had officially ended her career ten years ago (at the time of the lawsuit) there was no such risk.
- When you are a famous public figure, you often endure more than a regular person does. In the case, the Court also argued that the photo on the poster was taken in a public setting and that its use was not overly invasive.
- In Germany, and in the rest of Europe, copyright law requires a balancing exercise between artistic freedom and personality rights when determining the legality of using a person's likeness for commercial purposes.
- Despite this case, the use of a performer's name and image in other contexts without their consent can be an infringement of an intellectual property right or privacy rights according to the GDPR.

Disclosure of personal data for the enforcement of civil law claims

Summary

An individual who did not have a Facebook Messenger account learned that her personal data was being discussed in a group chat on Messenger by her family members.

The family members wrote messages like “She is the biggest bitch” or “What a disgrace she is for the proud family”. In addition to the insulting content, the family members made false factual claims about her.

The individual requested access to the information being disclosed about her in the group chat including IP addresses of the users, the messages, e-mail addresses of the users etc. to have the opportunity to establish a civil claim. This request was denied by Facebook.

The Individual then filed a complaint with the Irish Data Protection Comission (DPC), as Facebook’s European headquarters are in Ireland. The Irish DPA referred the case to the German Federal Court of Justice (Bundesgerichtshof) as the applicant was German.

The case raised questions in relation to whether the information could be provided according to the German Telemedia Act (TMG) and the GDPR.

The Court found that Facebook Messenger comes under the purview of the TMG, which allows service providers to disclose user data to enforce civil law claims. Furthermore, the Court deemed this disclosure as a necessary and proportionate action within a democratic society, in line with GDPR, Article 23(1)(j).

The Decision of the German federal Court

The German federal Court **ruled** that according to GDPR, Article 17, the individual had the right to be provided with the personal data being discussed about her in the group chat on Messenger.

Our remarks

- The right to access personal data under the GDPR also applies to individuals who are not users of a particular service. In this case, the person who did not have a Facebook Messenger account was still entitled to access the personal data being discussed about her in a group chat on Messenger.
- The right to privacy is an important consideration in determining whether an individual should be granted access to personal data, as there can be opposing privacy rights that need to be assessed. The German Court found that the person’s right to privacy outweighed Facebook’s interests in protecting the privacy of other Messenger users.
- The case shows how GDPR can influence the application of other laws. The Court concluded that TMG’s provisions regarding the disclosure of user data for the enforcement of civil law claims must be applied in accordance with the GDPR’s requirements of necessity and proportionality.
- The ruling highlights the importance of transparency and accountability in data processing practices. The GDPR requires companies to be transparent about their data processing practices and to ensure that individuals can exercise their rights to access, rectify, and delete their personal data.

Dismissal of DPO in concerns of potential conflicts of interests justified under national legislation

Summary

An employee, who had been working for X-FAB since 1st November 1993, held the positions of chair of the works council and vice-chair of the central works council for three undertakings within the group of companies, all of which belonged to X-FAB and were situated in Germany. Beginning in June 2015, the employee was appointed as the DPO for X-FAB, its parent company, and other subsidiaries established in Germany.

However, in response to a request from the Thüringen DPA, X-FAB and the undertakings in question dismissed the employee from his duties as DPO, citing concerns of potential conflicts of interest due to his concurrent roles as DPO and chair of the works council. The company argued that the dismissal was justified under national legislation that allowed for dismissal with 'just cause'. As a result, the employee brought an action before the German courts seeking a declaration that he should retain the position of DPO.

The Decision of the European Court of Justice (CJEU)

The preliminary ruling by the CJEU ruled that the dismissal of the DPO grounded in the 'just cause' notion in national legislation was justified with the following arguments:

- According to national legislation, a controller or processor has the authority to dismiss a data protection officer who is an employee of that controller or processor, even if the dismissal is not related to the officer's tasks. This provision does not violate the second sentence of *GDPR, Article 38(3)* provided that such legislation does not undermine the objectives of the Regulation and remains compatible with EU law.
- A conflict of interests may arise if a data protection officer has additional tasks or duties that would enable them to determine the objectives and methods of processing personal data for the controller or processor *(GDPR, Article 38(6))*. The national court must determine whether such a conflict exists on a case-by-case basis by assessing all relevant circumstances, including the organizational structure of the controller or processor and applicable rules and policies.

Our remarks

- The DPO should be able to perform their duties and tasks in an independent manner. In that regard, such independence must necessarily enable them to carry out those tasks in accordance with the objective of the GDPR. The DPO cannot be assigned responsibilities that involve deciding on the objectives and methods of processing personal data for the controller or its processor. It is necessary to evaluate all the relevant circumstances on a case-by-case basis, including the organizational structure of the controller or its processor, applicable regulations, and any policies of the controller or its processor, to identify any potential conflicts of interest.
- According to the CJEU, Member States are allowed to lay down more protective legislation relating to the dismissal of a DPO employed by a controller or by a processor, if such legislation is intended to preserve the functional independency of the DPO and is compatible with EU law. When operating as a DPO in multiple countries, make sure to evaluate the legal landscapes in each country to ensure sufficient functional independence.

Published: 09-02-2023 **Journal number:** C-453/21 **Tags:** 01 Legal Basis and principles

Largest fines – Belgium

05

Google Belgium SA Fined for violating the right to be forgotten

Summary

A Belgian citizen, who is well-known in Brussels and has held various high-ranking positions in the energy sector, filed a complaint to the Belgian Data Protection Authority (DPA) concerning the delisting of 12 URLs from Google's search results. The complainant argued that the links, which presented the complainant as affiliated with a political party and included outdated information about an unfounded harassment complaint, were detrimental to his honor and reputation. Google responded by removing one link, stating that another could not be accessed, and refusing to block the remaining links. The complainant did not receive noteworthy information as to how this decision was justified by Google.

A substantial part of the case was concerned with determining whether Google Belgium SA (Google Belgium), Google Ireland Ltd. (Google's main establishment in the EU) or Google LLC, established in California, should be considered the data controller. The issue raised complex questions on the territorial scope of the GDPR and became the determining factor in why the historic fine was ultimately annulled by an appeals court.

Decision of the Belgian DPA

The Belgian DPA **fined** Google Belgium SA **600,000** EUR, based on the annual turnover of its parent company, Alphabet, for the following violations:

- Breaching the complainant's right to be forgotten and inadequately balancing the complainant's rights and interests against Google's legitimate interests in processing the relevant personal data *(GDPR, Articles 17(1)(a)* and *6(1)(f))* (500.000 EUR).
- Failing to provide the complainant with sufficient information regarding the decision not to dereference the relevant links *(GDPR, Article 12)* (100.000 EUR).

On the issue of competence

The Belgian DPA found that Google LLC, of which Google Belgium is a subsidiary, could be considered the data controller and asserted its competence to take action against Google Belgium, arguing that the activities of the two entities were inextricably linked.

The DPA noted that the one-stop-shop mechanism, which allows companies operating across multiple EU member states to deal with only one supervisory authority for their cross-border processing activities, did not apply in these circumstances. Had this been the case, the Irish DPA would have assumed the role as lead supervisory authority since Google Ireland Ltd. is Google's main establishment in the EU. However, the one-stop-shop mechanism did not apply for two reasons. Firstly, the DPA argued, since the data processing in question did not concern cross-border activities, and secondly, since Google Belgium's counsel had confirmed that Google Ireland Ltd. was not involved in the processing activities related to the complaint. Instead, the DPA argued that the GDPR applied to Google LLC, and that Google Belgium as an establishment of Google LLC triggered the applicability of the GDPR under *Article 3(1).*

On the requests for dereferencing

The Belgian DPA found the search results relating to the harassment to be outdated and having potential prejudicial impact on the complainant's professional and private life. The DPA concluded that Google Belgium had infringed the complainant's right to be forgotten as well as his right to information by refusing to dereference the search results. However, the links relating to the political affiliation of the complainant were deemed able to remain online due to their continuing public relevance.

Published: 30-06-2021 **Journal number:** 2020/AR/1111 **Tags:** 01 Legal basis and principles of processing, 07 Scope of the GDPR

Decision of the Market Court of Appeals

The Market Court of Appeals (the Market Court) **annulled the decision of the Belgian DPA, including the fine of 600,000 EUR.** Basing its arguments on national principles of administrative law, the Market Court found that the decision of the DPA lacked proper motivation. In particular, the decision did not provide an adequate or satisfactory explanation for directing the complaint and sanctions solely against Google Belgium SA, when Google LLC was found to be the actual data controller responsible.

The Market Court highlighted that Google Belgium SA is primarily responsible for Google's marketing activities in Belgium, and therefore is not involved in determining the means and purposes of data processing through the Google search engine.

The Market Court also noted that the GDPR contains obligations only for data controllers and data processors. A subsidiary or local establishment engaged in other activities, such as Google Belgium, may only be held accountable where its activities are indissociably linked to the personal data processing carried out by Google LLC. This link must be identified on a case-by-case basis and cannot be presumed or demonstrated by referring to decisions from other national jurisdictions or courts of other EU member states. The Market Court argued that the Belgian DPA may only pursue a local establishment if there is clear, unambiguous, and non-contradictory evidence of an inextricable link between the local establishment (Google Belgium SA) and the data controller (Google LLC).

In sum, the Market Court did not replace its own judgement with that of the DPA. The disputed decision was overturned and referred back to the Belgian DPA, who must now make a new decision from scratch, provided that a valid complaint is still pending. In its new decision, the DPA may impose a new fine on Google Belgium SA or even target other entities within the Google group, such as Google LLC or Google Ireland Ltd.

Our remarks

- By issuing its largest fine to date, the Belgian DPA sent a strong signal to global organizations, urging them to consider their data protection strategies in view of the GDPR. The case also demonstrates the Belgian DPA's intentions to challenge multinational entities on their intended company structures when these do not adequately align with reality.

- The case furthermore illustrates the approach taken by the Belgian DPA in striking a balance between the privacy rights of public figures and the public's right to access information about them online. By finding that certain articles related to the complainant's political affiliations could remain online, the Belgian DPA acknowledges the importance of public interest. However, the DPA emphasizes the need to protect public figures from potential harm, such as the repercussions from unfounded harassment allegations. The case illustrates the commitment of the Belgian DPA to carefully weighing the competing interests of privacy and information access when addressing questions relating to public figures.

- Finally, the Market Court's decision in the appeal case has set a standard for the Belgian DPA when pursuing transnational companies in data protection matters, highlighting the interplay between European regulations and national procedural rules. The case is centered around a national provision regarding the adequate motivation of administrative decisions, as stated in the Act of 29 July 1991. In cases where administrative authorities have broad discretionary power, and particularly when the arguments of a party are dismissed, the need for adequate motivations is particularly important, and must be based on clear and concrete elements.

Interactive Adverting Bureau Europe fined for the non-compliance of its Transparency & Consent Framework

Summary

The Interactive Adverting Bureau Europe (IAB Europe) developed an operational consent solution for parties in the digital advertising industry known as the Transparency and Consent Framework (TCF).

IAB Europe represents the digital advertising and marketing industry across Europe. The association was the subject of several complaints concerning various breaches of GDPR due to its alleged large-scale processing of personal data in the context of the TCF.

The TCF provides an environment where website publishers can communicate with consumers, specifying how data is collected and disclosing its intended use by the website owner and its partners. User preferences are captured by generating a so-called TC String (Transparency and Consent String), consisting of a combination of letters, numbers and other characters. As users browse websites using the TCF (pop-ups) to collect consent, the placement of cookies or other advertisement identifiers and tracking technologies on their devices allow adtech vendors to bid on user profiles, exposing users to advertisements according to their individual commercial preferences. A question central to the case is whether TC Strings qualify as personal data under GDPR.

In relation to the TCF, the role of IAB Europe under GDPR is disputed. Arguments were made by the Belgian DPA that IAB Europe acted as data controller for the recording of TC Strings as well as joint data controller alongside other actors implementing the TCF such as website owners, adtech vendors and others collecting and disseminating users' preferences. In this regard, the DPA pointed to the decisive influence of IAB Europe on the purposes and means of data processing through its role as designer of the TCF and managing body of organizations participating in the TCF. By enabling the generation of the TC String and determining the policies for how consent might be obtained and disseminated, the DPA held that IAB Europe was exerting control in the capacity of data controller. According to IAB Europe itself, however, the association merely held the status of data processor in the context of the TCF for two main reasons. Firstly, the association argued that TC Strings contain technical information only, i.e. the binary indication of whether a user consented to the processing purposes on a given website. As such, TC Strings contain no unique identifier (such as the IP address) and should not be qualified as personal data according to IAB Europe. Secondly, regardless of the legal qualification of TC Strings, IAB Europe did not own, process, or coordinate the use of specific TC Strings and consequently argued that its role did not amount to that of a data controller.

As a result of the misconceptions related to IAB Europe's role as being either data controller or processor, the association did not establish sufficient legal basis under GDPR according to the Belgian DPA. Similarly, the DPA found that IAB Europe had breached several provisions by failing to conduct a data protection impact assessment, appointing a DPO, and maintaining a register of their processing activities.

The Belgian DPA issued the fine on 2 February 2022 and ordered IAB Europe to produce, within two months, an action plan for securing the compliance of the TCF. IAB Europe appealed the decision to the Brussels Market Court of Appeal on 4 March 2022.

Published: 15-01-2021, **Journal number:** DOS-2019-01377 **Tags:** 01 Legal basis and principles of processing, 02 Right of access and obligation to provide information, 05 Data security

Decision of the Belgian DPA

The Belgian DPA **imposed** a fine of **250,000** EUR for the following violations:

- Processing user preferences in the form of TC Strings without legal basis *(GDPR, Articles 5(1)(a) and 6).*
- Failing to sufficiently inform data subjects and thus comply with transparency requirements *(GDPR, Articles 12, 13 and 14).*
- Failing to ensure the security of the processing *(GDPR, Articles 24, 25, 5(1)(f) and 32).*
- Failing to keep a record of the relevant processing activities *(GDPR, Article 30).*
- Failing to perform a data protection impact assessment *(GDPR, Article 35).*
- Failing to appoint a data protection officer *(GDPR, Article 37).*

The Belgian Data Protection Authority furthermore **imposed an obligation** on IAB Europe to undertake several corrective measures. IAB Europe should develop an action plan to include:

- A valid legal basis for processing and sharing user preferences within the TCF.
- Auditing the GDPR compliance of all organizations participating in the TCF.

Decision of the Market Court of Appeals

In an interim ruling of 7 September 2022, the Market Court found that the decision of the Belgian DPA was insufficiently substantiated while referring two questions to the Court of Justice of the European Union. These questions concern the interpretation of data controllership as well as the legal status of TC Strings under GDPR. Once answered, the Market Court will rule on the substantive issues raised in IAB Europe's appeal of the Belgian DPA's decision. A decision is expected in 2024.

Our remarks

- According to the Belgian DPA, the processing of a TC String in combination with a user's IP address amounts to personal data within the meaning of GDPR. As the purpose of TC Strings is to single out individuals and capture their personal preferences, the DPA argues, it can be assumed that the data subject will likely be identified, although indirectly. However, this interpretation of the notion of personal data has been criticized by IAB Europe for being overly broad from a consumer protection point of view and has since been referred to the Court of Justice of the European Union by the Market Court. The question is currently unanswered.
- The case will likely have far-reaching implications for the status of standard setting organizations. Although industry standards are highly impactful in establishing best practices within a particular sector, assigning these organizations the responsibilities of (joint) controllers based on codes of conduct may prove a drastic step. Following the reasoning of the Court of Justice of the European Union in the coming months will hopefully provide much anticipated clarity on this issue.

Brussels Zaventem Airport fined for processing health data about travelers

Summary

Brussels Zaventem Airport installed thermal cameras to identify and screen passengers with a body temperature of more than 38°C, thus processing health data of passengers entering the airport (first line of control). Furthermore, a specialized 'Ambuce Rescue Team' was engaged to conduct second temperature scans and examinations of further symptoms of passengers whose temperatures were above 38°C (second line of control). Findings were then issued in a report based on the examinations. Both Brussels Zaventem Airport and the Ambuce Rescue Team were considered data controllers.

The data processing was based on a Protocol which, according to the Belgian DPA, was not binding under Belgian law.

The decision of the DPA was later partly annulled by the Market Court of Brussels.

Decision of the Belgian DPA

The Belgian DPA **imposed a fine of 200,000** EUR on Brussels Zaventem Airport for the following violations:

- Lacking a valid legal basis and basic data protection principles *(GDPR, Articles 5(1)(c), 6(1)(e)* **and** *9(2)(g)).*
- Failure to comply with information and transparency requirements *(GDPR, Articles 12, 13(1)(c)* and *13(2)(g)).*
- Failure to conduct comprehensive impact assessments *(GDPR, Articles 35(1), 35(3)* and *35(7)(b)).*

The Belgian Data Protection Authority **imposed a fine of 20.000** EUR on the Ambuce Rescue Team for the following violations:

- Lacking a valid legal basis and breach of basic data protection principles *(GDPR, Articles 5(1)(c), 6(1)(e)* and *9(2)(g)).*
- Failing to conduct comprehensive impact assessments *(GDPR, Articles 35(1)* and *35(3)).*

Published: 07-12-2022, **Journal number:** 2022/AR/560&564 **Tags: 01** Legal basis and principles of processing, 02 Right of access and obligation to provide information

Decision of the Market Court of Brussels

The Market Court **annulled the decision and fine** regarding the Ambuce Rescue Team.

Our remarks

- Invoking a legal obligation within the meaning of GDPR, Article 6(1)(c) or public interest within the meaning of GDPR, Article 9(2) requires the presence of legal necessity under national or EU law. The protocol invoked by the airport did not, however, directly impose the use of temperature checks on passengers in the opinion of the Belgian DPA. As the protocol in question did not constitute a law in a strict sense, the legal obligations originating from it could not be considered clear and precise enough to constitute standards of law within the meaning of GDPR, Articles 6(1) and 9(2).

- When indicating the legal basis for processing activities in a privacy policy, general references to "legal obligations and tasks of general interest" will not comply with the requirements of transparency under the GDPR. Instead, the policy must clearly indicate which of the cases listed in Articles 6 or 9 are applicable to the disputed processing activities.

- The decision underlines the importance of conducting comprehensive impact assessments (DPIA's). Data Protection Impact Assessments ensure the thorough evaluation of risks of data subjects due to the processing of their data. It should be noted that the "large-scale" nature of the processing of special categories of personal data is not solely determined by the number of data subjects involved. In this regard, the Ambuce Rescue team pointed out that only eight people had been subjected to second-line controls, arguing that the disputed processing did not fall under GDPR, Article 35(3)(b). However, according to the DPIA Guidelines of the Article 29 Working Party, processing activities may also be considered "large-scale" based on factors such as the quantity of personal data involved, the duration or continuous nature of the processing activity, and the geographical scope of the processing. Therefore, in the present case, the data controller should have included the second line of control in its DPIA.

