PRIVACY WEEK 2024:

BDO Legal insights into 2023 EU Case Law

INTRODUCTION

DATA PRIVACY WEEK 2024 IS AN IMPORTANT EVENT THAT HIGHLIGHTS THE SIGNIFICANCE OF DATA PRIVACY IN OUR LIVES.

Some of our BDO Legal European privacy experts have come togeher to prepare this **series of articles to give insights into some of the most impactful judgments of the Court of Justice of the European Union (CJEU) in 2023**.

The CJEU is the highest court in the European Union in matters of European Union law, and its judgments are binding on EU institutions and member states. **The judgments included in this publication have been instrumental in shaping the data privacy landscape in the EU** and we hope that it helps you to keep track of some of the key legal developments in EU data privacy in 2023.

CASE C-154/21

12/01/2023

Every person has the right to know to whom his or her personal data have been disclosed

INTRODUCTION

The Court of Justice of the European Union (CJEU) delivered a groundbreaking verdict in Case C-154/21, underscoring an individual's right to know the recipients of their personal data, underlining the significance of data transparency. To that extent, the Austrian Supreme Court referred the following question to the ECJ: *"Is Article 15(1)(c) of [the GDPR] to be interpreted as meaning that the right of access is limited to information concerning categories of recipients where specific recipients have not yet been determined in the case of planned disclosures, but that right must necessarily also cover recipients of those disclosures in cases where data [have] already been disclosed?"*.

SUMMARY OF THE CASE

Österreichische Post faced legal action when a citizen, citing the GDPR, demanded information on recipients' personal data. Initially providing vague details, the postal service disclosed during the proceedings that data had been shared with advertisers, IT companies, and charitable organisations.

The CJEU's judgment, issued on 12 January 2023, stipulates that when personal data are disclosed, the controller must, upon request, reveal the actual identity of recipients. However, if identification is impossible or the request is deemed unfounded, categories may be disclosed. The ruling reinforces the right of access, crucial for individuals to exercise GDPR rights, including rectification, erasure, and restriction of processing.

In consequence, to respect the right of access, all processing of personal data of natural persons must comply with the principle of transparency (information about the processing must be easily accessible and easy to understand) resulting in the choice of obtaining either information about the specific recipients to whom the subject data have been or will be disclosed, where possible, or information about the categories of recipients and, additionally that must enable the data subject to verify whether the data concerning him or her are accurate and whether they are processed lawfully.

CONCLUDING REMARKS: HOW IS THIS RELEVANT?

The CJEU's decision in Case C-154/21 sets a vital precedent, affirming individuals' right to know the actual recipients of their personal data. Emphasising transparency and accountability principles within the GDPR, the ruling empowers data subjects to effectively exercise their data protection rights. **The decision underlines the pivotal role of the right of access in facilitating a broader array of GDPR-mandated protections and safeguards for individuals in the European Union.**

For further information:

ALBERT CASTELLANOS
BDO Legal | Spain

albert.castellanos@bdo.es

DECISION T 557/20

26/04/2023

What is personal data (... and what IS NOT)?

INTRODUCTION

Despite eight years already of GDPR and even twenty-nine years since its predecessor directive was incepted, the very **notion of "personal data" in data protection law remains unclear. New decisions of EU courts (may) shed some new light.**

SUMMARY OF THE CASE

During the banking crisis, the Single Resolution Board (SRB) - an EU Trustee for banks in case financial turmoil – **was dealing with the struggling Banco Popular. SRB had asked for comments by shareholders and creditors on the valuation of the bank**. These comments were sent to Deloitte acting as independent experts. **Five commentators complained to the European Data Protection Supervisor (EDPS), stating that they were not informed about the transfer of their information, and that this violated their rights under GDPR**.

The SRB had implemented technical and organisational measures to collect the comments anonymously. It also claimed that it later manually ensured that Deloitte received no personal data. The reference to commentators was replaced by placeholders.