Brussels South Charleroi Airport fined for processing health data about travelers

Summary

Brussels South Charleroi Airport installed thermal cameras to identify and screen passengers with a body temperature exceeding 38°C, thus processing health data of passengers entering the airport (first line of control). The scans were conducted both for departing and arriving passengers. Furthermore, a specialized team was assigned to conduct second temperature scans and examinations of further symptoms of passengers displaying temperatures above 38°C (second line of control). Findings were then issued in a report based on the examinations.

The data processing was based on a Protocol which, according to the Belgian DPA, was not legally binding under Belgian law.

Decision of the Belgian DPA

The Belgian DPA **imposed a fine of 100,000 EUR** on Brussels South Charleroi Airport for the following violations:

- Lacking a valid legal basis and disregarding basic data protection principles *(GDPR, Articles 5, 6* and *9).*
- Failure to comply with information and transparency requirements *(GDPR, Articles 12* and *13).*
- Failure to conduct comprehensive impact assessments *(GDPR, Articles 35(1)).*
- Breaching the obligation to implement technical and organizational measures to secure data *(GDPR, Article 32).*
- Breaching the principle of data protection by design and default *(GDPR, Article 25).*
- Failing to ensure the independence of the data protection officer (DPO) *(GDPR, Article 38(3)).*

Decision of the Market Court of Brussels

The Market Court **reduced the fine** to **25,000** EUR.

Our remarks

- When indicating the legal basis for processing activities in a privacy policy, general references to "legal obligations and tasks of general interest" do not meet the transparency requirements outlined in the GDPR. Instead, the policy must clearly indicate which of the cases listed in Articles 6 or 9 are applicable to the disputed processing activities.
- Invoking a legal obligation within the meaning of GDPR, Article 6(1)(c) or a public interest within the meaning of GDPR, Article 9(2) requires the presence of legal necessity under national or EU law. The Protocol invoked by the airport did not, however, directly impose the use of temperature checks on passengers in the opinion of the Belgian DPA. As the protocol in question did not constitute a law in a strict sense, the legal obligations originating from it could not be considered sufficiently clear and precise to constitute legal standards within the meaning of GDPR, Articles 6(1) and 9(2).

Published: 07-12-2022 **Journal number:** 2022/AR/556 **Tags:** 01 Legal basis and principles of processing, 02 Right of access and obligation to provide information

Financial company fined for lacking sufficient organizational measures

Summary

The complainant, a client of a financial company, discovered that her personal data hosted by the Belgian National Bank ('BNB') had been unlawfully accessed 20 times between 2016 and 2018.

The defendant was a company operating within the financial sector which offered services such as personal loans. The ex-husband of the complainant was employed at the company. According to the defendant's data protection officer, employees were only allowed to access the personal BNB files of clients in order to grant or manage credit. However, the complainant's ex-husband accessed the personal file of the complainant in violation of these guidelines.

Although the complainant's ex-husband was accountable for the unauthorized access to the complainant's file, the data controller retained responsibility as a data controller and employer under GDPR, Articles 5(2) (accountability principle) and 24 (responsibility of the controller). Therefore, the employer was responsible for ensuring the safety of its data processing and remained accountable for any violations.

The complainant inquired with the data protection officer, on more than one occasion, about the data that was accessed, the identity of the individuals who accessed the data, as well as the purpose and legal basis. This information, despite the numerous requests, was not provided to the complainant.

Decision of the Belgian DPA

The company was **fined 100,000** EUR for the following violations:

- Lacking sufficient organizational and technical measures ensuring the security of processing *(GDPR, Article 32* in conjunction with *Article 24).*
- Failing to provide the data subject with requested information *(GDPR, Article 15).*

The company was **ordered** to implement a compliance process for access to BNB files.

Our remarks

- The employer, who is also the data controller, holds the responsibility for the data processing carried out by its employees in line with its predefined purposes. However, the employer may also be held liable for unauthorized data processing carried out by its employees. In cases where employees engage in unauthorized data processing, it is the entity, not the employee, that is accountable for adhering to data protection legislation, unless specific circumstances indicate otherwise. As per the Opinion 1/2010 of the Article 29 Working Party, companies and organizations are often considered responsible for data processing, rather than the individual employees within them. Therefore, it is imperative for the data controller to implement suitable technical and organizational measures to prevent any abusive data processing by its employees, especially when it comes to special categories of personal data such as financial information relating to persons.
- Although the defendant is considered the data controller for the purposes of the data processing carried out by its employees, this does not mean that it is the only entity responsible in this case. The employee was also considered a data controller for the specific, unauthorized data processing activities he carried out, and actions were brought against him in a separate case.
- The Belgian DPA emphasized the value of following best practices when securing personal data. Although not explicitly mentioned in the GDPR, measures such as keeping log files allow the data controller to demonstrate compliance with Article 32 (security of processing) by documenting that technical steps have been taken to limit unauthorized access by an employee to a database of personal data.
- Data controllers must respond to access requests in accordance with the GDPR, Article 15, providing the data subject with a list of the data that has been accessed, the identity of the individuals who accessed it, the purpose, and the legal basis.

Published: 26-04-2021 **Journal number:** DOS-2019-02288 **Tags:** 05 Data security

Bank fined due to a conflict of interest regarding its DPO

Summary

An individual filed a complaint with the Belgian DPA, claiming that a bank had violated his right to rectification *(GDPR, Article 16)*. During the investigation, the DPA broadened its scope to examine a potential conflict of interest regarding the bank's data protection officer (DPO). The Belgian DPA examined the different roles assumed by the DPO. In addition to being the DPO, the employee also headed the bank's operational risk management department, the information risk management department, and its special investigation unit.

It follows from GDPR, Article 38, that a DPO may have other roles within a company. However, the tasks and duties of the DPO must not result in a conflict of interest.

The bank claimed that the DPO merely held a position of formal responsibility as head of the three departments. As such, his supervisory role did not entail decision making competences in relation to the purposes and means of personal data processing. To support its argument, the bank referred to the organizational structure of the departments and previous caselaw from the Belgian DPA. However, the DPA proceeded to evaluate to what extent the independence of the DPO was ensured with respect to each of the three departments.

The DPA determined that issues regarding conflicts of interests must be determined on a case-by-case basis, taking into account the data controller's organizational structure. The DPA then found that the organizational structure of the bank *de facto* resulted in the DPO having responsibilities and performing tasks as head of the three departments that were incompatible with his role as DPO.

Decision of the Belgian DPA

The Belgian DPA **fined** the bank **75,000** EUR for the following violations:

- Failing to ensure the independence of the DPO *(GDPR, Article 38(6))*.
- Failing to provide the data subject with requested information *(GDPR, Article 15)*.

The bank was also **ordered** to implement a compliance process to properly handle access requests from its clients.

Our remarks

- Organizations should exercise caution when appointing DPO's who hold multiple roles within the company. Conflicts of interest may arise if the DPO acts as the head of other departments where they are responsible for making decisions related to the purposes and means of personal data processing in some capacity.
- Avoiding conflicts of interest is always important to prioritize when appointing a DPO, regardless of the size of the organization. However, in cases where organizations process personal data relating to a large number of data subjects, as in the present case, the presence of a conflict of interest is even more significant. The greater the number of data subjects potentially impacted, the higher the risk of harm due to conflicts of interest, and as a result, the larger the potential fine that may be imposed.

Published: 16-12-2021 **Journal number:** DOS-2020-03763 **Tags:** 01 Legal basis and principles of processing

SA Rossel & Cie media company fined for unlawful use of cookies

Summary

SA Rossel & Cie ('Groupe Rossel'), a Belgian press site, was among the subjects of a broad investigation carried out by the Belgian Data Protection Authority (DPA) regarding the placement of cookies on the most widely accessed Belgian online news media sites. The case was examined together with the case regarding Roularta Media Group, which is described below. The DPA examined several websites administered by Groupe Rossel to assess how non-essential cookies were managed and whether visitors' consent was obtained in accordance with the GDPR.

The DPA's investigation found that Groupe Rossel had used non-essential cookies without obtaining valid consent from visitors, including cookies on third-party domains. Additionally, Groupe Rossel obtained user consent using the 'further browsing' mechanism, which linked users' expressions of cookie consent to their decision to continue browsing the website. According to the DPA, this method of obtaining consent does not meet the requirements for specification and distinction outlined in GDPR, Article 4(11).

The DPA found that Groupe Rossel had continued to place cookies on users' devices after they had withdrawn their consent. The placement of cookies in such a situation is unlawful due to the lack of (consent as a) legal basis.

The DPA also found that the cookie policies of Groupe Rossel's websites were incomplete and not easily accessible to users. Additionally, these policies failed to provide mandatory information, such as the names of all third-party partners. As a result, Groupe Rossel breached GDPR, specifically Articles 12(1), 13, and 14, which requires organizations to provide data subjects with complete and accessible information about the processing of their personal data.

The decision was later appealed.

The decision of the Belgian DPA

The Belgian DPA **imposed a fine** of **50,000** EUR on Groupe Rossel for the following violations:

- Placing non-essential cookies before obtaining user consent, including cookies placed by third-party domains *(GDPR, Article 6(1)(a)* and *Article 129* of the *Belgian Electronic Communications Act)*.
- Obtaining consent through the "further browsing" technique, which links the expression of consent for cookies with the choice to continue using the website *(GDPR, Articles 4(11), 6(1)(a),* and *7(1)).*
- Depositing non-essential cookies, namely social media and audience measurement cookies, before obtaining user consent *(GDPR, Article 6(1)(a)).*
- Presenting the selection screen for partners to whom personal data was sent in "allow" mode by default for the approximately 500 listed partners *(GDPR, Articles 4(11), 6(1)(a)* and *7(1)).*
- Only mentioning 13 external partners in the cookie policy, whereas the partner selection screen accessible via the volatile cookie banner referenced around 500 partners of this type *(GDPR, Articles 4(11), 12(1), 13* and *14).*
- Failing to provide sufficient accessible and/or language-appropriate mandatory information to data subjects *(GDPR, Articles 12(1), 13, and 14).*
- Allowing the placement of new cookies after the withdrawal of user consent without justification deemed relevant by the DPA *(GDPR, Article 7(3)).*

Appeal to the Belgian Market Court

According to Belgian law, when the Belgian DPA initiates a case on its own, it must be based on a referral. The referral must be made by the management board of the DPA and provide "serious indications" of a potential violation of the fundamental principles of personal data protection.

However, in the referral for this case, no serious indications were mentioned or proven. Even though the investigation service (not the management board) created a handwritten note listing various reasons for initiating the investigation, the Market Court found that there was no official referral which made the investigation irregular and suggested that the investigation service was improperly involved or seized in an irregular manner. Therefore, the Market Court made the case invalid.

Final decision of the Belgian Market Court

The Court **invalidated** the decision by the Belgian DPA, as the referral on which the investigation was based was insufficient.

Our remarks

- For cookie placement to be lawful, user consent must be obtained prior to the placement of cookies, and continued browsing may not be considered a legal form of consent under GDPR. Rather, consent should be considered valid only if it results from a clear and sufficiently specific active action from the user. Finally, if users withdraw their consent, this withdrawal must be effective and prevent the placement of further cookies.
- Article 129 of the Belgian Electronic Communications Act contains two exceptions regarding user consent and cookie placement. As a main rule, the consent of data subjects must be obtained prior to the placement of cookies on their devices. This, however, is not required in the following two situations:
  - When the cookie is only intended to carry out the transmission of a communication over an electronic communications network, or
  - When the cookie is strictly necessary for the provision of a service explicitly requested by the subscriber or end user (such as cookies allowing the storage of items in an online shopping cart or ensuring the security of a banking application).
- All other cookie placements or installations of other tracking measures require the prior consent of the data subject.
- Data protection authorities must oblige to procedural rules. Even though their assessment of the processing in question is correct, the case or decision can be invalidated if procedural rules are not followed.
- As the invalidation only happened due to the missing justification in the referral, the DPA's assessment of the cookie solution is still relevant as a takeaway for other data controllers.

Roularta Media Group fined for unlawful use of cookies

Summary

Roularta Media Group, a Belgian media company, was among the subjects of a broad investigation carried out by the Belgian Data Protection Authority (DPA) regarding the placement of cookies on the most widely consulted Belgian online news media. The case was examined together with the case about SA Rossel & Cie, which is described above. The DPA inspected several websites administered by Roularta Media Group, focusing on the management of non-essential cookies and whether visitors' consent had been obtained in accordance with the GDPR.

The DPA found that Roularta Media Group had used non-essential cookies without first obtaining valid consent from website users.

Furthermore, Roularta Media Group had obtained user consent to the placement of third-party cookies in an ambiguous manner, contrary to the GDPR requirements, by presenting users with pre-ticked boxes. Additionally, it was more difficult for users to withdraw consent to the placement of cookies than it was for them to provide it.

Finally, the DPA noted that the cookie policy of Roularta Media Group on the relevant websites did not provide adequate details regarding the use of cookies, and that cookies were being retained for unjustified periods of time. The company did not fulfill its obligation to enable users to revoke their consent.

The decision was later appealed.

The decision of the Belgian DPA

The Belgian DPA **imposed** a fine of **50,000** EUR on Roularta Media Group for the following violations:

- Placing non-essential cookies before obtaining user consent, including cookies placed by third parties *(GDPR, Article 6(1)(a)* and *Article 129(2))* of the *Belgian Electronic Communications Act*).
- Non-compliance with the conditions for obtaining valid consent from users, namely by presenting users with pre-checked boxes on two websites, with partner companies' cookies marked as 'active' by default *(GDPR, Articles 4(11)*, *6(1)(a)* and *7(1))*.
- Due to the publication of a disclaimer on the websites in question, claiming that Roularta Group was not responsible for the placement of third-party cookies on users' devices *(GDPR, Articles 5(2)* and *24)*.
- Failing to provide information to data subjects in a transparent, understandable, and easily accessible form *(GDPR, Articles 12(1), 13,* and *14*).
- Non-compliance with the principle of storage limitation *(GDPR, Articles 5(1)(e))*.
- Failing to ensure that withdrawing consent to the placement of cookies is as easy as providing it *(GDPR, Article 7(3))*.

Appeal to the Belgian Market Court

According to Belgian law, when the Belgian DPA initiates a case on its own initiative, it must be based on a referral. The referral must be made by the management board of the DPA and provide "serious indications" of a potential violation of the fundamental principles of personal data protection.

However, in the referral for this particular case, no serious indications were mentioned or proven. Even though the investigation service (not the management board) created a handwritten note listing various reasons for initiating the investigation, the Market Court found that there was no official referral which made the investigation irregular and suggested that the investigation service was improperly involved or seized in an irregular manner. Therefore, the Market Court made the case invalid.

Decision of the Belgian Market Court

The Court **invalidated** the decision by the Belgian DPA, as the referral on which the investigation was based was insufficient.

Our remarks

- For the placement of cookies to be lawful, user consent must be obtained prior to the placement of cookies. Consent may only be considered valid if the conditions set out in the GDPR are met. This includes the requirement that the data subject provides consent in the form of a freely given, specific, informed, and unambiguous indication of their wishes to agree to the processing of personal data, as outlined in GDPR, Article 4(11).
- The owner of a website is responsible for the processing of cookies installed or read by its website. This responsibility may not be waived by publishing a disclaimer on the website in question.
- The case clarified that the use of statistical cookies does indeed constitute a processing of personal data under GDPR in conjunction with the Belgian implementation of the ePrivacy Directive. Therefore, prior user consent is required when placing statistical cookies with available IP addresses.
- To observe the principle of storage limitation, note that the lifespan of cookies must be directly linked to the purpose for which it is used and must be configured to expire as soon as it is no longer necessary, considering the reasonable expectations of the data subject.
- Article 129 of the Belgian Electronic Communications Act contains two exceptions regarding user consent and cookie placement. As a main rule, the consent of data subjects must be obtained prior to the placement of cookies on their devices. This, however, is not required in the following two situations:
    - When the cookie is only intended to carry out the transmission of a communication over an electronic communications network, or
    - When the cookie is strictly necessary for the provision of a service explicitly requested by the subscriber or end user (such as cookies allowing the storage of items in an online shopping cart or ensuring the security of a banking application).

All other cookie placements or installations of other tracking measures require the prior consent of the data subject.

- When providing data subjects with information regarding cookies, as required by GDPR, Articles 12, 13 and 14, be sure to include:
    - A complete list of the different types or categories of cookies placed on the users' devices.
    - Sufficient information on the criteria for determining the lifespan of the cookies placed on user's devices and the duration of retention of the data collected.
    - Information on the processing carried out by external partners and vendors.

Note that all information must be provided in a transparent, understandable, and easily accessible manner.

- Withdrawing consent to the placement of cookies must be as easy as it is to provide in the first place. The cookie management tools used on a website must provide an effective mechanism for withdrawing consent, after which the number of cookies placed should decrease.
- Data protection authorities must obey procedural rules. Even though their assessment of the processing in question is correct, the case or decision can be invalidated if procedural rules are not followed.
- As the invalidation only happened due to the missing justification in the referral, the DPA's assessment of the cookie solution is still relevant to other data controllers as a takeaway.

Family Service fined for unlawful consent practices

Summary

Family Service is an advertisement agency, offering so-called 'gift packages' for expecting parents, containing offers and samples of products and services. Expecting parents can subscribe to the service, allowing Family Service to pass on data to other entities. The gift packages are distributed through a network of partners, including hospitals and gynecologists.

An individual filed a complaint with the Belgian Data Protection Authority (DPA) after receiving targeted advertising from an external company, which had obtained the complainant's personal data from Family Service. The complainant claimed that she had received multiple phone calls without giving her explicit consent to Family Service, and that these inquiries continued even after she had withdrawn her consent and objected to receiving targeted advertising.

Although the complainant had given her consent while subscribing to the gift packages, the agreement failed to provide adequate information about how, to whom, and under which circumstances her personal data would be shared. As a result, the complainant was unable to make an informed decision about the intended use of her data, rendering her consent invalid and not freely given as required by the GDPR.

Among other circumstances central to the case, Family Service had a policy of retaining personal data about its subscribers for up to 18 years, when newborn children registered in the database would no longer be legally represented by their parents. Furthermore, no record was kept of requests for rectification. Finally, subscribers' email addresses were intentionally kept even after data subjects had requested erasure to ensure that no new accounts were created using the same email address later. According to the DPA, these activities were against both the letter and the spirit of the GDPR.

Decision of the Belgian DPA

The Belgian DPA **imposed a fine of 50,000 EUR** on Family Service for the following violations:

- Providing subscribers with a misleading impression regarding the use of their personal data when subscribing to receive gift packages *(GDPR, Article 5(1)(a)).*
- Retaining personal data for up to 18 years, which was deemed disproportionate, considering most of the offered products concerned infants *(GDPR, Articles 5(1)(c) in conjunction with Article 25).*
- Failing to obtain free, specific, informed, and unambiguous consent from data subjects, and for processing data without the presence of a legitimate interest which could outweigh the interests of the data subject *(GDPR, Articles 6(1)(a) and (f)).*
- Failing to ensure that withdrawing consent was as easy for data subject as providing it *(GDPR, Article 7(3)).*
- Failing to provide sufficient information to data subjects *(GDPR, Article 13).*
- Non-compliance with the principle of storage limitation *(GDPR, Article 5(1)(e)).*
- Not taking the appropriate technical and organizational measures to secure the rights and freedoms of the data subjects, considering the nature, context, and purpose of the processing activities in question *(GDPR, Article 24).*
- The lack of processing agreements between Family Service and one of their data processors *(GDPR, Article 28(3)).*

Published: 27-01-2021 **Journal number:** DOS-2019-04798 **Tags:** 01 Legal basis and principles of processing

Our remarks

- When relying on consent as a legal basis, several connected requirements must be met. One of these is that data subjects should be able to give consent to different processing purposes individually (granulated consent), rather than accepting a single agreement where several processing purposes are 'bundled' together. Note also that it must be as easy for the data subject to revoke their consent as it is to grant it in the first place. It is advisable to inform the data subjects of their right to withdraw consent at the time of obtaining it. Once consent is withdrawn, the data controller must ensure that the data is erased, unless there is another legal basis for processing the data. Please consult GDPR, Articles 4(11) and 7 for more information on what constitutes valid consent under the Regulation.

- Data controllers must consider the reasonable expectations and interests of data subjects when determining the validity of a legitimate interest as a legal basis, ensuring that the legitimate interest aligns with the expectations of the data subjects. Data controllers should refrain from using abstract language, but instead explicitly describe the activities for which personal data is processed, such as targeted advertising. This transparency is essential for data subjects to understand how their personal data may be used by other entities and to exercise control over their personal data. Please consult GDPR, Article 6(1)(f) for more information about legitimate interests as a legal basis.

- It is crucial for data controllers to provide adequate information to data subjects about the different ways personal data may be processed, before and after its trade. This includes clear information about the categories of recipients of personal data, allowing data subjects to identify partners of the data controller. When distributing products through hospitals and gynecologists, it is possible that individuals may get a misleading impression about the entities involved. Specifically, they may perceive Family Service as a non-profit organization or a governmental initiative rather than a private company that trades personal data. Therefore, companies should be transparent about the advantages associated with the exchange of personal data.

Parking ticket control company fined for several GDPR violations

Summary

A company responsible for parking ticket controls issued a fine for illegal parking to an individual ('the data subject'). However, the data subject claimed that he had never received the fine. He first learned about the fine when a debt collection agency sent him a reminder letter, which included additional fees. It was later discovered that this reminder letter was sent out just a day after the original fine was issued. Thus, information about the data subject's name and address had been processed unnecessarily during the period in which individuals can pay the fine before a reminder is sent, contrary to the principle of data minimization in GDPR, Article 5(1)(c).

The data subject contacted the parking control company, requesting information about the data being processed about him. When the request was not properly fulfilled—partly due to the data controller's inaccurate instructions regarding the correct communication channels, and partly due to an incorrect interpretation of the exemption to the data subject's right to access. As a result the data subject filed a complaint about the data controller with the Belgian Data Protection Authority (DPA).

As separate data controllers, both the parking control company and the debt collection firm were investigated and sanctioned by the DPA.

Decision of the Belgian DPA

The parking control company **was fined 50,000** EUR for the following violations:

- Failing to comply with the data subject's right to access *(GDPR, Articles 14(1) and (2) in conjunction with Article 12(1) and (3))*.
- Unnecessarily processing the personal data of the data subject *(GDPR, Article 5(1)(c))*.
- Failing to implement appropriate technical and organizational measures, considering the nature, context, and purpose of processing *(GDPR, Articles 5(2) and 24(1) and (2))*.

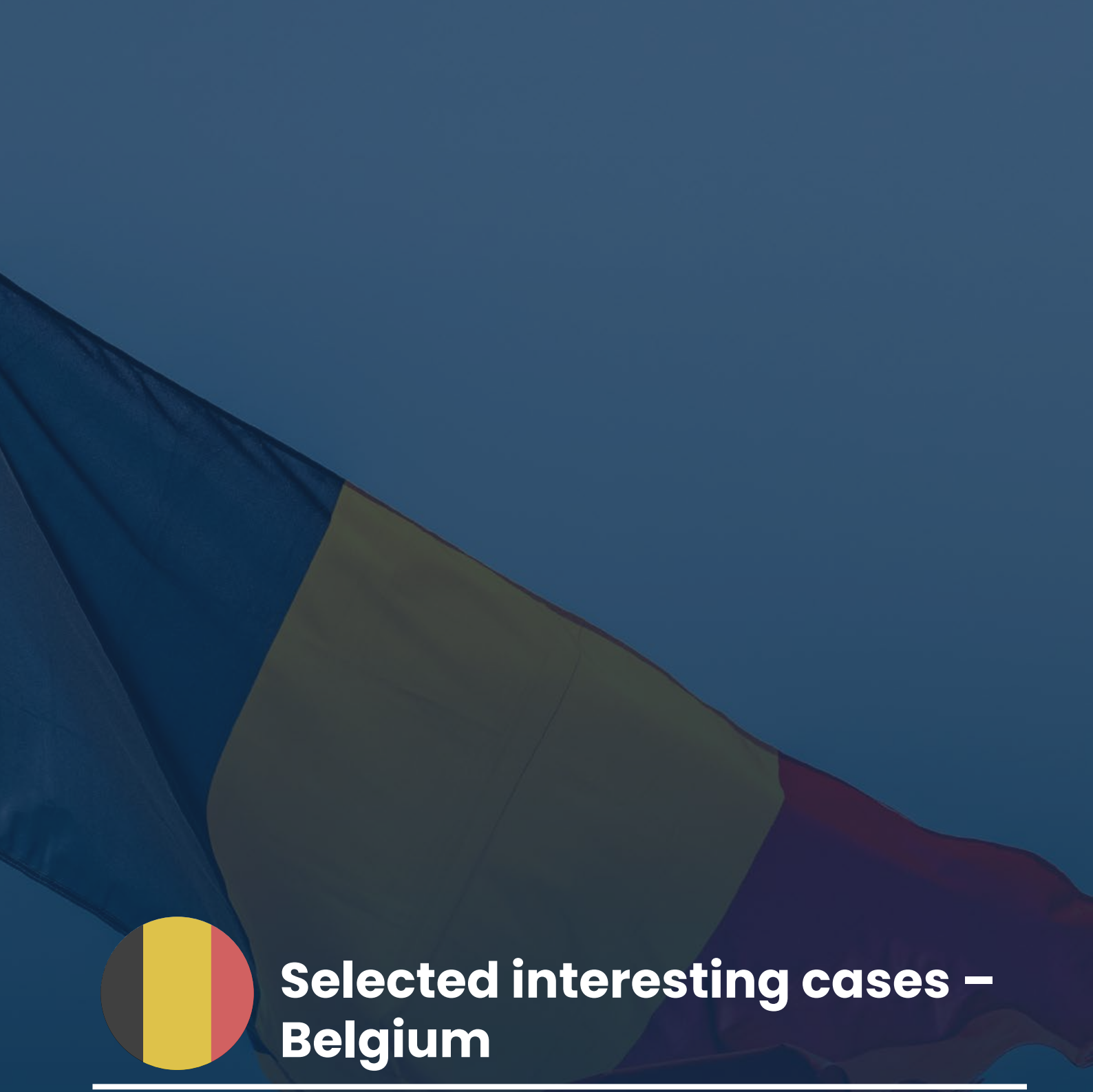
The debt collection firm was **fined 15,000** EUR for the following violations:

- Requesting excessive amounts of information about the data subject *(GDPR, Article 5(1)(c))*.
- Processing data without a legal basis *(GDPR, Article 6)*.
- Failing to provide the data subject with adequate information *(GDPR, Article 12(3) in conjunction with Article 14))*.
- Failing to implement appropriate technical and organizational measures, considering the nature, context, and purpose of processing *(GDPR, Articles 5(2) and 24(1) and (2))*.

Our remarks

- Data controllers must establish standardized internal procedures to effectively accommodate data subject's exercise of their rights under GDPR. This involves providing the data subject with clear information about to whom and using which communication channels their right to access can be exercised.
- Data controllers should remain cautious when interpreting the exemptions to the rights of data subjects. The restriction of data subjects' rights is regulated in Article 13 of the Belgian Data Protection Act. These exemptions must be understood restrictively as they deprive the data subjects of their rights to information, including information about the existence of other rights such as the rights to rectification, objection, or erasure.

Published: 23-12-2020 **Journal number:** DOS-2019-02751 **Tags:** 01 Legal basis and principles of processing



Selected interesting cases – Belgium

06

EU DisinfoLab fined for processing and classifying tweets and Twitter accounts according to political orientation

Summary

In an effort to combat the issue of online fake news, a Belgian NGO called EU DisinfoLab undertook an analysis of a large number of 'tweets' posted on Twitter now concerning the "Benalla affair". This criminal case involved a senior French security officer employed by the President of France. As part of their study, the NGO categorized Twitter accounts according to users' political, religious, ethnic, and sexual orientations, with the aim of identifying the political affiliations of the Twitter users in question.

The study, published in 2018, included personal data from over 55,000 Twitter accounts. The NGO performed several processing activities for this study, including processing the publicly available information from Twitter, as well as publishing an Excel spreadsheet online, which contained the raw personal data extracted from Twitter. This spreadsheet was published in response to challenges regarding the integrity of the study.

Following more than 240 complaints from data subjects, the Belgian Data Protection Authority (DPA) launched an investigation in collaboration with its French counterpart, CNIL.

Collaborative decision of the Belgian DPA and the French DPA

The DPA's imposed a **fine of 2,700** EUR on EU DisinfoLab for the following violations:

- For activities related to the conduct of the study:
  - Not having a privacy policy (GDPR, Articles 5(1)(a), 12 and 14).
  - Not having carried out a balancing of interests (GDPR, Article 6(1)(f)).
  - Not having contracts in place with data processors (GDPR, Article 28(3)).
  - Not having a record of processing activities (GDPR, Article 30).
  - Not implementing sufficient technical and organizational measures within the non-profit organization (GDPR, Article 32).
  - Not having carried out an impact assessment (GDPR, Article 35).
  - Not observing the principle of accountability (GDPR, Articles 5(2) and 24).

The DPA **imposed** a fine of **1,200** EUR on an individual researcher who was deemed the data controller for the publication of the Excel file containing raw personal data, alongside the NGO. The researcher was fined for the following violations:

- *GDPR, Articles 5(1)(a), 5(1)(c), 5(1)(f), 6(1), 9, 12, 14, and 32.*

Our remarks

- The public nature of personal data posted on social networks such as Twitter does not mean that such data is not protected by the GDPR. When processing personal data obtained from such platforms, the general principles must be observed, and an appropriate legal basis identified.
- In cases where personal data is processed for journalistic purposes, exemptions to the GDPR may apply. In the present case, the Data Protection Officer (DPO) acknowledged that the NGO was exempted from the obligation to individually inform the data subjects pursuant to GDPR, Article 14. This exemption was granted to protect the integrity of the study. Nonetheless, the DPA concluded that the publication of sensitive personal data used in the study, without proper pseudonymization, did not have a legal basis. According to the DPA, the legal publication of such sensitive data without pseudonymization would have required the consent of the individuals concerned.

Company fined for restoring data on a former managing director's work laptop

Summary

A former managing director of a private company filed a complaint with the Belgian Data Protection Authority (DPA) against his former employer. After being dismissed by the employer, the employee had erased a substantial amount of data on his work laptop before returning it to his former employer. The employee claimed to have only erased his private data, whereas the employer claimed that both private and professional data had been erased. During the investigation, the employer presented two employee testimonies stating that the former employee had deleted both private and professional email accounts.

Due to a possible civil case between the former employee and the employer, the employer restored the deleted data, resulting in the former employee invoking his right to erasure, restricting the processing of his personal data, and objecting to the processing of personal data. The employer refused to comply with these requests based on the employment contract between the parties, as well as referring to GDPR, Article 6(1)(f), which, in the employer's opinion, justified the processing of the personal data of the former employee.

The Belgian DPA **Imposed** a fine of **7,500** EUR on the employer for processing the personal data of the former employee without sufficient legal basis. The case was later appealed to the Court of Appeal.

The Court of Appeal found that the DPA had not fixed the start date of the processing and failed to assess the legitimate interest of the employer in restoring and processing personal data about the former director due to the possibility of a civil claim.

The Court found that the employer had a legitimate interest in restoring and processing the personal data of the former employee.

Final decision of the Court of Appeal

The Court **annulled** the decision of the DPA.

Our remarks

- After the end of employment, the employer maintains a legitimate interest in storing personal data about the former employee. This can be for several reasons:
    - First and foremost, the employer may be required by law, such as tax law, to retain certain personal data. Additionally (as in this case), the employer may have a legitimate interest in storing personal data that could be relevant to potential legal proceedings, such as a claim for damages.
- When deciding on the appropriate duration for retaining personal data about a former employee, a data controller should consider the time limits specified in existing laws. For example, in tort law, there is often a limitation period that defines the timeframe in which a claim can be made. After this period, there is no reason to store the personal data any longer.
- Data controllers should have practices and policies in place for how to handle former employees' data. It is advisable for companies to regulate the scenario of resignation, dismissal, or any other form of termination of employee activity and its consequences in an internal instruction relating to the use of electronic devices. For example, prohibiting the employees from using work e-mails from sending personal mail. Thereby, one is not in doubt if the e-mails stored are work-related or entirely private. Implementing a policy removes any potential confusion around the classification of stored emails as either work-related or private.
- If e-mails are kept after the end of employment, access to them should be limited to a selected few trusted employees.

Published: 07-04-2022 **Journal number:** DOS-2020-02892 (overturned by 2022/AR/549) **Tags:** 01 Legal basis and principles of processing, 02 Right of access and obligation to provide information, 03 Right to erasure and rectification

CCTV operator fined for illegally installing cameras

Summary

An individual filed a complaint to the Belgian Data Protection Authority (DPA) regarding the installation of surveillance cameras in an apartment building by one of the owners. The complaint was filed against Mr. Z, the delegated manager of the company overseeing the apartment building. Mr. Z was also responsible for determining the placement and usage of the cameras during the initial construction and development phase of the apartment complex.

The complaint was not concerned with the use of cameras but rather the fact that only Mr. Z had access to the recorded camera footage. As a homeowner association was being established for the apartment complex, arguments were made that the role of data controller should belong to this association rather than Mr. Z. Additionally, it was disputed whether Mr. Z had carried out the surveillance activities in a lawful manner, particularly whether a legal basis could be identified.

Mr. Z contended that the installation of surveillance cameras was in the best interest of the homeowners, claiming that their consent had been obtained through the signing of the purchase contracts which incorporated clauses related to security and home safety regulations. Despite Mr. Z's claim that neglecting to provide such surveillance cameras would constitute a breach of his contractual obligations, the DPA determined that the necessary consent was not actually given, making the data processing unlawful.

Decision of the Belgian DPA

A fine of 50,000 EUR was **imposed** on the operator for processing personal data without a valid legal basis *(GDPR, Article 6(1))*.

Our remarks

- The case highlights the complexities of data privacy and protection in the context of shared living spaces. In these circumstances, understanding the roles of various parties connected to the administration of a living complex is crucial. The identity and responsibilities of the data controller must be clearly defined. This is essential in order for the rights of individuals under the GDPR to be respected, for example in relation to the processing of personal data through the installment and monitoring of video surveillance systems.

Published: 09-07-2020 **Journal number:** DOS-2019-02649 **Tags:** 01 Legal basis and principles of processing

Private individuals fined for installing video cameras on private property

Summary

The Belgian Data Protection Authority (DPA) received a complaint regarding three surveillance cameras in a residential area. According to the complainants, the cameras were filming "the entire property" where the complainants resided. Additionally, one camera was filming "the entire street" on which the property was situated. Images captured by the cameras were presented during an exchange between the parties relating to an environmental lawsuit, where also governmental representatives and traffic experts participated. These images contained personal data as the cameras captured individuals moving on the public road and private properties. The complainants argued that the images not only provided evidence of the unlawful recording of public roads and private property, but also the unlawful transfer of these recordings to unauthorized parties.

Decision of the Belgian DPA

The owners of the surveillance cameras were **fined 1,500** EUR for not having a legal basis for transmitting images containing personal data to third parties *(GDPR, Article 6(1))*.

Our remarks

- When installing surveillance cameras, the owner/operator is responsible for ensuring that the principles of lawfulness, fairness, minimization, and transparency as outlined in GDPR, Article 5, are observed. The purpose of processing personal data in the context of surveillance must be clearly defined and align with a legitimate interest recognized by the GDPR.
- The case offers procedural insights into scenarios where private individuals are found to have breached GDPR obligations. The Belgian DPA sent a form to the defendants, allowing them to respond to a proposed fine of 2,000 EUR. The arguments presented by the defendant were taken into account by the DPA and ultimately resulted in a reduction in the amount of the fine. Notably, the Belgian DPA considered the financial situation of the defendant when deciding the final amount of the fine.

Published: 24-11-2020 **Journal number:** DOS-2019-04412 **Tags:** 01 Legal basis and principles of processing

Music company wrongfully fined for management of musician's social media fan page

Summary

The Facebook fan page of a musician was controlled by a music company through a contractual relationship. After termination of the management agreement, the musician wanted to reclaim control over the fan page.

The Belgian Data Protection Authority (DPA) issued an order for the music company to transfer the page on the basis of data portability. The case was brought before the Court of Appeal who annulled the DPA's decision.

The DPA revisited the case and issued a second decision, fining the music company 10,000 EUR for not transferring the fan page after the musician had exercised their rights to data portability and objection. The fine was imposed because the music company was found to have used the artist's name without their consent after the termination of the management contract.

The music company appealed the second decision, arguing that their right to manage the Facebook page was not based on the management agreement. Rather, it was based on the company's exclusive license to market and commercialize the artist's music, which was derived from various agreements with the artist and a music producer.

The music company argued that the termination of the management agreement did not affect their rights to the Facebook fan page, and that it had a legitimate interest to control the page based on their intellectual property rights to the artist's music.

The second decision was once again brought before the Court of Appeal which annulled the decision, referencing an agreement which confirmed that the music company had exclusive rights to the commercial use of the artist's name and image for a specified period of time.

Decision of the Court of Appeal

The Court of Appeal **annulled** the decision of the DPA, **including the fine of 10,000** EUR.

Our remarks

- The rights contained in the GDPR are considered fundamental for data subjects. However, these rights must always be balanced with other rights, such as intellectual property rights. In cases, such as the present, where the personal data processing is limited in scope, the data controller's legitimate interests may outweigh those of the data subject, particularly when those are necessary for the exercise of their intellectual property rights.
- This case illuminates the nuanced interplay between GDPR provisions and pre-existing contractual commitments. When establishing contracts, especially those involving personal data and associated digital assets, clarity is paramount. The dispute emphasizes the need to proactively align GDPR-compliant practices with the specific terms of contractual agreements. In essence, ensuring that GDPR guidelines are embedded within contracts, while respecting the essence of existing rights and obligations, can be a critical step in mitigating such conflicts.