The EDPS considered the comments on personal data even though Deloitte had no knowledge of the identity of the authors. It reprimanded the SRB which sued the EDPB before the court.

The court held that the EDPS wrongly considered the data to be personally identifiable also for Deloitte even though they had no means to identify the commentators.

The General Court's decision is under appeal.

CONCLUDING REMARKS: HOW IS THIS RELEVANT?

The General Court decision is remarkable as it confirms the "relative" approach to personal data already mentioned in the Breyer Decision on IP-addresses. I.e. it is important if a recipient has the legal and factual means to (re-)identify the data subjects. Only where the recipient can identify individual persons, GDPR will apply.

The decision and its fate before the ECJ is important because new legislation such as the EU Data Act aims at making industrial data available for use. This, however, only works where such data is no longer subject to GDPR.

We may see a paradigm shift in data law in 2024!

For further information:

MATTHIAS NIEBUHR
BDO Legal | Germany

matthias.niebuhr@bdolegal.de

CASE C-300-21

04/05/2023

Compensation for non-material damages resulting from the infringement of GDPR

INTRODUCTION

Case *C-300/21* *(UI v Österreichische Post AG)* determines that the right to compensation does not arise from the infringement of the GDPR alone, an effective damage determined by the infringement must be proven.

CJEU emphasises that national courts must apply domestic rules to determine the compensation granted to data subjects.

SUMMARY OF THE CASE

The referring court sought clarification on whether the infringement of GDPR generates the right for the data subject to claim compensation in respect of art.82 of the Regulation.

The situation that led to the ruling consists of the fact that an Austrian company processed in the past the personal data of an individual without his consent and linked them, by using an algorithm "that takes into account various social and demographic criteria", to the individual's political preferences/affinities. **As a result of the processing, the individual claimed reputational damage and sought non-material damages.**

CJEU ruled that a mere infringement of the GDPR does not automatically generate the right for data subjects to claim compensation. Further, the Court laid down the 3 cumulative conditions under art.82 of GDPR that must be fulfiled to request such compensation, namely the infringement of the GDPR, the result of the infringement consisting in either material or non-material damages, and the existence of a link between the infringement and the damages suffered by the individual.

Further, the Court emphasised that the value of such compensation should be determined per the legislation of each member state as GDPR does not regulate such criteria for assessing the damage and CJEU cannot determine a minimum threshold.

CONCLUDING REMARKS: HOW IS THIS RELEVANT?

The importance of the ruling is represented by the fact that it clarifies the aspects related to the possibility of requesting compensation in case of an infringement of the GDPR only if the cumulative conditions indicated by the Court are fulfilled. The minimum threshold of these compensations is determined in accordance with the legal provisions of each Member State.

For further information:

CATALINA DAMASCHIN
BDO Legal | Romania

catalina.damaschin@tudor-andrei.ro

CASE C-487-21

04/05/2023

The extent of the data subject's right of access to his or her data

INTRODUCTION

Through *Case C-487/21* (*F.F. v Österreichische Datenschutzbehörde*) the CJEU determined the limits in which data subjects may exercise the right to access. Their data and the extent to which a copy of such data may be provided to them.

SUMMARY OF THE CASE

The referring court sought clarifications concerning the extent to which a data subject may exercise the right to access his/her data and a definition of the concepts of "copy" and "information".

CJEU determined that a data subject is entitled to receive from the data controller a "faithful and intelligible" reproduction of all the data "undergoing processing". In this sense, the Court interpreted the concept of "information" referred to in Article 15(3) GDPR in a broad context, namely referring to a "copy of all personal data undergoing processing".

CJEU determined that the term "copy" used by GDPR refers to obtaining a reproduction/duplication of the data processed, without referring as a rule to obtaining a duplicate of physical documents, nevertheless, not excluding the possibility of obtaining extracts or even entire documents containing the data subject's data if the provision of such documents is essential to enable the data subject to exercise effectively its rights under GDPR.