Published: 12-01-2021 **Journal number:** DOS-2020-01192 **Tags:** 01 Legal basis and principles of processing

Meta Platforms Ireland Ltd. fined for unlawful data processing

Summary

In 2018, a Belgian Instagram user filed a complaint against Meta, alleging that Instagram's processing practices amounted to 'forced consent'. The complaint was initially filed with the Belgian DPA, which referred the case to the Irish DPA.

Similarly, an Austrian Facebook user complained about Meta, arguing that the processing practices on the Facebook platform and the consent required to access the platform could not be considered 'freely given', in turn also constituting 'forced consent'. The complaint was filed with the Austrian DPA, who also referred the case to the Irish DPA.

In both cases, the data subjects were represented by the Austrian Data Privacy NGO NOYB (None of Your Business).

Prior to the GDPR entering into force, Meta Ireland modified the Terms of Service governing its Facebook and Instagram services. As part of this change, Meta Ireland informed users that it was altering the legal basis used to legitimize the processing of their personal data. Previously, Meta Ireland relied on user consent for processing personal data in relation to the provision of Facebook and Instagram services, including behavioral advertising. However, it sought to switch to the "contract" legal basis for most of its processing activities.

To continue accessing Facebook and Instagram services after the implementation of the GDPR, existing and new users were required to indicate their acceptance of the updated Terms of Service by clicking "I accept." Users who declined to accept would not be able to access the services.

Meta Ireland considered that by accepting the updated Terms of Service, a contractual agreement was established between Meta Ireland and the user. It also argued that the processing of users' data in connection with the provision of Facebook and Instagram services, including personalized services and behavioral advertising, was necessary for fulfilling that contract. Therefore, Meta Ireland maintained that such processing operations were lawful under GDPR, Article 6(1)(b), which designates the "contract" legal basis for processing.

However, the complainants disputed Meta Ireland's claims and argued that Meta Ireland was still seeking to rely on user consent as the legal basis for processing their data, contrary to its stated position. The complainants contended that by making accessibility to its services conditional upon accepting the updated Terms of Service, Meta Ireland was effectively pressuring users to consent to the processing of their personal data for behavioral advertising and other personalized services, thereby violating the provisions of the GDPR.

In October 2021, the Irish DPA issued a draft decision, which received objections from ten other DPAs. Subsequently, the cases were referred to the European Data Protection Board, which adopted a binding decision on 5 December 2022. The Irish DPA published the final decisions on 11 January 2023.

Final Decision

The two decisions in question were both issued by the Irish DPA, which **fined** Meta **210,000,000** EUR for breaches related to its Facebook Service and **180,000,000** EUR for the breaches related to its Instagram service. The fines were issued for the following violations:

- Lack of a legal basis for the processing (GDPR, Article 6(1)(b)). The Irish DPA and EDPB addressed whether Meta could rely on the fulfillment of a contract as the lawful basis for processing personal data. The Irish DPA agreed with Meta that processing was necessary for contract performance, while the EDPB disagreed. The EDPB highlighted that behavioral advertising was not essential to the contract.
- Failure to provide meaningful information about the processing operations, making it impossible for the users to understand what data was processed and on what legal basis, as the information provided was lacking in clarity and conciseness (GDPR, Articles 5(1)(a), 12 and 13).
- Infringement of the principle of fairness as the 'take it or leave it' model, which created a significant imbalance between the platforms and their users (GDPR, Article 5(1)(a)).

Additionally, the DPA **ordered** META Ireland to bring its processing operations into compliance within a three-month period.

Besides the DPA decision, the **EDPB directed the Irish DPA** to investigate Facebook and Instagram's data processing activities in regard to special categories of personal data that may be processed by these services. This is, however, inconsistent with the jurisdictional structure laid down by the GDPR, which is why the Irish DPA considered it appropriate to bring an action for annulment before the European Court of Justice. It is therefore not clear whether such an investigation will be conducted.

Our remarks

- When relying on the fulfillment of a contract as a legal basis, ensure that the processing is in fact necessary for the performance of the contract.
    - The necessity of processing is to be determined by reference to a particular contract. In this case, the Irish DPA took a broad approach to determine what was necessary, based on "the nature of the services provided and agreed upon by the parties". The DPA then stated that "it seems that the core of the Facebook model is... an advertisement model". The EDPB, however, argued that the main purpose of the services was to enable their users to communicate with others. Additionally, the EDPB specified that the understanding of necessity should be interpreted in a manner that fully reflects the objective pursued by the GDPR, stating that the draft decision by the Irish DPA posed a risk of potentially legitimizing any collection and reuse of personal data.
- In this case, the combination of factors, such as the asymmetry of the information created by Meta regarding Facebook service users combined with the 'take it or leave it' situation that they are faced with, was argued to be systematically disadvantageous for Facebook service users, limiting their control over the processing of their personal data and undermining the exercise of their rights.
    - When assessing the contract between the controller and data subject, ensure that the contract is not asymmetrical by considering principles relating to processing of personal data in conjunction with the data subject's actual ability to exercise their rights.

Beverage company fined for using eID cards to create customer loyalty cards

Summary

A customer lodged a complaint regarding the use of loyalty cards by a beverage company. The loyalty cards were issued by reading the eID cards, which are the official national identification cards in Belgium for individuals. The complainant argued that the company collected more information than necessary when creating the loyalty cards, including clients' social security numbers, gender, and date of birth. The complainant also argued that valid consent for processing this data was not obtained.

Decision by the Belgian DPA

The Belgian Data Protection Authority (DPA) found that the company had violated both the principle of data minimization and that the consent of their customers could not be considered 'freely given' in accordance with the GDPR. The DPA imposed a fine of 10,000 EUR on the company.

Court of Appeal

The decision was appealed to the Court of Appeal of Brussels. They annulled the fine as they found that (i) The new eID legislation could not retroactively apply. (ii) The fine lacked adequate justification. (iii) The shop owner did not process the data associated with the complainant's eID as the data subject had declined to provide it.

The DPA then appealed the decision from the Court of Appeal to the Belgian Supreme Court.

The Supreme Court found that the Court of Appeal of Brussels failed to consider potential violations of data minimization and freely given consent under the GDPR. The Supreme Court also highlighted that the loss of benefits, like discounts, should be considered in evaluating freely given consent. They also affirmed the authority of the Belgian DPA to handle complaints even when no personal data has been processed.

The decision of the Belgian Supreme Court

The Supreme Court **annulled** the decision of the Court of Appeal and referred it back to the Court of Appeal. The case is pending at the time of writing.

Our remarks

- When creating loyalty programs, one must observe the GDPR principles of data minimization by using only necessary data, limiting retention time, and using data for specific purposes shared by the data subject. For example, it is rarely necessary to process the social security numbers of customers for providing a loyalty program.
- If one wants to use consent for processing personal data one should consider the following:
  - Consider whether consent is required for each processing step. If not, assess if one can use other legal bases such as contract (GDPR, article 6(1)(a) or legitimate interest (GDPR, article 6(1)(f)).
  - When seeking permission from (potential) customers, ensure they have access to and understand your clear and detailed privacy policy before making a choice. Active and voluntary consent is essential, avoiding preselected choices or implied consent. People should have the freedom to choose whether to provide consent, except in cases where data is absolutely necessary.
  - To use the personal data of existing customers in direct marketing (newsletters), explicit consent may not be required. However, explicit consent is necessary for non-customers and other marketing purposes such as profile building or data sharing with partners. Obtain separate consent for these activities, clearly stating the scope in the privacy policy.

Published: 07-10-2021 **Journal number:** C.20.0323.N/1 **Tags**: 01 Legal basis and principles of processing

- Regardless of what legal basis you use, document your decisions and choices. Accountability is a key aspect of the GDPR, and you should be able to provide justifications and explanations for your actions at any given time. Maintain a comprehensive and detailed data register, as it is a fundamental obligation for nearly all data controllers.

- Exercise caution when using eID card readers, especially when creating loyalty cards or engaging in customer promotions. It is advisable to avoid such practices if possible. If you decide to implement electronic loyalty cards, ensure that the software vendor you choose has adhered to the fundamental principles of data minimization and privacy by design during the software's development.

Medical laboratory fined for several GDPR violations

Summary

An individual filed a complaint against a medical analysis laboratory. The complainant alleged that the laboratory violated principles of confidentiality and transparency. Specifically, the complainant argued that the laboratory had not conducted a data protection impact assessment, that inadequate information was provided to data subjects, and that sensitive personal data, namely health related information, was processed using an insecure website.

The complainant had interacted with the laboratory multiple times for medical analyses and was informed that their doctor had electronic access to their test results. However, the complainant discovered that the laboratory's website, named "Cyberlab," had a page for accessing medical analysis data using an unsecured HTTP protocol.

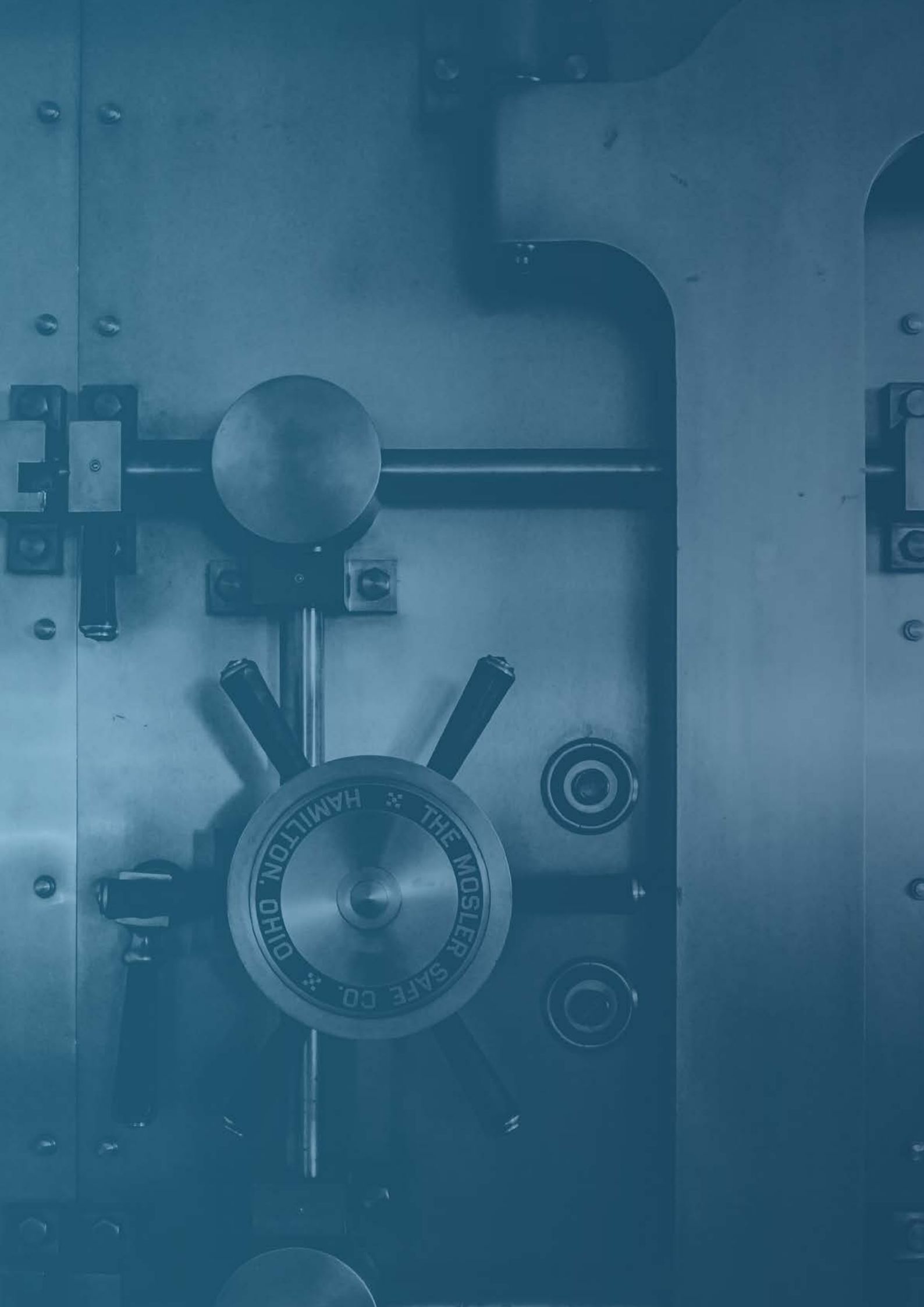
Decision of the Belgian Data Protection Authority

The DPA **imposed** a **fine of 20,000 EUR** on the medical laboratory for the following violations:

- Failing to comply with the principles of confidentiality and integrity *(GDPR, Article 5(1)(f))*.
- Not respecting the data subject's right to information *(GDPR, Articles 12-14)*.
- Lacking adequate data security measures, such as two factor authentication *(GDPR, Article 32)*.
- Failing to carry out an impact assessment *(GDPR, Articles 35(1)* and *(3))*.

Our remarks

- The case highlights a key aspect of the GDPR, namely the accountability principle listed out in GDPR, Articles 5(2) and 24 and the fundamental obligation of data controllers to clearly identify their responsibilities under the GDPR. If data controllers are not aware of the extent of their obligations, the effective protection of data subjects will be compromised.
- When special categories of information are processed, such as health data, appropriate technical and organizational measures should be observed to protect the security and integrity of the data. Complying with GDPR, Article 32, will require additional measures in these situations, compared to situations where sensitive data is not processed.


THE MOSLER SAFE CO.
HAMILTON, OHIO

Employer reprimanded for discussing sensitive personal data about an employee during internal HR meeting

Summary

The HR team of a medium-sized public organization held a meeting to discuss the dismissal of a senior consultant, during which she was not present. The meeting referenced and cited paragraphs from a report conducted by an external service for prevention and protection at work, documenting the employee's extended absence and indefinite incapacity to work as determined by the company doctor.

The details discussed in the meeting were documented in the minutes of the meeting, which were shared with all employees in the department, irrespective of their attendance at the meeting. Furthermore, the minutes were posted on the organization's Intranet, accessible to employees from all departments within the organization.

Decision of the Belgian Data Protection Authority

The Belgian Data Protection Authority **issued** a **reprimand** to the employer since it lacked the authority to impose fines on public organizations.

Our remarks

- This case offers significant insights about the scope of the GDPR and the admissibility of complaints. The employee had initially filed a complaint to the Belgian DPA based on the verbal statements made during the meeting. This complaint was rejected on the grounds that oral statements are not covered by the GDPR. However, when the employee based her complaint on the minutes of the meeting and their availability on the public authority's server, her complaint was deemed admissible.
- When informing staff about personnel changes, written statements should be limited to factual data while avoiding the disclosure of sensitive personal data regarding the individual involved. If processing special categories of personal data, such as health data, data controllers must ensure that one of the legal bases provided in GDPR, Article 9(2), applies to justify the processing as lawful.

Published: 09-02-2021 **Journal number:** DOS-2018-06125 **Tags:** 01 Legal basis and principles of processing

School fined for processing data about minors without parental consent

Summary

A Flemish educational institution introduced a well-being survey directed at its students who were minors. The survey was carried out using a digital SmartSchool system, which processed the students' personal data. An individual filed a complaint with the Belgian Data Protection Authority (DPA), claiming that the school was processing students' personal data without parental consent and that excessive information was processed beyond the necessary scope, contrary to the principle of data minimization. The complainant also argued that the school should have conducted a data protection impact assessment (DPIA) but failed to do so.

The school argued that the data processing was lawful, referring to a legal obligation as the basis for their processing activities.

The Belgian DPA ordered the school to bring its processing activities into compliance with the GDPR and **issued** an administrative **fine of 2,000** EUR. The decision was appealed to the Brussels Market Court and subsequently referred back to the DPA who reduced the initial fine of 2,000 EUR.

Final decision

A fine of 1,000 EUR was upheld due to the following violations:

- Excessive processing of personal data in light of the processing purpose, contrary to the principle of data minimization *(GDPR, Article 5(1)(c))*.
- Lacking a valid legal basis *(GDPR, Article 6(1))*.
- Failing to obtain parental consent for data processing related to minors *(GDPR, Article 8)*.

Our remarks

- Compliance with the principles set out in Article 5 of the GDPR, particularly the principles of lawfulness and data minimization, is crucial as they constitute fundamental tenets of data protection. Collecting only the necessary and relevant data for the intended purpose and avoiding excessive retention periods is crucial. Violations of these fundamental provisions are likely to be considered as significant breaches by the DPA and may result in fines being imposed.

Published: 06-10-2021 **Journal number:** AR/2021/576 **Tags:** 01 Legal basis and principles of processing

Selected interesting cases – Denmark

07

Publication of old club magazines

Summary

A citizen complained to the Danish DPA that Jyllinge Sejlklub, a sailing association, had published three of its club magazines from 1981 and 1982 on the internet, which contained information about the complainant's name, address, age, and picture, and that the association refused the complainant's request for erasure of the information.

The Danish Data Protection Agency's decision

The Danish DPA did **not** express criticism, as Jyllinge Sejlklub's processing of personal data was carried out in accordance with the rules in GDPR, Articles 6(1) and 17.

Our remarks

- The decision provides an example of how the balancing of interests under GDPR, Article 6(1)(f) can favour the data controller. The Danish DPA emphasized, among other things, that in this case:
  1. the data controller had a legitimate interest in safeguarding, protecting, and informing about its history in a natural context,
  2. the club magazines had been available for almost 40 years, and
  3. the types of personal data in the magazines were of a very non-invasive nature.
- The decision serves as an example of when the data subject may not exercise their right to erasure. In the opinion of the Danish DPA, the prerequisites for erasure, as outlined in GDPR, Article 17(1)(a-f), were not met. The DPA emphasized, among other things, that the data controller still needed to process the complainant's information and that the data controller processed the complainant's data on a lawful basis. The authority also emphasized that the complainant did not provide specific grounds that would override the controller's legitimate interests in processing the complainant's data under GDPR, Article 17(1)(c), and Article 21(1).

Published: 08-06-2020, **Journal number:** 2019-31-2363 **Tags:** 01 Legal basis for processing and principles for processing

Processing of personal data in the context of online competitions

Summary

SmartResponse obtained consent from data subjects who participated in its online competitions to process personal data for marketing purposes. Consent for this was obtained on behalf of SmartResponse and its 45 business partners.

Contestants were asked to provide information and were informed of the consent request on the same page. They were made aware that their personal data would be shared with 45 partners, and a link was provided for information about these partners.

Participants were given the option to complete additional questionnaires for more targeted marketing information but it was not a requirement to participate in the competition.

SmartResponse included a link to withdraw consent on each competition page which could be accessed regardless of whether they entered the contest (again) or not. Additionally, contestants received a confirmation email with information and a link to withdraw consent.

If contestants withdrew their consent, SmartResponse recorded the contestants' phone numbers and email addresses on an internal "no thanks" list. The data was stored for five years based on the limitation period in Section 41(7) of the Danish Data Protection Act.

The Danish Data Protection Agency's decision

The Danish DPA concluded that SmartResponse's processing of personal data based on data subjects' consent was carried out **in accordance** with GDPR, Article 6 (lawful basis).

However, the Danish DPA expressed **serious criticism** that SmartResponse's processing of personal data using the company's internal "no thanks" list had not been carried out within the framework of GDPR, Article 6.

The Danish DPA **imposed an injunction** on SmartResponse to delete the personal data included in the company's "no thanks" list, as the data can only be temporarily stored to clarify whether a specific dispute exists or arises.

The Danish DPA expressed **serious criticism** that SmartResponse's storage of personal data for the purpose of documenting consent was in breach of GDPR, Article 5(1)(e) (storage limitation).

Finally, the Danish DPA **criticized** that SmartResponse did not sufficiently comply with the obligation to inform under GDPR, Article 13, cf. Article 12.

Published: 30-09-2022, **Journal number:** 2020-431-0075 **Tags:** 01 Legal basis for processing and principles for processing

Our remarks

- It is worth noting that a link to SmartResponse's partners provided sufficient information about their partners within GDPR, Article 13. It has earlier been unclear if this was enough to fulfill the obligation to inform.
- Regarding the processing and transfer of data via questionnaires, SmartResponse relied on GDPR, Article 6(1)(f) (legitimate interest), and the exception in Section 13(2) of the Danish Data Protection Act *(transfer of general customer data for direct marketing purposes without the data subject's consent).* When relying on the exception, two conditions must be met:
    - It must be general (customer) information.
    - The transfer must be in accordance with a balancing of interests under GDPR, Article 6(1)(f).
- In this case, the conditions for the use of the exception were not met. The information obtained via questionnaires was not general customer information, as it included detailed personal data such as the data subject's mobile phone provider, TV provider, labor market affiliation, mortgage credit institution (if any), and electricity supplier. Therefore, the transfer did not comply with the balancing of interest rule. SmartResponse should have obtained consent before disclosing this information. Therefore Section 13(2) of the Data Protection Act could not be relied on as the lawful basis for processing.
- Under GDPR Article 7(1), the controller may retain the information regarding obtained consent throughout the processing period for the purpose of providing evidence, as per the requirements for legal consent.
- In contrast, information on the withdrawal of consent may only be kept for a limited period, as there must be a genuine and present interest. This interest may be present for a limited period while it is determined whether a concrete dispute exists or not. The specific length of time for which the data may be kept must be based on a case-by-case basis. The Danish DPA determined that retaining a register of withdrawn consents for five years, in line with the limitation period in section 41(1) of the Data Protection Act is not necessary. Such retention would go against the principle of storage limitation outlined in GDPR, Article 5(1)(e).

Serious criticism for processing personal data about website visitors

Summary

The case originated from the Danish DPA's decision on January 28, 2021, to investigate the website www.alstrom.dk, following a complaint.

During a visit to the website www.alstrom.dk 18 different cookies were placed on the visitor's device before obtaining consent.

Alstrøm used Google Analytics to generate statistical information about website visitors.

The case concerned two consent solutions:

1. The first involved a piece of text giving the website visitor the option to choose "read more about cookies" or "close".

This solution was replaced in January 2021 by a new one where:

2. The "Accept" button was in orange font on a white background, blending in with the white background of the consent solution, while the "ACCEPT ALL" button was in white font on an orange rectangular background, as shown in the image below:

The Danish Data Protection Agency's decision

The Danish DPA expressed **serious criticism** that, until the start of January 2021, Alstrøm's processing of personal data about website visitors on www.alstrom.dk had not been carried out in accordance with the rules in GDPR, Article 6 *(legal basis for processing)*.

The Danish DPA **criticized** that, after January 2021, Alstrøm's processing of personal data about website visitors on www.alstrom.dk had not been in accordance with GDPR, Article 6.

The Danish DPA expressed **serious criticism** that Alstrøm's implementation of the consent solution, at the beginning of January 2021, had not been in accordance with GDPR, Article 5 *(processing principles)*, and Article 6.

Our remarks

- It's important to ensure that cookies are not placed on a user's device before they have accepted them and that all other conditions for obtaining valid consent under GDPR are met. For more information, see our section on the decision against Dating.dk of 21 September 2021.
- When designing a consent solution, the wording used for accepting and rejecting cookies should be carefully considered. Specifically, in this case, the Danish DPA stated that "Accept" and "ACCEPT ALL" did not make it clear whether users could reject cookies. Instead, the data controller could have used "Reject all cookies except necessary" and "Accept all cookies".
- Additionally, the colors for the "accept" and "reject" fields should be carefully chosen. In this case, the Danish DPA stated that the "Accept" field appeared inactive, while the "ACCEPT ALL" field appeared clear and distinct. This created a visual distinction between the two fields, potentially pushing users toward accepting all cookies.
- If using Google Analytics, it should be set up in such a way that information about visitors to the website is not transferred to third parties outside of the EU.

The dating service's legal basis and personal data security

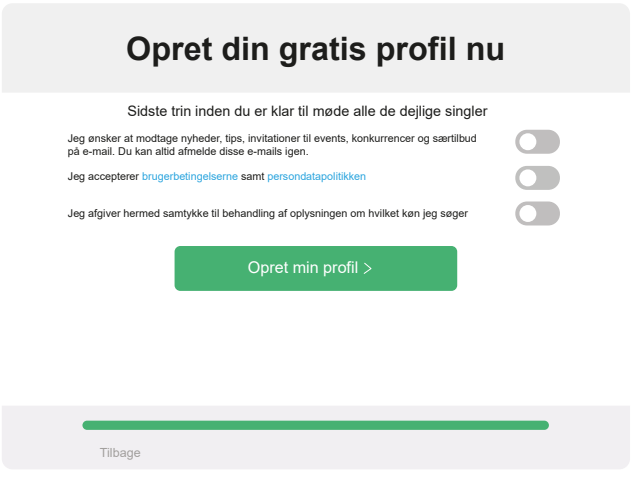
Summary

Dating.dk ApS ("Dating.dk") was among the selected companies supervised by the Danish DPA in the fall of 2018. The planned supervision was aimed at the dating service's processing of personal data that took place in connection with users creating profiles and using the service. The focus was on the dating service's legal basis for processing and personal data security.

Before the supervision, the Danish DPA sent a series of questions to Dating.dk. However, Dating.dk refused to disclose the number of users, considering it a business secret. As a result, the police searched Dating.dk's address enabling the Danish DPA to obtain the required information.

Dating.dk's consent solution was designed as follows:

The user would accept the Terms and Privacy Policy by checking the same box. Additionally, the user should consent to the processing of personal data concerning gender.



Dating.dk's consent solution design

During the audit, Dating.dk asserted that they did not process the personal data of a large number of users, as all profiles were anonymous, and users created a fictitious usernames. Furthermore, they stated that they did not process sensitive or confidential personal data unless users voluntarily provided such information in free text fields.

The Danish Data Protection Agency's decision

The Danish DPA expressed **serious criticism** that Dating.dk's processing of personal data had not been carried out in accordance with the rules in GDPR, Article 6(1) *(legal basis for processing general personal data)*, and Article 9(1) *(prohibition against the processing of special categories of personal data)*.

The Danish DPA ordered Dating.dk to bring their processing of personal data about users in accordance with GDPR, specifically Article 6(1), cf. Article 9(1) by November 16, 2021. They also required Dating.dk to submit a copy of their consent solution by the same deadline if processing continues

The Danish DPA also expressed **serious criticism** that Dating.dk ApS processed personal data, including location information and special categories of personal data, without demonstrating that the processing was conducted with regard to the risks to the data subject's rights and freedom in accordance with GDPR, Article 32(1) and (2) *(security of processing)*.

Our remarks

- If you refuse to provide information about processing to the DPA on the basis that it constitutes a trade secret, then it may lead to an investigation or search.
- If there is a service where users can be created, you will almost always process personal data about these users, such as a username or an e-mail address as the clear starting point constitutes personal data. Regardless of whether a username or an email address in the specific case can be characterized as personal data, you will always process personal data in the form of users' IP addresses.
- You are a data controller for the personal data that users provide in free text fields. This is the case even if they are optional.
- The Danish DPA thinks that dating sites process sensitive information about sexual relations or sexual orientation by virtue of being a dating site.
- When basing your personal data processing on the consent of the data subject, this consent can be given by the data subject ticking a box. However, you should pay attention to how your consent solution is designed. Here are some good rules of thumb:
  - In the consent solution, user Terms and Privacy Policy must not be accepted by ticking the same box. Instead, they should be presented as separate options and thereby allow the user to make a choice.
  - If both general and sensitive personal data are processed, the user must consent to these individually.
  - If personal data is processed for multiple purposes, the user must also consent to these individually.

Næstved municipality: Public interest and cookies

Summary

In October 2020, the Danish DPA initiated an own-initiative case against Næstved Municipality regarding its processing of personal data about website visitors.

The website displayed the following text to visitors of the website:

"This website uses cookies to improve your experience, to assess the use of the individual elements of the website, and to support the marketing of our services. By clicking further on the website, you agree to the website's use of cookies."

The basis for processing for Næstved Municipality's collection of personal data via cookies was stated as GDPR, Article 6(1)(e) and was therefore for the purpose of performing a task carried out in the public interest, including for the purpose of providing information about the municipality's performance of municipal tasks. The purpose was pursued by, among other things:

- Maintaining the overall security of the website, for example by identifying illegal and malicious traffic.
- Measuring the impact of communication efforts based on data on the pages and links citizens use.

The use of cookies on Næstved Municipality's website was set up in such a way that individual cookie data set was collected by Siteimprove, which generated irreversibly anonymized statistics for the municipality.

Siteimprove used Amazon Web Service (AWS) Frankfurt as a sub-processor, which was disclosed in the data processing agreement between Næstved Municipality and Siteimprove. The agreement ensured that personal data was only stored in the EU. AWS Frankfurt provided guarantees in the agreements and publicly that this restriction would be maintained and that there was no transfer of data to countries outside the EU, including the United States.

The Danish Data Protection Agency's decision

The Danish DPA **criticized** Næstved Municipality, in connection with the processing of personal data about website visitors, which did not comply with GDPR, Article 5(1)(a) *(personal data must be processed lawfully, fairly and in a transparent manner)*.

The Danish DPA also concluded that Næstved Municipality's processing of personal data about website visitors for statistical purposes was within the scope of GDPR, Article 6(1)(e) *(processing is necessary for the performance of a task carried out in the public interest or the exercise of official authority vested in the controller)*.

Our remarks

- The Danish DPA criticized Næstved Municipality for stating that cookies were collected for marketing purposes, even though this was not the case. Thus, the data controller must ensure that their cookie information or a privacy policy accurately reflects the purposes of the personal data processing involved.
- Public authorities may use their authority to perform official tasks as a legal basis for processing personal data by collecting statistical cookies, as long as they can demonstrate that the cookies contribute to the performance of their tasks. In this case, measuring impact on communication and ensuring security on the website was within the task of the municipality.
- If personal data is processed for statistical purposes, it is good practice to anonymize the data to ensure that personal data is not processed more extensively than necessary.
- The Danish DPA concluded that Siteimprove did not transfer to third countries in connection with its use of AWS.

Unauthorized access to video surveillance

Summary

An employee in Salling (Danish supermarket) allowed a former employee to enter the store through the staff entrance. The former employee was shown video surveillance footage from the store, which included images of the former employee's ex-girlfriend shopping with a friend.

Despite the incident, the Danish DPA concluded that Salling had taken appropriate organizational and technical measures to ensure a level of security appropriate to the risks inherent in the processing of personal data in question and that the company could not be held responsible for the incident in question.

In addition to many of the measures taken by Salling, the Danish DPA emphasized that an employee deliberately and against company guidelines violated the guidelines in several ways, such as giving a former employee access to the building. The Danish DPA also concluded that the employee took several actions that went beyond what Salling could reasonably be expected to have been prepared for or taken measures to avoid.

The Danish DPA therefore only criticized the fact that Salling did not report the breach until 10 days after the company became aware of the incident.

The Danish Data Protection Agency's decision

The Danish DPA **criticized** Salling for not complying with GDPR, Article 33(1), as Salling did not report the security breach to the Agency until 10 days after the company became aware of the incident.

The Danish DPA **concluded** that Salling's processing of personal data had been carried out **in accordance** with GDPR, Article 32(1) on security, and Article 34(1) on notification of breaches to data subjects.

Our remarks

A controller is not held liable for exceptional or unforeseeable actions of employees that lead to a personal data breach if the controller itself has taken appropriate organizational and technical measures. The division of liability between employer and employee is thus similar to the principal liability in tort law.

- It must be possible to document to the Data Protection Authority what measures have been taken. This documentation must be easily accessible and must be produced within a reasonable time.
- The ISO/IEC 27001 standard can be a useful tool for ensuring and documenting proper information security. The standard is not in itself a requirement under the GDPR. However, it can be useful for many reasons and can also be a prerequisite for compliance with ISO/IEC 27701, which is an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy protection and can be used to ensure compliance with the GDPR.

Published: 18-06-2020, **Journal number:** 2020-441-4652 **Tags:** **05** Data security

Complaint about failure to erase

Summary

A former employee complained about DMR A/S's failure to delete video recordings and images of him that were included in a series of films on the company's website, Facebook page, and YouTube.

On the 7th of June 2018, the complainant signed a consent declaration for the publication of images and videos. The complainant had authorized DMR A/S to use video recordings of him for use on the company's website, in leaflets, newsletters, or other externally targeted informative material.

On the 6th of September 2019, the complainant asked DMR A/S to remove a film from YouTube in which he appeared, as his employment relationship with DMR A/S had ended. DMR A/S replied that they would cut the complainant out of all films.

On the 10th of September 2019, the complainant wrote to DMR A/S informing them that he had still not been removed from DMR A/S' commercials. DMR A/S stated the same day that the company was "in progress" and asked the complainant to be patient.

On the 17th of September 2019, DMR A/S informed the complainant that he had now been removed from the employee film. On 11 December 2019, the Danish DPA nevertheless concluded that the complainant still appeared in a video on DMR A/S's website and on YouTube, after the complainant had contacted the Danish DPA on September 27. The video was subsequently deleted.

The Danish Data Protection Agency's decision

The Danish DPA **seriously criticized** the fact that DMR A/S' processing of the complainant's request for erasure had not been carried out in accordance with GDPR, Article 17(1) *(right to erasure)*.

Our remarks

- According to the Danish DPA, if the data subject withdraws his or her consent, erasure pursuant to GDPR Article 17(1)(b) must take place immediately after the withdrawal. It is not specified how long this is, but in this specific case, three months was too long.
- It can be difficult to remove a person from a video while maintaining the original quality of the video. The Danish DPA did not appear to consider whether significant resources are needed to remove a person from a marketing video or if the marketing video becomes ineffective when a person featured in it withdraws their consent. A data controller who wants to produce marketing videos or the like should therefore consider that a person who appears in the video based on his or her consent may demand that he or she no longer appears in the video.
- If your company wants to use images or videos for marketing purposes on the internet, it should consider the risk that it may have to delete the video or cut a person out of the video, which could render it meaningless.

Considering this risk, we suggest the following should be considered:

- **If the processing is based on the legitimate interests of the organization:** Marketing is a legitimate interest, so the basis for processing is not useless. However, a former employee will typically have a fairly strong interest in not appearing in a significant role in marketing material from a company that no longer employs them. Legitimate interests should therefore oftentimes only be used as a basis for processing in the case where individuals involved have a more discreet role in the material, for example, an employee working in the background, or where participation in marketing is a natural part of the job of the individuals involved.

- **If the processing is based on a contract with the employee:** If the processing relates to an employee who has a more prominent role in, for example, a video, the organization may choose to enter into a contract with the employee instead of consent. This is likely to require, firstly, that the employee receives some form of payment for their participation. Secondly, there must be a written agreement to demonstrate that the processing is carried out based on a contract.
- **If the processing is based on consent:** take into account the risk that one or more of the employees appearing in the material may have to be removed.

Gladsaxe Municipality: Court ruling in the Gladsaxe case

Summary

The case concerned a personal data breach in Gladsaxe Municipality, where four computers were stolen from the municipality's town hall. One of these computers contained a spreadsheet with information on approximately 20,000 citizens. This information was not encrypted and the spreadsheet contained information such as civil registration number, age, and gender.

Seven individuals subsequently sued Gladsaxe Municipality, claiming compensation for non-material damage under GDPR, Article 82. The individual claimants had made claims in the range of DKK 7,500 and DKK 30,000.

The Danish Data Protection Agency's decision

The Court concluded that Gladsaxe Municipality **had not acted in breach** of the principles for processing personal data in GDPR, Article 5(1)(a), (b), or (c) *(processing principles)*. The processing had also been carried out in accordance with GDPR, Article 6(1)(f) *(legitimate interest)* and Article 9(2)(f) *(processing is necessary for the establishment of legal claims)*, and Section 5(1) of the Danish Data Protection Act *(processing in accordance with purpose)*.

The Court concluded that the municipality, as data controller, **had not complied** with the GDPR's requirements for the security of processing within the meaning of GDPR, Article 32(1) and (2) *(security of the processing)*, cf. Article 5(1)(f).

After an overall assessment of the data security breach and in comparison, with the nature of the information on each of the applicants to which the breach related, there was no basis to conclude that the applicants had suffered damage that could justify compensation. Consequently, the Court held that there was no basis for awarding the applicants compensation under GDPR, Article 82 for non-material damage.

Gladsaxe Municipality was therefore **dismissed** from the plaintiffs' claim for compensation.

Published: 11-05-2021, **Journal number:** BS-19120/2019-GLO **Tags:** 05 Data security

Our remarks

- The Court concluded that GDPR, Article 82(1) must be interpreted as including compensation for non-material damage.
- Collecting personal data on approximately 20,000 citizens in a single Excel sheet does not violate the principle of data minimization. Therefore, a controller may collect large amounts of personal data in individual files if it is necessary to process the data in the same document to fulfill a task.
- Even if an employee breaches internal guidelines, the controller can be accountable if the controller is aware that the unlawful act is being carried out. In this case, employees of Gladsaxe Municipality were prohibited from storing personal data locally on the computers, but at the same time, the municipality was aware that employees had to store the file locally to be able to work in it.
- The district court held that GDPR, Article 82(1) provides for the possibility of awarding compensation/indemnification to the data subject for damages that are not of a non-material nature. This may increase the disadvantages of being criticized, as the data controller will risk being faced with claims for compensation from the data subjects who have been affected by the unlawful processing, even if the Data Protection Authority does not issue a fine.
- The Court stated that the subjective feeling of being infringed is not sufficient to award damages under GDPR, Article 82(1). Instead, it requires that the unlawful act under data protection law has caused damage or imminent risk of damage to, for example, reputation, loss of confidentiality, etc., or other consequences of a certain qualified nature. Specifically, in this case, one of the citizens had DKK 95,000 stolen from his bank account. This loss was compensated, but the citizen's fear of future misuse of his information was not damage of a "qualified" nature according to the District Court's assessment.
- At the time of writing, this judgment is under appeal to the High Court. The legal position regarding compensation for non-material damage in Denmark is therefore not carved in stone and can probably only be considered definitively clarified when a similar judgment is delivered by the Court of Justice of the European Union or the Supreme Court.