The Court emphasised that in case of conflict between the data subject's right to access his/her data extensively and the rights or freedoms of others, a compromise must be reached. Consequently, the controller must choose those methods of sharing personal data that, on one hand, do not infringe the personal rights and freedoms of other individuals, and on the other hand, do not limit the data provided to the data subject as a result of exercising his/her right to access.

CONCLUDING REMARKS: HOW IS THIS RELEVANT?

The ruling is important as it sets the limits in which a controller must act in response to the exercise by a data subject of the right to access his/her data under GDPR. It emphasises the obligation of the controller to provide a copy of all data that are being processed, with the express mention that in certain cases it may be necessary to provide physical extracts or copies of the documents containing this data, and the need to observe and respect the freedoms and rights of other individuals.

For further information:

CATALINA DAMASCHIN
BDO Legal | Romania

catalina.damaschin@tudor-andrei.ro

CASE C-252/21

04/07/2023

On appropriate security measures and non-material damage

INTRODUCTION

In Case C-252/21, the Court of Justice of the European Union (CJEU) affirmed the German Federal Cartel Office's ruling on Meta's unauthorised data linking, reinforcing national competition bodies' role in GDPR compliance. The decision challenges Meta's data necessity claims, while their introduction of a Paid Ad-Free Subscription continues to fuel debate on consent and privacy within digital services.

SUMMARY OF THE CASE

Meta Platforms Ireland, the operator of Facebook in the European Union, collected data about user activities on and off the social network and linked them with users' Facebook accounts without their consent. The German Federal Cartel Office found this practice to be an abuse of Meta Platforms Ireland's dominant position on the German market for online social networks and directed Facebook to change how it tracks customers' web surfing and use of browser apps.

The CJEU now upholds this decision, confirming that a national competition authority may assess compliance with the GDPR when it investigates whether a dominant position is abused. The national competition authorities must however consult and cooperate with the Data Protection Authorities to ensure consistent application of the regulation.

But more importantly, the court establishes that visiting websites or apps that may reveal special categories of data (such as racial origin, political opinions, sexual orientation, etc.) **does not in any way mean that the user manifestly makes this data public.** That means that processing such data is in principle prohibited by the GDPR.

In addition, Meta's claim that processing of data is necessary for the performance of the contract with the user was (more or less) **rejected**: this only applies if the data processing is objectively indispensable, and the main subject matter of the contract cannot be achieved without processing the data.

The claim that processing is necessary to fulfil legitimate interests faced the same fate: personalised advertising (by which Facebook finances its activity), cannot justify the processing of the data at issue; the data subject's consent is needed.

As you may know, Meta has found hope in one small sentence in the ruling mentioning that users who object to data processing are to be offered, if necessary for an appropriate fee, an equivalent alternative not accompanied by such data processing operations. This has brought Meta to offer a Paid Ad-Free Subscription in Europe. This has sparked new debate, as to whether this paid plan establishes "consent" of people who do not wish to pay for their privacy.

To be continued!

CONCLUDING REMARKS: HOW IS THIS RELEVANT?

This decision hinders Facebook's ad targeting capabilities and prevents Meta from leveraging data from all its services, as users must be free to refuse to data processing (unless necessary for the performance of the contract)**, without being obliged to stop using the social network**. The ruling highlights the need to obtain valid consent from users for the processing of their personal data (in this particular context) and sets a precedent for the business models used in the data economy.

For further information:

MICHA GROENEVELD
BDO Legal | Netherlands

micha.groeneveld@bdo.nl

CASES C-683/21 and C-807/21

05/12/2023

Only wrongful infringement of the GDPR merits administrative fines

INTRODUCTION

The Court of Justice of the European Union (CJEU) **in Cases C-683/21 and C-807/21, made significant rulings that provided important perspectives on the enforcement of the General Data Protection Regulation** (GDPR). These groundbreaking decisions not only established fresh benchmarks for administrative fines within the GDPR framework but also offered valuable insights into its application.