Transmitting sensitive information through text message

Summary

During the evening of 2nd September 2021, a young person approached Joannahuset, which is a child/youth crisis center offering shelter to young people. Joannahuset then contacted the young person's current foster home to obtain consent for the young person to spend the night at Joannahuset.

The Danish DPA was informed that Joannahuset had previously been in dialogue with the young person and had given him or her shelter. According to Joannahuset, the dialogue with the young person's municipality of origin had previously been difficult.

On this basis, the staff at Joannahuset assessed that in the specific situation, there was a particular need to ensure that the identity of the young person and the identity of the person who gave consent from the municipality were clearly established and could be documented. Joannahuset, therefore, requested the municipality of origin to transfer the young person's social security number via transmitting sensitive information through text message. The normal procedure for securely obtaining social security numbers thus deviated from fulfilling the young person's urgent request for shelter.

The Danish Data Protection Agency's decision

The Danish DPA **did not** overturn Joannahuset's assessment in this specific situation, considering the young person's best interests, arising in an acute situation and with limited possible solutions. This outweighed the consideration of the protection of personal data since the young person could have suffered a greater loss of rights if the transmitting sensitive information through text message in question had not been sent.

Our remarks

- The Danish DPA is generally of the opinion that the transmission of sensitive data via transmitting sensitive information through text message involves a significant risk to the rights and freedoms of data subjects. As with transmission by e-mail, the risk of transmitting sensitive information through text message via the Internet is at the "high end of the scale". The Danish DPA states that these risks can only to a very limited extent be mitigated by measures taken by the data controller itself.
- In the specific case, the Danish DPA assessed that data protection requirements in special cases must give way to other weightier considerations, including, for example, the urgent need to safeguard life and health in relation to particularly vulnerable groups of people. According to the Danish DPA, such relaxation of data protection must be based on a specific assessment, and the considerations must be documented.

Published: 27-04-2022 **Journal number:** 2021-431-0151 **Tags:** 05 Data security

Serious criticism for insufficient testing of a software update

Summary

In 2021, the University of Southern Denmark experienced a data breach after an update of an HR system, whereby the settings for rights management were changed. Employees were assigned different roles in the system which, depending on the employee's work-related needs, would give them access to view content, including job applications, containing personal data.

Due to an error with the update, the existing management of rights was canceled, after which all employees at the University of Southern Denmark, i.e., 7011 employees, were given potential access to applications from a total of 417 applicants. Of these, approximately 400 employees had an access-related need to access the applications.

The University of Southern Denmark had not tested the update on the test system before it came into force. The university had a practice of 14 days of testing updates that lead to changes in roles and their associated functions, but this was not carried out in this specific case. This was due to the University's lack of knowledge that the update would lead to changes of the nature in question.

The Danish Data Protection Agency's decision

The Danish DPA **seriously criticized** the University of Southern Denmark for not processing personal data in accordance with the rules in GDPR Article 32(1) *(security of processing).*

Our remarks

- A controller's responsibility to test updates that, for example, reset or change previously selected settings does not cease, even if the controller is unaware of these features of the update. This applies regardless of whether the lack of knowledge is because the software vendor has not adequately communicated this.
- Controllers should therefore seek knowledge about the consequences of updates themselves, even if the software supplier may have provided adequate information.

Published: 12-05-2022 **Journal number:** 2021-442-13989 **Tags:** 05 Data security

Sub-processor refused to provide data to the controller

Summary

A company, as a data controller, had engaged another company as a data processor. The data processor (A) later entered into a data processing agreement with its IT supplier (Data processor (B)), which then became a sub-processor for the original data controller.

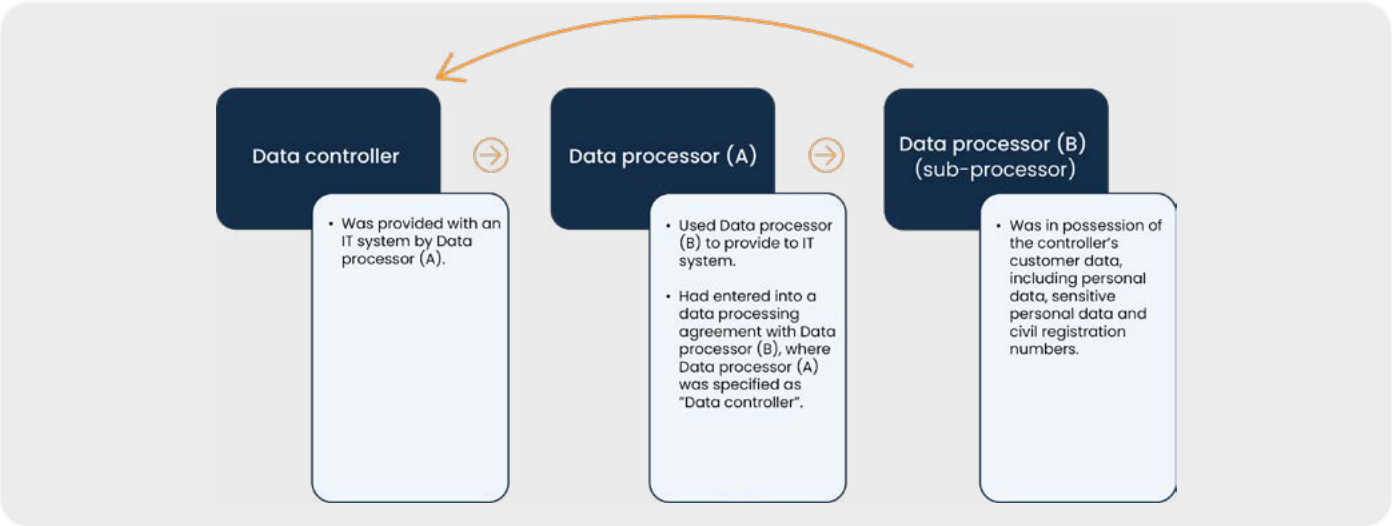
The sub-processor had refused to meet the data controller's demand for the return of customer data with reference to the agreement in question, including by challenging the data controller's power of instruction.

This picture explains the relationship between the parties:

The Danish Data Protection Agency's decision

The Danish DPA **seriously criticized** the sub-processor's processing of personal data, which had not been carried out in accordance with the rules in GDPR, Articles 6 *(lawful processing)* and 9 *(processing of special categories of personal data)* and Section 11 of the Danish Data Protection Act, cf. GDPR, Article 28 *(requirements for data processors)*.

The Danish DPA issued an order to the data processor to disclose the data controller's customer data. In addition, the data processor was prohibited from processing the data controller's customer data after disclosure, unless this was done on the instructions of the data controller.



Our remarks

- A controller's responsibility to test updates that, for example, reset or change previously selected settings does not cease, even if the controller is unaware of these features of the update. This applies regardless of whether the lack of knowledge is because the software vendor has not adequately communicated this.
- Controllers should therefore seek knowledge about the consequences of updates themselves, even if the software supplier may have provided adequate information.

Published: 07-02-2022 **Journal number:** 2022-431-0167 **Tags:** 04 Data processing agreements and supervision of data processors and sub-processors

Criticism of failure to fulfill information obligations

Summary

The case began when the Danish DPA became aware of the Conservative political party's processing of personal data in relation to sending letters to selected households about the European Parliament elections and general election in 2019 following several specific inquiries in 2019.

The Conservative Party collected the names and addresses of selected recipients to send them letters about the party's key issues. When asked to provide information to the data subjects (recipients of the letters), the party stated that they were exempted from this obligation as the collection of names and addresses for the purpose of sending a letter is an explicitly established right under Danish case law and does not override the interests of the data subject.

The Conservative party cited GDPR, Article 6(1)(f) *(legitimate interest)* as the basis for processing.

The Danish Data Protection Agency's decision

The DPA **concluded** that the Conservative Party's processing of personal data was conducted within the framework of GDPR, Article 6(1) *(legal basis for the processing of general personal data)*.

The Danish DPA **criticized** that the party's processing of personal data had not been carried out in accordance with the rules in GDPR, Article 14 *(obligation to provide information when the data has not been collected from the data subject)*.

Our remarks

- Sharing information about a party's key issues to potential voters may constitute a legitimate interest that can serve as a legal basis for processing personal data in the form of names and addresses.
- The exception to the obligation to provide information in Article 14(5)(c), which allows for exemption when personal data is an explicitly established right according to Danish practice, should be interpreted narrowly. For the exemption to apply, legislation must explicitly state that the obligation to provide information is exempted from the processing activity in question.
- In the context of sending letters, publishing information on the controller's website does not fulfill the information obligation, as the controller is not actively providing the information to the data subject.

Authorization for municipalities to use the AI profiling

Summary

The Danish Data Protection Authority (DPA) was asked by the Danish Agency for Labor Market and Recruitment (STAR) to evaluate the legal basis for municipalities, including job centers, to use an AI profiling tool called Asta.

Asta used statistical methods and machine learning analysis to determine the risk that a recently unemployed citizen's contact with the job center would be prolonged. Based on anonymized historical data on the most recent years' unemployment benefits cases to construct personal characteristics and show the correlation between approximately 50 variable characteristics and the duration of contact with the job center.
The characteristics included information from the citizen's CV, such as language skills and job history, as well as details such as gender, age, interpreter need and previous contact processes.

The Danish DPA examined whether citizens' consent under GDPR, Article 6(1)(a) could constitute a lawful basis for processing when using the tool but determined that this was not the case. Instead, the DPA concluded that GDPR, Article 6(1)(e) which addressed the use of public authority could constitute the lawful basis for processing. However, this legal basis is subject to several requirements, including that the processing must be foreseen in EU law or national law. The stricter requirements for a national legal basis apply to more intrusive the processing activities.

The Danish Data Protection Agency's decision

The Danish DPA **assessed** that in connection with the use of the Asta tool, the municipalities' legal basis for processing personal data would be GDPR, Article 6(1)(e), which requires implementation in national legislation, and Article 9(2)(g) if special categories of personal data are also processed, such as health data about the citizens in question.

Our remarks

- Valid consent requires that it is given voluntarily. In a situation where a municipality (job center) is the data controller and an unemployed citizen is the data subject, the power imbalance between the parties is considered too great for consent to be given voluntarily.
- The lawful use of a profiling tool such as Asta requires the existence of a legal basis under national or EU law that foresees the processing of data subjects' data. The requirements for clarity of this legal basis depend on the intrusiveness of the tool. In addition, it is still possible that processing based on such a legal basis would require the individual data subject's consent for the tool to be used in his or her case.

Published: 18-05-2022 **Journal number:** 2022-212-3676 **Tags:** 01 Legal basis for processing and principles for processing

The Chromebook Case 1

Summary

Helsingør Municipality provided Google Chromebooks to its school pupils giving them access to the G-suite software package, which required the creation of a school account with Google. To create these accounts the pupils' full names, schools, and grade levels were transferred to Google, which also made the full names of pupils with name and address protection available to Google products such as YouTube, of which the municipality was unaware.

A control panel was used to manage which programs pupils could access and how their information was shared with Google.

The Chromebooks with G-Suite were distributed based on the Public Schools Act so that the municipality did not consider it necessary to obtain consent from the pupils' parents.

The case was initiated following two complaints to the Danish DPA that Helsingør Municipality had created Google accounts for pupils without parental consent. In addition, the complainants pointed out that the pupils' login details were pasted on the laptops, leaving them vulnerable to unauthorized access.

The Danish Data Protection Agency's decision

- The Danish DPA **seriously criticized** that the processing of personal data by the Helsingør Municipality was not in accordance with the General Data Protection Regulation.
- The Danish DPA **issued a warning** to Helsingør municipality stating that using G-Suite's add-on programs without carrying out a data protection impact assessment would be a clear violation of the GDPR.
- If the risk assessments showed a high risk to the rights and freedoms of data subjects, and the risks had not been reduced to a level below high, the DPA would notify the municipality of a **temporary restriction on processing operations**.

Our remarks

- If you process personal data about children, you must be extra careful to ensure that your legal basis for processing is in order, as children have special protection under the General Data Protection Regulation. In this case, the Danish DPA concluded that the legal basis for processing of personal data under The Public Schools Act was not sufficient. Therefore, Helsingør Municipality should have either obtained consent from the pupils or their parents or ensured that no unnecessary personal data was shared with G-Suite.

- It is not GDPR-compliant to label login credentials on computers, as the controller does not ensure an adequate level of security by doing so.

- If different functionalities of a program package involve different processing activities and personal data flows, these functionalities must be risk assessed separately. As a rule, in situations where the personal data of children are processed in complex technology, this will pose a high risk to the data subject. When sharing personal data with Google features, the risk assessment should consider that Google's business model includes collecting personal data and using it for marketing purposes.

- At the same time, attention must be paid to a possible transfer to a third country when using Google applications. Specifically, the Helsingør municipality had entered into a data processing agreement that ensured that data did not leave the EU/EEA. Therefore, the Danish DPA did not address the issue of third-country transfers.

Published: 10-09-2021, **Journal number:** 2020-431-0061 **Tags:** 01 Legal basis for processing and principles for processing

The Chromebook Case 2

Summary

In September 2021, the Danish DPA issued a decision in which Helsingør Municipality was instructed to conduct a new risk assessment of the processing of personal data in primary and lower secondary schools when using Chromebooks and Workspace Education (formerly G Suite). The Danish DPA subsequently assessed the content of Helsingør's Municipality's new risk assessment and whether the conditions for third-country transfers were met.

Helsingør Municipality had prepared a TIA, adopted the EU Commission's standard contractual clauses, and conducted a risk assessment regarding the use of Chromebooks and Workspace Education. However, the risk assessment was concluded to be incomplete as it did not address all potential risks, such as the risk of unauthorized access to personal data stored in Chromebooks.

In its risk assessment, Helsingør Municipality acknowledged that Google may breach its contractual obligations not to use the personal data for marketing purposes but assessed that the likelihood of that happening was low.

The Municipality also ensured that personal data were only stored in data centers in the EU/EEA but acknowledged that personal data could be transferred to third countries in support situations where Google's US department would have access to the personal data in question.

Helsingør Municipality argued that Google could not be subject to surveillance via FISA 702, as the personal data was not transferred by Google LCC, but to Google LCC for use in support services. However, the Danish DPA concluded this argument to be insufficient, as FISA 702 prohibits surveillance of US persons, but not surveillance of foreign individuals.

This case relates to: Chromebook Case 1: Serious Criticism of Helsingør Municipality for incomplete risk assessment.

decision

- The Danish DPA issued a **prohibition** against the Municipality of Helsingør from processing personal data using Google Chromebooks and Workspace for Education. The prohibition applied until the municipality brought the processing activity into compliance with data protection legislation and prepared adequate documentation for this.
- Any transfer of personal data to the United States was **suspended** until Helsingør Municipality could demonstrate that the rules in Chapter V of the General Data Protection Regulation on transfers to third countries had been complied with.
- The Danish DPA **severely criticized** the fact that the municipality's processing of personal data had not been carried out in accordance with GDPR, Article 5(2) *(accountability)*, cf. Article 5(1)(a) *(lawfulness, fairness, and transparency)*, Article 24 *(responsibility of the controller)*, cf. Article 28(1) *(requirements for data processors)*, Article 35(1) *(impact assessment)*, and Article 44 *(general principle for transfers)*, cf. Article 46(1) *(transfers subject to appropriate safeguards)*.

Our remarks

Risk assessment

- In a risk assessment, it is important to document all the risk scenarios that may arise when using a given service (e.g., Google Workspace). In this case, Helsingør Municipality had not sufficiently addressed how Google collected information about users and used it in other situations, such as marketing and further distribution of this information.
- When conducting a risk assessment, data controllers must evaluate the use of data processors and ensure that they fulfill their obligations under the data processing agreement. To verify this, the data controller may need to test the online environments to ensure that personal data is not being mishandled or misused.
- If there is a risk that the processor may engage in unlawful activities, the controller must take concrete technical or organizational measures to mitigate the risk - even if the likelihood of it happening is low.

Third country transfer

- The Danish DPA has clarified that even if personal data is transferred to a US company through Workspace, it could still be subject to monitoring under FISA 702, given the data pertains to Danish citizens. Google LCC must therefore be considered an "electronic communications service provider". As a result, a data controller using Workspace would need to implement supplementary measures to comply with data protection regulations.
- These measures must generally be technical measures, as organizational and contractual measures will not prevent US authorities from accessing personal data.
- Although encryption is a useful technological measure for protecting personal data, it may not be effective in the context of FISA 702. If the recipient of the data itself has access to the encryption key this will not enhance the protection of personal data since FISA 702 may still require access to personal data held by a US data processor. In such cases, the processor would be obliged to assist the authority in providing access to the personal data, rendering the encryption ineffective in preventing access to the data.

Please note that this decision was made prior to the EU Commission's adoption of the EU-U.S. Data Privacy Framework. The framework solves the challenges of the SCHREMS II case and thereby ensures that entities in the EU can transfer personal data to entities in the US that comply with the framework without conducting a TIA. However, general considerations concerning the transfer of personal data to other unsafe third countries still apply.

The Chromebook Case 3

Summary

The Danish DPA reviewed new documentation submitted by Helsingør Municipality following its decision on July 14, 2022, to prohibit Helsingør Municipality from using Google Chromebooks for primary school education.

A central issue in the case was that the Danish DPA believed that the use of Chromebooks and Workspace generated personal data that Google used for purposes such as marketing and f application improvement, which went beyond the purposes that Helsingør Municipality had assumed in their risk assessment, impact assessment, and data processing agreement with Google.

For more information, see the two previous decisions, "Chromebook Case 1: Serious criticism of Helsingør Municipality for incomplete risk assessment" and "Chromebook Case 2: The Danish Data Protection Agency imposes processing ban on Helsingør Municipality".

The Danish Data Protection Agency's decision

- The Danish DPA concluded that Helsingør Municipality's use of Google Chromebooks and Workspace for Education to process personal data **was still not in compliance** with GDPR. The DPA also concluded that the documentation prepared by the municipality on 1 August 2022, did not conform with Article 35(1) *(impact assessment when using new technologies)* and (7) *(minimum requirements for impact assessment)*, as well as Article 36(1) *(prior hearing with the Danish Data Protection Agency)*.
- The Danish DPA's **prohibition** of 14 July 2020 was **upheld**.

Our remarks

- When conducting a risk assessment or an impact assessment of a particular service, it is essential for the data controller to evaluate the entire environment in which the service is provided. In the case of Helsingør Municipality, it had only assessed how personal data was processed in Workspace and had not considered how personal data was processed in the Google Chrome browser or Google OS (the operating system for Chromebooks).
- When a data processor uses personal data to improve its own applications, it becomes an independent data controller for this processing. If this is done for a public authority, a separate legal basis is required for the transfer of the personal data, since the personal data is then carried out for a purpose that goes beyond the legal basis for processing to fulfill public authority tasks.
- When using contractual measures to mitigate risk with a specific data processor, it is important that the data controller is aware of the types of personal data that are being processed and when. In the data processing agreement with Google, Helsingør Municipality had not contractually protected the data that could be derived from the use of Chromebooks and Workspace. As a result, Helsingør Municipality had not minimized the risk of this processing.

Please note that this decision was made prior to the EU Commission's adoption of the EU-U.S. Data Privacy Framework. The framework solves the challenges of the SCHREMS II case and thereby ensures that entities in the EU can transfer personal data to entities in the US that comply with the framework without conducting a TIA. However, general considerations concerning the transfer of personal data to other unsafe third countries still apply.

Published: 18-08-2022 **Journal number:** 2020-431-0061 **Tags:** 06 Transfers to third countries

The Chromebook Case 4

Summary

In July 2022, the Danish DPA imposed a ban on the use of Google Workspace in Helsingør Municipality, and in August 2022, the DPA upheld the ban.

Subsequently, the Helsingør Municipality had, in dialog with the Danish DPA, identified several circumstances where the use of Google Workspace, etc. was either not legal or where the risk to school pupils had not been sufficiently identified and reduced. In light of this finding, the Danish DPA temporarily lifted the ban and issued several orders to the municipality to ensure that the use of Google Chromebooks and Workspace for Education was in compliance with GDPR.

For more information, see the two previous decisions, "Chromebook Case 1: Serious criticism of Helsingør Municipality for incomplete risk assessment", "Chromebook Case 2: The Danish Data Protection Agency imposes processing ban on Helsingør Municipality" and "Chromebook Case 3: Danish Data Protection Agency upholds ban".

The Danish Data Protection Agency's decision

- The Danish DPA's **prohibition** to Helsingør Municipality on August 18, 2022, **was suspended** until November 5, 2022.
- The Danish DPA **issued** an **order** to Helsingør Municipality to amend the in-depth agreement with the data processor in such a way that the matters mentioned in the Agency's decisions of July 14 and August 18, 2022, as well as the material submitted by the municipality on September 1, 2022, which originated from the overall contractual basis with the supplier, were brought into compliance with the GDPR.
- The Danish DPA further **ordered** Helsingør Municipality to provide a detailed description of the data flows that took place and to identify the personal data that was transferred to the provider. The municipality must also clarify whether it acted as an independent or shared data controller in each instance. Additionally, the documentation had to cover the entire technology stack used by Helsingør Municipality for processing the data.
- The Danish DPA further **ordered** Helsingør Municipality to prepare an updated data impact assessment based on all the risks identified by the municipality during the documentation process, in the eventuality that there were additional high, non-mitigable risks. The order also included consultation with the Danish DPA under GDPR, Article 36.
- Finally, the Danish DPA **ordered** Helsingør Municipality to submit a final, time-bound plan for legalizing any processing operations that were not able to be legalized before the deadline for the orders, which was set on 3 November 2022.

Our remarks

- If a data impact assessment reveals that a specific residual risk to the rights of the data subjects cannot be reduced from a high to a low level, the controller has the possibility to consult the Data Protection Authority. The DPA can then advise the controller on how to reduce the risk.
- If the use of a data processor is unlawful, it may be necessary to amend the data processing agreement.

Please note that this decision was made prior to the EU Commission's adoption of the EU-U.S. Data Privacy Framework. The framework solves the challenges of the SCHREMS II case and thereby ensures that entities in the EU can transfer personal data to entities in the US that comply with the framework without conducting a TIA. However, general considerations concerning the transfer of personal data to other unsafe third countries still apply.

Serious criticism for unintended changes to shared medical record

Summary

On 13 August 2021, the Danish Health Data Authority reported a personal data breach to the Danish DPA. This breach followed two other similar breaches reported in August 2020 and July 2021, respectively, which resulted in the Danish DPA criticizing "Region Hovedstaden" (the capital region), as it was responsible for the Health Platform.

The security breach occurred when a code change in the platform unintentionally altered the Shared Medicine Record, causing the end date of dosing for 267 individuals on the Shared Medicine Record to not appear in the platform. The Capital Region of Denmark is the data controller for the Health Platform, while the Danish Health Data Authority is the data controller for the Shared Medicine Record.

The Danish Data Protection Agency's decision

The Danish DPA **seriously criticized** the Danish Health Data Authority for not processing personal data in accordance with the rules in GDPR, Article 32(1) *(security of processing)*, and Article 33(1) *(late notification of personal data breaches)*.

Our remarks

- The case concerns a situation where several actors exchange data in a service-based architecture. The case specifically shows how a third party's changes to a system can lead to unintended changes in a system that was not the intended target of the change.
- The Danish DPA emphasizes that the data controller is responsible for testing all likely error scenarios when developing or modifying software that processes personal data, including when changes are implemented by third parties. In these situations, clear agreements should be made between all actors in the architecture of the system so that the controller can maintain control and integrity of the system. This follows the requirement for appropriate organizational measures in GDPR, Article 32(1).
- Personal data breaches must be notified to the DPA without undue delay and, if possible, within 72 hours, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. In this case, the Danish Health Data Authority became aware of the breach on 9 August 2021 but did not report the breach until 13 August 2021, which the Danish DPA deemed too late.

Published: 22-06-2022, **Journal number:** 2021-442-14071 **Tags:** 05 Data security

University's use of a monitoring program for online exams

Summary

On 30 April 2020, the Danish DPA received a telephone inquiry regarding the IT University's (hereinafter "ITU") intention to monitor students' computers during a home exam using a monitoring program called ProctorExam. The program would record video, audio, and screen activity, as well as browser search history on students' computers during the three-hour exam.

To monitor compliance with the applicable rules, the recordings would be conducted through a Google Chrome web browser extension.

The Danish Data Protection Agency's decision

The Danish DPA **did not criticize** ITU's processing of personal data and concluded that the processing was in compliance with GDPR, Article 5 of *(principles for processing of personal data)*, Article 6(1) *(lawful processing)*, and Section 11(1) of the Danish Data Protection Act *(processing of personal identity numbers by public authorities for identification purposes)*.

The DPA further concluded that the ITU's processing for the use of ProctorExam **complied** with GDPR, Article 5(1)(f) *(principle of integrity and confidentiality)*, Article 32 *(security of processing)*, and Article 35 *(data protection impact assessment)*.

Our remarks

- This decision thus serves as an example of the great importance of carrying out a concrete assessment of the risk for the data subjects in connection with certain processing operations, and that it can be demonstrated that the processing fulfills the principles of Article 5 of the GDPR.
- Information on the processing of personal data must be clear, accessible, and transparent, with a method of delivery tailored to the specific group of data subjects.
- For processing operations that are likely to result in a high risk to the individual's rights and freedoms, it is essential to assess the potential risks before undertaking any processing activities.

Published: 26-01-2021, **Journal number:** 2020-432-0034 **Tags:** 01 Legal basis for processing and principles for processing

FysioDanmark: Use of facial recognition system

Summary

The Danish DPA initiated an investigation into FysioDanmark Hillerød ApS's ("FysioDanmark") concerning their proposed implementation of a biometric identification system. This system, which utilized facial recognition technology, was intended to regulate access to the company's fitness center by both customers and employees. The system would collect direct and derived data for the purpose of optimizing business operations.

According to FysioDanmark, the system would only be used with the prior consent of customers and employees. To regulate access, users' photos would be uploaded to an underlying database, and a camera at the entrance would scan faces to determine whether they matched any of the photos uploaded in the database. However, the system would scan a person's face, regardless of whether they had given consent and was registered in the user database.

Through the intended use of the system, FysioDanmark would process the biometric data for the purpose of uniquely identifying individuals, which in general is prohibited to process, cf. GDPR, Article 9(1), unless an exception to this prohibition can be identified in paragraph 2 of the article. The Danish DPA stated that the only possible legal basis for the intended processing would be consent, GDPR cf. Article 9(2)(a).

It should be noted that in the decision, the Danish DPA only considered whether GDPR, Article 6 or 9 could form the basis for the proposed processing, and not any other data protection law issues.

The Danish Data Protection Agency's decision

The Danish DPA **issued a warning** to FysioDanmark that it would probably violate the GDPR if FysioDanmark:

- for statistical and business optimization purposes, processes biometric data for the purpose of uniquely identifying a data subject without obtaining consent from the data subject in accordance with GDPR, Article 9(2)(a) and
- use the facial recognition system in the manner envisaged, as this would involve the processing of biometric data for the purpose of uniquely identifying a natural person on those individuals who have not consented to the processing, which is prohibited, as no exception can be identified in GDPR, Article 9(2).

Published: 17-03-2022 **Journal number:** 2021-431-0145 **Tags:** 01 Legal basis for processing and principles of processing

Our remarks

- The decision emphasizes that biometric data within the meaning of GDPR, Article 4(14) includes the processing of individuals' facial images or fingerprint data.
- The Danish DPA clarifies that the data subject's consent pursuant to GDPR, Article 9(2) is the only possible legal basis for processing biometric data of the nature in question. However, if the data are to be used for different purposes, the data subject is required to be able to give granular consent, i.e., to give separate consent for different processing purposes. This requirement can be met, for example, by allowing the data subject to specify the purposes for which he or she agrees to the processing of data in a consent form.
- Consent given by employees is not normally considered voluntary, given the unequal nature of the relationship between the employer and the employee. However, in this specific case, the employee's consent was considered voluntary for two reasons. Firstly, because employees had the option of using an access card and code instead of the facial recognition system, and secondly, because the system only registered information about the employees in connection with his or her access to the center, and not about their movements in the center in general.
- Use of the system would also require that customers and employees who did not wish to use the facial recognition system could avoid the processing in question by accessing the center. According to the Danish DPA, this can be accommodated by organizing the system in such a way that the system is only 'activated' when a customer or employee who wishes to perform a face scan activates the system - e.g., by pressing a key.

DBA: Right to refuse a request for erasure

Summary

A complainant had asked DBA (a secondhand selling website) to delete his profile and associated personal data. DBA refused the request because three independent buyers on DBA had complained about the user and that DBA needed to keep his data to block future access to the platform. DBA stated that the complainant had previously tried to circumvent the blocking by creating new profiles with different email addresses.

DBA emphasized that the storage and processing of the data were necessary to protect the vital interests of buyers, and to assist the police with any investigations in the event of identification.

The Danish Data Protection Agency's decision

The Danish DPA **concluded** that DBA **was** not under an obligation to erase the data in question pursuant to GDPR, Article 17(1) *(the right to erasure)*.

Our remarks

- The correct legal basis for processing such as that at issue in the case is GDPR, Article 6(1)(f) *(legitimate interest)*, and not Article 6(1)(d) *(vital interests)*, which DBA would otherwise have applied.
- DBA's legitimate interest in storing data relating to the data subject meant that neither the conditions of GDPR regarding the right to erasure were met.
- This case is an example of when other interests overrule the data subject's right to erasure.

Published: 31-01-2022, **Journal number:** 2021-31-5439 **Tags:** Erasure and rectification

Selected interesting cases – from other EU member states

08

Consent-pay solution

Summary

An Austrian newspaper had structured its online presence as follows: Users had to agree to so-called "marketing cookies" to access all articles available online. Those who did not wish to consent to such cookies were unable to fully access all the newspaper's articles. Alternatively, users could opt for full access via an online subscription that cost EUR 6 per month.

It was contested whether this constituted freely given consent, as the complainant argued that consent to cookies and different marketing activities could not be deemed freely given if it is given to avoid a payment obligation.

The decision of the Austrian DPA

The Austrian DPA **rejected** the complaint and found that the "consent or pay" solution was in accordance with the GDPR.

Our remarks

- A "consent or pay" solution can be legally viable if the following requirements are followed:
  - The user is provided with clear information on how the solution works.
  - Cookies are only placed after the user has made their choice.
  - The content provided to the user should be comparable regardless of their choice.
  - The pricing should be proportionate in light of the service. In this case, 6 EUR per month for a news website was deemed reasonable.
- Cookie walls have previously been the subject of debate due to doubts about whether it is possible to do it in a way where consent is given voluntarily by the data subject. This decision confirms that cookie walls can be considered lawful if the user has an alternative to consent to cookies through paid access.
- The decision is supported by two recent cases from the Danish DPA. In one of the cases, 4 EUR a month for access to the Danish equivalent to Craigslist was accepted. In the other case, a news media was criticized as it did not provide the same access to people that consented to cookies as to those who had a paid subscription.

Lack of evidence of fraudulent use does not affect the classification of a breach

Summary

In 2015, a payment service provider called SLIMPAY reused personal data from its databases for testing purposes as part of a research project on an anti-fraud mechanism, and the data was left stored on a server without proper security measures. This led to personal data being freely accessible by anyone from the internet.

The database contained information such as civil status and bank information (e.g., IBAN) related to around 12 million persons. In 2020, a SLIMPAY client reported the data breach, and SLIMPAY took measures to stop it and notified the French Data Protection Authority (DPA). However, SLIMPAY did not notify the data subjects affected, even though they were in possession of the contact information for about 6 million of the affected data subjects.

In this case, no data subjects suffered any harm, which SLIMPAY argued should indicate that no fine should be imposed on them.

The decision of the French DPA

The French DPA **imposed** a fine of **180,000 EUR** on SLIMPAY for not ensuring an adequate level of security *(GDPR, Article 32)*, and for failing to inform the affected data subjects of a data security breach *(GDPR, Article 34)*.

Our remarks

- One important technical measure that can help ensure compliance with Article 32 is logging server activity. Server logs are records of all activity that occurs on a server, such as who accessed the server, what data was accessed, and when the access occurred. By logging server activity, data controllers and processors can monitor and track potential security breaches, unauthorized access attempts, and other suspicious activity. The data controller will also be able to monitor which data potential intruders had access to during a personal data breach.
- It is not a mitigating factor that a breach occurs due to human errors. On the contrary, organizational and technical measures should try to compensate for human shortcomings.
- The lack of evidence of fraudulent use of data does not affect the classification of the security breach. This is because the risk of fraudulent use of personal data was real, regardless of whether any cases of fraud occurred. The fact that many people's data was made accessible to unauthorized third parties was enough to create a risk.
- The data controller is only obliged to inform the data subjects if the personal data breach is "likely to result in a high risk to the rights and freedoms of natural persons". A personal data breach concerning financial information like IBAN constitutes a high risk for the data subjects, and therefore they should have been notified about the breach in this case. This notification should be sent directly to the data subject or can in some situations be done via public communication. The DPA notes in the case that, even though public communication would probably not be sufficient in this case, it would have been better than not doing anything at all.

Published: 28-12-2021, **Journal number:** N/A **Tags:** 05 Data security

Is information about private relations sensitive personal data?

Summary

Under the Lithuanian anti-fraud law, officials were required to provide information about their spouse, cohabitant, or partner. such as full name, social security number, place of employment, etc. An official contested this requirement, arguing that the information he was required to give revealed sensitive personal details, as the sexuality of the official could be deduced from this information.

The preliminary questions that were brought before The Court of Justice of the European Union (CJEU) were the following:

1. Is national legislation that requires online publication of name-specific data relating to an official's family members precluded by GDPR, Article 6(1) and (3)?
2. Is personal data that can indirectly reveal the special categories of a natural person considered special category data under the GDPR?

The decision of the European Court of Justice

The CJEU **found** that national legislation that requires online publication of name-specific data relating to an official's family members or other close individuals is precluded by GDPR, Article 6(1)(c) and (e) and Article 6(3).

The CJEU also **ruled** that the publication of personal data which indirectly discloses someone's sexual orientation constitutes the processing of special categories of personal data under GDPR, Article 9(1).

Our remarks

- There is generally a prohibition against processing special categories of personal data. Prior to processing sensitive personal data, it is imperative to have a lawful basis in GDPR, Article 6(1), and to meet one of the exemptions in GDPR, Article 9(2).
- Personal data that is not sensitive in itself but can indirectly reveal information about sexual orientation is considered sensitive data. This can be data like:
    - The full name of a partner that can reveal sexual orientation.
- It is a bit uncertain how this judgment should be applied in practice, but overall, it is advisable to initially to assess whether personal data being processed includes any information that reveals sensitive personal data. The data controller needs to evaluate if they process any regular types of data that can reveal special types of information.
- The judgment could also be a prompt to rethink your erasure policy, as potentially more personal data can be considered to be sensitive personal data.

Grindr preliminarily fined for 100 million NOK for consent solution

Summary

The Norwegian Consumer Ombudsman complained to the Norwegian Data Protection Authority (DPA) about Grindr LLC's ('Grindr') processing of users' personal data, including, for example, information on users' sexuality and location. The Ombudsman's complaint centered on Grindr's consent solution and the fact that the user's personal data was shared with a large number of third-party advertisers, which was not clear to the user.

Grindr is the world's largest social media platform for people in the LGTBQ+ community, with 13.7 million users worldwide and approximately 17 thousand users in Norway.

Grindr's consent solution worked in such a way that the user was first presented with Grindr's entire privacy policy, after which the user could choose whether to continue. Next, the user was asked if he or she wanted to accept the data processing by clicking "accept". Users could avoid having their personal data shared with third-party advertisers if they upgraded their accounts and paid a monthly fee.

Grindr's defense in the case was that the company could not be held responsible for the consent standards that had just been published by the European Data Protection Board. In response, the Norwegian DPA stated that Grindr's consent solution had been illegal since the implementation of the GDPR in 2018 and that the rules on consent as a basis for processing ordinary personal data had not been substantially changed since the 1995 Data Protection Directive.

The above resulted in a preliminary decision, to which Grindr could make their final submissions before the Norwegian DPA issued a final decision.

The decision of the Norwegian Data Protection Authority

In the preliminary decision, the Norwegian DPA **fined Grindr 100 million NOK** for having:

- Shared personal data with third-party advertisers without a legal basis for the processing *(GDPR, Article 6(1))*.
- Shared personal data with third-party advertisers without a valid exception *(GDPR, Article 9(1))*.

Our remarks

The consent solution

- If consent is to be used as a basis for processing, it is important to observe the requirements for valid consent, including that it constitutes a freely given, specific, informed, and unambiguous indication of the data subject's wishes. To fulfill the "informed" criterion, the data subject must be adequately informed of the processing purposes pursued and the activities carried out. This is achieved in the following ways:
  - The data subject separately gives consent for each processing purpose. In this case, the user consented to several different processing purposes with one click.
  - The information provided to the data subject is presented clearly and concisely. In this case, the user was presented with the entire privacy policy at once, where Grindr should have highlighted essential information such as whom the personal data was shared with.
  - The data subject must not be harmed by not giving consent or by withdrawing consent. In this case, the user could pay NOK 3,240 per year to use the app without the personal data being shared with third parties. According to the Norwegian DPA, this was enough for the data subject to suffer harm by not giving or withdrawing consent.