SUMMARY OF THE CASE

In the Lithuanian case (C-683/21), the National Public Health Centre contested a €12,000 fine for a Covid-19 monitoring app developed with a private partner. Simultaneously, Deutsche Wohnen, a German real estate giant, challenged a hefty €14 million fine for the extended storage of tenant data, derived from the case C-807/21.

The CJEU emphasised that only wrongful infringements, committed intentionally or negligently, merit administrative fines. Importantly, the awareness of the data controller regarding the nature of the infringement is pivotal, irrespective of the involvement of the management body. The rulings clarified that joint control does not necessitate a formal arrangement and entities acting as joint controllers must delineate responsibilities. Additionally, fines for entities within a group must be calculated based on the entire group's turnover.

CONCLUDING REMARKS: HOW IS THIS RELEVANT?

The CJEU's decisions mark a significant milestone in GDPR enforcement, establishing a stringent criterion of wrongful conduct for imposing fines. Holding legal persons accountable for infringements, irrespective of management body involvement, reinforces a robust data protection framework. The rulings provide flexibility in recognising joint control without a formal arrangement and underline the EU's commitment to comprehensive data protection. This clarity strengthens GDPR compliance and sets a precedent for future cases in the European Union.

For further information:

ALBERT CASTELLANOS
BDO Legal | Spain

albert.castellanos@bdo.es

CASE C-340/21

14/12/2023

On appropriate security measures and non-material damage

INTRODUCTION

After the 2019 cyberattack on Bulgaria's National Revenue Agency, leading to compensation claims for potential data misuse, the Court of Justice addressed the GDPR in Case C-340/21. It underlined the necessity of robust security measures, holding data controllers responsible for damages from third-party cyber attacks. Remarkably, the Court acknowledged the fear of data misuse as a legitimate form of non-material damage in the legal proceedings.

SUMMARY OF THE CASE

Following a cyberattack on the Bulgarian National Revenue Agency (the NAP) in 2019, personal data concerning millions of people was published on the internet. Many individuals brought legal actions against the NAP for compensation for non-material damage caused by the fear that their data might be misused.

The Bulgarian Supreme Administrative Court referred several questions to the Court of Justice for a preliminary ruling on the interpretation of the General Data Protection Regulation (GDPR), specifically regarding appropriate security measures and the conditions for awarding compensation for non-material damage.

On the topic of security measures, the Court confirmed:

- **that the controller of personal data should implement appropriate technical and organisational measures to ensure that processing is performed in accordance with the GDPR and to be able to demonstrate this.**
- **that the mere fact that unauthorised disclosure or access to personal data has taken place is not enough to establish that the technical and organisational measures were not 'appropriate'.** However, the controller bears the burden of proving that the protective measures implemented were appropriate.

On the matter of compensation for non-material damage the court confirmed that the fact that the damage resulted from a cyber attack from a third party does not release the controller from its liability, unless it can prove that it is in no way responsible for that damage. The Court also held that the fear experienced by a data subject with regard to a possible misuse of their personal data by third parties as a result of an infringement of the GDPR is capable, in itself, of constituting non-material damage.

CONCLUDING REMARKS: HOW IS THIS RELEVANT?

The Court of Justice of the European Union has clarified that the fear of possible misuse of personal data is capable of constituting non-material damage, even if there is no actual misuse of the data. The ruling also emphasises the importance of appropriate protective measures by controllers to prevent unauthorised access to personal data, and the need for controllers to prove the appropriateness of such measures. The decision also highlights the potential liability of controllers for the consequences of cyberattacks carried out by third parties, unless they can prove that they are not responsible for the damage caused.

For further information:

MICHA GROENEVELD
BDO Legal | Netherlands

micha.groeneveld@bdo.nl

FOR MORE INFORMATION:

MENNO WEIJ
HEAD OF GLOBAL IP/IT
& PRIVACY WORKING GROUP
BDO LEGAL | NETHERLANDS

+31 6 109 190 24
menno.weij@bdo.nl

CAROLINE MACDONALD
COORDINATOR | LEGAL SERVICES
BDO GLOBAL OFFICE

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