Published: 24-01-2021, **Journal number:** 20/02136-5 **Tags:** 01 Basis for processing and principles of processing

- For more information on the requirements for valid consent, you may wish to read the EDPB's guidelines on consent.

- It is also relevant to consider the types of personal data being processed. Even if one does not directly process information about the sexuality of the data subject, the processing could probably still fall under Article 9 of the GDPR if, in cases such as the one in question, sensitive personal data could be inferred from knowing which community the data subject belongs.

- The fact that a person creates an online (dating) profile with millions of users does not automatically mean that sensitive personal data from that profile can be processed under the exemption in Article 9(2)(e), even though it says that sensitive personal data made public by the data subject himself can be processed.

The imposition of a fine

- When calculating the fine, the nature of the offense may be considered. A larger fine is likely to be imposed if many people have unlawfully accessed personal data and if the unlawful processing has taken place over a long period.

- It is important to consider the types of personal data that have been processed and how they interact with each other. In this specific case, the Norwegian DPA considered it an aggravating circumstance that information about users' sexuality, together with their exact location, was shared, as this constituted a threat to the data subjects' freedoms. According to the Authority, this should be seen in the context of the fact that Grindr is considered a "safe space" for people in the LGTBQ+ community and that those in the community are particularly concerned that others do not have access to this information.

- In this context, it is interesting to consider whether these circumstances would be considered by a court to be so serious that data subjects would be able to obtain damages from Grindr, if such an action were to be brought.

- According to German and Austrian courts, harm does not have to be economic, but it must be objectively significant and involve social or personal consequences for the data subject, such as negative public exposure or humiliation.

- It is not inconceivable that this could be the case if this information came into the possession of unauthorized persons - especially considering the Norwegian DPA's premise that Grindr is considered a "safe space" for people in the LGTBQ+ community.

    - If the offense could give rise to a claim for damages, it is interesting that the case involves a large number of data subjects, each of whom could potentially claim damages. This could pose a serious financial threat to Grindr if the Norwegian DPA even ends up upholding the NOK 100 million fine.

    - It is an aggravating circumstance if the data processor has made money from unlawful processing. This takes into account what other fines have been imposed in Europe in similar cases, where, for example, Google was fined EUR 50 million in 2020. When you have monetized unlawful processing, the supervisory authority in question will probably often find that the unlawfulness is committed intentionally, which will also be an aggravating circumstance.

    - Finally, it is interesting that the Norwegian DPA recognized the COVID-19 situation as a mitigating circumstance regarding the amount of the fine.

SCHREMS II

Summary

The case was brought by Max Schrems, an Austrian privacy activist, who challenged the transfer of his personal data by Facebook Ireland to servers located in the United States. Schrems argued that U.S. laws did not provide sufficient protection for the personal data of European Union citizens, and that EU citizens had no effective legal remedies in the U.S. courts.

The case was referred to the Court of Justice of the European Union (CJEU), which examined the legality of the transfer of personal data from the EU to the United States under the EU-U.S. Privacy Shield Framework.

The decision of the European Court of Justice

In its ruling, the CJEU **invalidated** the Privacy Shield, finding that it did not provide adequate protection for the personal data of EU citizens transferred to the United States. The Court stated that U.S. laws **did not offer** EU citizens adequate protection from U.S. intelligence agencies, and that EU citizens had no effective legal remedies in the U.S. courts.

Our remarks

- Before transferring personal data to a third country like the US, one should assess the risk of the transfer and evaluate the adequacy of the protection offered by the recipient country. This is done through a Transfer Impact Assessment (TIA). We have made a roadmap for doing this, which you can read here.
- When assessing the adequacy of the level of data protection in the third country, the following needs to be assessed:
    - The adequacy of the legal framework. This can involve assessing the comprehensiveness of the legal framework, as well as the enforcement mechanisms in place to ensure compliance.
    - The practice conducted by the legal entities of the country. For example, should the possibility of government surveillance be conducted. This can involve evaluating the legal framework for surveillance, as well as any known instances of government surveillance or censorship.
- At the time of writing the agreement the transatlantic data transfer agreement, named the EU-US Data Privacy Framework (DPF), has been approved by the European Commission. This means that entities in the EU can transfer personal data to entities in the US that comply with the framework without conducting a TIA. However, general considerations concerning the transfer of personal data to other unsafe third countries still apply. You can read more about it here:safe third countries still apply. You can read more about it here.

Deliveroo fined 2.5 million EUR for not informing about automated processing

Summary

An Italian food delivery company, Deliveroo, used AI technology to manage their couriers' ability to choose shifts. Shifts between 19:00 and 21:00 on Fridays, Saturdays, and Sundays (called 'super peak' shifts) paid higher wages and were therefore more popular. The courier with the best score had priority in booking shifts. A bidder's score was based on previous participation in super peak shifts, how many times they had canceled a booked session, and how quickly they delivered orders. A bidder could see its score but could not see how it was calculated.

The decision of the Italian Data Protection Authority

The Italian Data Protection Authority **fined Deliveroo 2.5 million EUR** for failing to ensure sufficient transparency *(GDPR, Article 5(1)(a))*, and for not implementing appropriate measures to safeguard the data subject's rights in relation to profiling *(Article 22(3) of the GDPR)*.

Our remarks

- Using AI technology to score an individual based on personal data constitutes profiling. To ensure that the profiling is compliant with the GDPR, you must inform the data subject clearly and in language that is clear and easy to understand, and includes the following:
    - That the profiling is taking place.
    - What data is used for profiling.
    - How the technology behind the profiling calculates the results.
    - That the data subject is allowed to object to the outcome of the profiling.
    - That the AI technology is only fed with the data necessary to achieve the desired output.
- When performing profiling via AI technology, a data impact assessment should always be carried out beforehand, testing the technology for bias to ensure that the profiling arrives at a correct result and is not discriminatory.

Meta tracking tools found to breach EU rules on data transfers

Summary

An Austrian local news website used tracking tools made by Meta in August 2020. This included the use of cookies (for the use of "Facebook Login") and pixels (for "Facebook Pixel" for tracking purposes).

Cookies are small files stored on the users device or in their browser, whereas pixels are pictures the size of 1x1 pixels which are also stored in the user's browser and can thereby collect a various amount of data usable for marketing purposes.

In the case it was established that the news website was data controller for the processing and the data processed via the pixels and cookies were personal data. This information included IP-addresses, User agent, User ID, etc.

The personal data processed by the tools was then transferred to the USA.

The Austrian DPA incorporated Meta's transparency report in their assessment of the case. They used it among other things to show that personal data regarding Austrian citizens was subject to surveillance by American entities.

The decision of the Austrian DPA

The Austrian DPA found that the use of Facebook Tools in the specific situation was **illegal** as there was no legal basis for transferring data to the USA *(GDPR, Article 44)*.

Our remarks

- When using pixels, the collection and processing of personal data occurs. Therefore, the applicable rules regarding legal basis, erasure, transfer to third countries etc. should be considered.
- It is crucial to ensure that the marketing tools purchased comply with the rules regarding the transfer of personal data to third countries, as these services are often supplied by American vendors.
- One way to solve the issue of using services that constitutes illegal transfers to third countries is to anonymize the data before it is transferred to the third country. For instance, this is possible to do with a reverse proxy server when using Google Analytics. The French DPA has made a guide on how to set this up.
- At the time of writing, the EU and US have reached a preliminary agreement on a new transatlantic data transfer agreement named the EU-US Data Privacy Framework (DPF). However, other EU institutions need to review and examine the agreement before it can be officially adopted. Assuming the framework is approved, the USA would be considered a safe third country, eliminating the challenges described in this case.

Please note that this decision was made prior to the EU Commission's adoption of the EU-U.S. Data Privacy Framework. The framework solves the challenges of the SCHREMS II case and thereby ensures that entities in the EU can transfer personal data to entities in the US that comply with the framework without conducting a TIA. However, general considerations concerning the transfer of personal data to other unsafe third countries still apply.

Published: 16-03-2023, **Journal number:** GZ: D155.028 - 2022-0.726.643 **Tags:** 06 Transfers to third countries

Italian DPA bans Chat GPT

Summary

ChatGPT is the best known among relational Artificial Intelligence (AI) platforms that are capable of emulating elaborate human conversations. The platform is developed by OpenAI, who trained the model on a large body of text gathered from various sources. In just a few months, the platform has amassed more than 1 billion users. As the number of use-cases for platforms like ChatGPT are predicted to be almost unlimited, the regulatory response to the massive success of the platform has gathered great attention throughout the EU.

The decision of the Italian DPA

The Italian DPA **imposed an immediate temporary limitation** on the processing of Italian users' data by OpenAI for the following alleged violations:

- The service fails to provide users and data subjects with transparent information about the processing of their personal data,
- There appears to be no legal basis underpinning the massive collection and processing of personal data used in 'training' the algorithms on which the platform relies.
- The information provided to the users might be factually incorrect, possibly constituting processing of inaccurate personal data.
- The lack of a user age verification mechanism exposes children to receiving a service that is inappropriate to their age and awareness.

Additionally, the Italian DPA launched an investigation on the matter.

A few weeks later, the Italian DPA **gave OpenAI a 'to-do list'** for the DPA to lift the suspension order. OpenAI had to:

- Become transparent and publish an information notice detailing its data processing.
- Immediately adopt age gating to prevent minors from accessing the platform (and later implement more robust age verification measures)
- Clarifying the legal basis it claims for processing people's data for training its AI models.
- Provide ways for users and non-users to exercise rights over their personal data.

The ban has since been lifted, but the investigation continues.

Published: 30-03-23, **Journal number:** N/A **Tags:** Legal basis for processing and principles of processing

Our remarks

- The swift and comprehensive action from the Italian DPA shows great regulatory attention in the field of AI powered platforms such as ChatGPT.
- Besides the Italian DPA, supervisory authorities in both France, Germany, Ireland, Canada and South Korea have initiated investigations into OpenAI's practices.
- Additionally, the EDPB has launched a dedicated taskforce to "foster cooperation and to exchange information on possible enforcement actions conducted by data protection authorities".
- With the widespread commercial success of Artificial Intelligence powered platforms, and the ongoing warnings from academics and professionals, the regulatory framework of platforms such as ChatGPT are highly disputed.
- The ongoing controversy surrounding the platform also illustrates the need for a comprehensive legal framework for artificial intelligence in general. It remains to be seen if the upcoming EU AI Act will claim that role.
- On a GDPR note, one should always remember to enter into a data processing agreement and carry out a risk assessment before using services like ChatGPT, if personal data is shared with the AI.
- If a data controller processes personal data using AI, it is important to assess whether the processing falls within the scope of Article 22 of the GDPR, regarding "Automated individual decision-making, including profiling". This article provides the data subject the right not to be subject to decisions *"based solely on automated processing, including profiling, which produces legal effects".*
- Regarding the obligation to inform about processing personal data in AI, please refer to the case *"Italian Deliveroo was fined €2.5 million for not informing about the automated processing".*

Pseudomized data might not be personal data if the recipient has no means of re-identifying the data subject

Summary

As a part of a creditor hearing concerning the resolution of a bank, the public authority known as the Single Resolution Board (SRB) sought comments from individuals through an electronic form. To streamline the process, SRB outsourced a part of the work to a third-party private entity, Deloitte. Before the transfer to Deloitte, SRB ensured that Deloitte had no means of re-identifying the data subjects by dividing the workflow into different phases. In the first phase, the SRB replaced the names in the forms with a 33-digit alphanumeric code and filtered, categorized, and aggregated all comments so that commenters could not be distinguished. SRB then entered the second phase, which involved a transfer to Deloitte. The data was placed on a virtual server separated from the data gathered in the registration phase, to which only directly involved Deloitte employees were granted access.

The alphanumeric code was developed for audit purposes to verify and if necessary, to demonstrate that each comment had been handled and duly considered in the hearing process.

Five complaints were issued to the European Data Protection Supervisor (EDPS), arguing that SRB did not fulfill its obligations to inform the data subjects on the transfer, as the SRB privacy policy did not mention any such transfer.

The EDPS decided that SRB did not fulfill its obligations regarding the transfer of personal data to the data subjects, as the data in question was pseudonymized personal data, and SRB retained the necessary information to decode the data. On the other hand, SRB claimed that the assessment of whether the data transmitted to Deloitte constituted personal data, relied on a 'risk of re-identification'. In this regard, SRB argued that Deloitte did not have any lawful means of accessing the information required for re-identification, making the risk of re-identification reasonably unlikely.

The decision of the Court of Justice of the European Union (CJEU)

The Court decision did not examine whether the answers to the questions themselves could be considered as personal data. The Court emphasized that the classification of personal opinions as personal data should not be automatic and must be contingent upon specific circumstances. These include evaluating the content, purpose, and effect of the opinion to determine whether it can be attributed to an identifiable individual. The Court limited its examination to whether the information transmitted to Deloitte was personal data.

The Court annulled the EDPS' decision based on the following arguments:

- The EDPS should have assessed whether the comments constituted personal data from Deloitte's perspective, stating that merely examining whether it was possible to re-identify the authors of the comments from the SRB's perspective, was insufficient.
- The CJEU stated that the EDPS should instead have determined whether the possibility of combining the information that had been transmitted to the third party, with the additional information held by the SRB, constituted a means likely to be used by the third party to identify the authors of the comments.

Our remarks

- When determining whether data qualifies as personal data, it is essential to consider the perspective of the data recipient.
- The ability of the data transmitter to re-identify the data subjects does not affect the recipient's classification of the transmitted data as personal data and does not automatically render the data personal for the recipient.
- If pseudonymized personal data is shared with a recipient who is effectively incapable of re-identifying the individuals, the data might be considered anonymous, thereby no longer considered personal data.
    - Consider what steps to take to ensure that the receiving party has no legal means to re-identify the data subject. In this regard, both organizational and technical measures should be considered. The less likely the receiving party is to be able to re-identify the data subjects, the more likely the data is to be considered non-personal.

Meta fined 405 million EUR for not handling teenagers' data appropriately

Summary

Instagram allowed teenagers aged between 13-17 to create business accounts whereby the children's contact information was publicly available by default.

The case was brought before the European Data Protection Board as the Irish DPA, as lead supervisory authority, triggered the dispute resolution procedure concerning the objections raised by several concerned supervisory authorities. The final decision was adopted by the Irish DPA.

The question in the case was whether Meta had a legitimate interest in disclosing the personal data of the children, as they used this as the legal basis for processing the personal data.

Binding decision from Irish DPA

The Irish DPA found that Meta did not have any valid basis for making their personal data publicly available. Therefore, Meta was **fined 405 million EUR.**

Meta was also **ordered** to change the setup of business accounts for children, so that children's data was not made public by default.

Our remarks

- Meta's financial gain from the infringement was decisive for the outcome of the case and the size of the fine.
- The case is a reflection of Better Internet for Kids strategy (BIK+). The European Better Internet for Kids strategy (BIK+) is an initiative focused on creating a safer and more positive online experience for children and young people. It aims to raise awareness about online risks, provide tools for protection, foster resilience in dealing with negative experiences, and advocate for effective policies to ensure child safety online. The initiative has been adopted by several countries and international organizations such as UNICEF.
- A data controller should be aware of how information about the data subject is provided, when they know they have young users. A good tip here is to use age filters. Another way to encounter the challenges, for example, is that TikTok has made a privacy policy for American children, that is written in a simpler language. Initiatives like this are a good step towards complying with the obligation to inform when it comes to children.
- The case reminds us that users may use services in unintended ways. Therefore, controllers should be aware of unexpected usage patterns and should test for them, before releasing new features in a system.
- The case is at the time of writing under appeal.

Methods and Scope

09

Methods and Scope

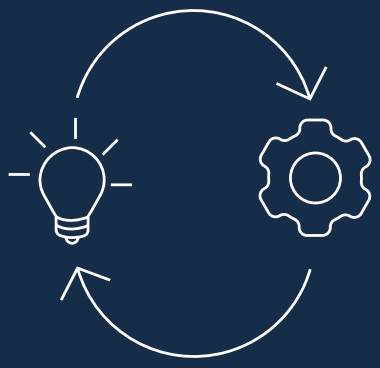
In this EU Casebook 2023, we have reviewed decisions published by the Data Protection Authorities of the Netherlands, Germany, Belgium, and Denmark in the period from May 2018 to May 2023. In compiling the statistical material, we have categorized decisions based on our judgment of the main themes of the cases.

For each decision in the Casebook, we present a summary delineating both the case's background and the decision taken by the respective data protection authority. In addition, we include our commentary on each decision, offering interpretive insights drawn from our legal case analysis. It should be noted that while the Casebook does not provide comprehensive coverage of all technicalities of the included cases, our summaries are deliberately tailored to highlight the questions we deem particularly significant or interesting for the reader.

Our summaries aim to provide an overview to readers working with GDPR and data protection law on a daily basis. Therefore, the Casebook should not be regarded as formal legal literature. Rather, the choice to write the Casebook in a user-friendly, accessible language is intentional. This approach enables our audience to gain a broad understanding of the rules' practical implications — catering to readers regardless of whether they have a legal background or not.

At ComplyCloud, we have been committed to delivering comprehensive and pertinent data protection resources since the General Data Protection Regulation came into effect in May 2018. We have consistently published a Danish Casebook each year, encompassing all decisions taken by the Danish Data Protection Authority. These Casebooks serve as a relevant resource for data protection professionals, offering concise and business-relevant legal analyses that help navigate the complexities of the field. Expanding on this commitment, we are now excited to announce the publication of our EU Casebook, providing an even broader perspective on data protection across the European Union.

The Casebook 2023 specifically highlights the decisions that lead to the 10 most substantial GDPR fines in each of our three focal countries; the Netherlands, Germany, and Belgium, complemented by 10 intriguing, handpicked cases from each of these countries. Recognizing ComplyCloud's core expertise, the Casebook also includes a collection of notable decisions by the Danish Data Protection Authority. To provide a broad perspective, the Casebook further incorporates 10 compelling cases from data protection authorities and judiciaries across various other EU countries.



About ComplyCloud

ComplyCloud is on a mission to empower businesses to achieve seamless compliance and build unwavering trust with simplified data protection and IT security.

We believe in privacy as an important human right, and we fight for a world where data and privacy are treated with fairness and transparency.

ComplyCloud was founded in 2017 and has established itself as a trailblazer in the realm of "IT-solution in legal/compliance. ComplyCloud is a full-service SaaS platform for data protection and IT security compliance that combines legal expertise and software to automate all task management and mandatory documentation.

Business Excellence Recognized: Proud Award Winner!

ComplyCloud ApS
CVR: 35813764
Borgergade 24B, 3.-4. sal
1300 København K
Danmark

www.complycloud.com

ComplyCloud