Vilnius Institute for Policy Analysis

JOURNALISTIC EXEMPTION UNDER THE EUROPEAN DATA PROTECTION LAW

NATALIJA BITIUKOVA

VILNIUS

2020

Table of Contents

Summary 3

Introduction 4

An introduction to the European legal framework 5

- Freedom of expression and freedom of media 6
- A right to privacy and data protection 7
- Approaches to balancing competing rights 8

An overview of the General Data Protection Regulation 10

- The scope of the Regulation 10
- The duties of controllers and processors 11
- The rights of the data subjects 12

A closer look at Article 85 of the GDPR 14

- Legislative history 14
- Comparative analysis 16
- The boundaries of a "journalistic exemption" 18
- Personal scope or who can rely on the exemption 19
- Material scope or what activities are exempted 20
- Nature of derogations or what rules do not apply 24
- Blurring boundaries and grey zones 26

Conclusions and recommendations 28

Annex I. An overview of Article 85 implementation in the selected EU Member States 31

Annex II. CoE Guidelines on safeguarding privacy in the media (excerpts) 34

Annex III. Summary in Lithuanian 38

About the Author 42

Vilnius Institute for Policy Analysis

POLICY PAPER
Natalija Bitiukova
"Journalistic Exemption Under European Data Protection Law"

www.vilniusinstitute.lt

SUMMARY

The primary aim of the "journalistic exemption" under the European data protection law is to address the tension between freedom of speech and a right to data protection and to codify the general need to balance these two fundamental rights.

The "journalistic exemption" is embedded in Article 85 of the General Data Protection Regulation (GDPR), and mostly follows the wording of the Article 9 of the Data Protection Directive (a predecessor of the GDPR).

It essentially creates a possibility for the Member States to exempt those who exercise their freedom of speech for "journalistic purposes" from specific GDPR rules and obligations, meaning that they would not need to comply with these rules. However, the boundaries of the exemption are not clearly outlined in the GDPR and are left to be defined by the Member States.

Therefore, the aim of the paper is to:

- understand the approaches taken by the Member States to implement Article 85 in the national legal frameworks,
- critically assess these approaches against the freedom of expression and data protection standards developed on the European level, and
- analyse their practical implications for journalists, media undertakings and anyone who exercises freedom of expression for journalistic purposes.

The research results in the conclusion that there are fundamental differences in how the Member States approach the definition and scope of the "journalistic exemption" across three dimensions:

- who can rely on the exemption or, in other words, what is its personal scope;
- what activities are exempted or what is the material scope;
- which rules do not apply as a result of the exemption or the nature of the derogations.

Such diverging approaches to the scope of the exemption create legal compliance challenges for those exercising freedom of expression, data subjects and, ultimately, is at odds with the primary goal of the GDPR - the establishment of "more coherent data protection framework in the Union". Moreover, the first constitutional challenge related to the national rules around "journalistic exemption" has recently resulted in finding the implementation of Article 85 of the GDPR unconstitutional in Bulgaria.

To address these challenges, the paper puts forward six recommendations, ranging from the legislative and regulatory to self-regulatory interventions. These recommendations are addressed to the EU Member States, supervisory authorities, and the interest groups, such as journalist and media associations, think tanks, and public interest groups.

INTRODUCTION

> "The GDPR was not created to be abused by politicians. I know some cases and I asked the European Data Protection Board to give us an interpretation. The GDPR should not be abused against journalists and access to information. Next year we will evaluate the GDPR to see how it works, I promise you this".
>
> Věra Jourová, Vice President-Designate – Values and Transparency[1]

Journalism refers to the production and distribution of information and news to an indeterminate number of people in pursuit of the public interest and contribution to the public debate. Inherently, journalism is about "collection and storage of huge amounts of personal information in the form of interviews, govern-ment and company records, as well as photo-graphs and films" and their dissemination. Thus, it is not surprising that when it comes to media activity, there have always been concerns related to privacy and data protection[2].

At the same time, it is recognized that the media plays an essential role in the exercise of freedom of expression. They serve as a "public watchdog" whose task is to control the conduct of public authorities, disseminate information on political issues and in other areas of public interest. Therefore, when acting in this capacity and to fulfil its watchdog obligations, the media has been granted exemptions from the general rules relating to data protection.

Such exemptions, collectively known as "journalistic exemption", has been recently re-introduced into the EU data protection law by virtue of Article 85 of the General Data Protection Regulation (GDPR). It essentially creates a possibility for the Member States to exempt those who exercise their freedom of speech for "journalistic purposes" from specific GDPR rules and obligations, meaning that they would not need to comply with these rules. However, the boundaries of the exemption are not clearly outlined in the GDPR and are left to be defined by the Member States.

This area has not received much scholarly attention yet[3] even though since GDPR became effective, the tensions between freedom of expression and data protection have only intensified. For instance, the Romanian data protection regulator had been criticized for using the GDPR to silence the critical voices in the national media[4]. While the Bulgarian Constitutional Court has recently declared the national approach towards the implementation of Article 85 unconstitutional[5].

Against this background, the aim of the paper is to:

- understand the approaches taken by the Member States to implement Article 85 in the national legal frameworks,
- critically assess these approaches against the freedom of expression and data protection standards developed on the European level, and
- analyze their practical implications for

[1] Pantazi C., Comisarul european pe Justiție, Vera Jourova, anunță evaluarea reglementărilor privind protecția datelor personale (GDPR) după sesizările presei independente privind abuzurile autorităților, 18 October 2019, https://www.g4media.ro/comisarul-european-pe-justitie-vera-jourova-anunta-evaluarea-reglementarilor-privind-protectia-datelor-personale-gdpr-dupa-sesizarile-presei-independente-privind-abuzurile-autoritatilor.html.

[2] Erdos D., European Regulatory Interpretation of the Interface between Data Protection and Journalistic Freedom: An Incomplete and Imperfect Balancing Act? (October 29, 2015). A revised version of this paper is in Public Law (2016 Forthcoming); University of Cambridge Faculty of Law Research Paper No. 61/2015, p 8.

[3] The legal scholarship on this issue is still developing, but see e.g. T. McGonagle, a note ECJ EU 14-02-2019, C-345/17, 19 May 2019, https://www.recht.nl/vakliteratuur/europa/artikel/460744/hvj-eu-14-02-2019-c-345-17/ and McCarthy, H. (2019). Expanding the GDPR's journalism exemption – is all the world a stage? Privacy & Data Protection, (4), 10.

[4] https://www.liberties.eu/en/news/politicians-in-romania-use-gdpr-to-intimidate-journalists/16384.

[5] Bulgaria's Constitutional Court rejects data protection law clause, 17 November 2019, https://sofiaglobe.com/2019/11/17/bulgarias-constitutional-court-rejects-data-protection-law-clause-on-media/.

journalists, media undertakings and anyone who exercises freedom of expression for journalistic purposes.

The timing of the inquiry is particularly relevant as the European Commission is currently undertaking the review of the GDPR, which, along with the possible proposals for changes, will be presented to the Council and the European Parliament by 25 May 2020. It is hoped that the analysis undertaken by the author will be useful for the interest groups who plan to take part in this review, specifically on the subject of the "journalistic exemption".

AN INTRODUCTION TO THE EUROPEAN LEGAL FRAMEWORK

This chapter provides an overview of the relationship between the right to privacy and data protection and freedom of expression in Europe. The first subsection is aimed at introducing the readers, less familiar with the European legal order, to the Council of Europe and the European Union legal systems.

Founded in 1949, the Council of Europe is one of the oldest and the biggest European orga-nization, which unites 47 member states and promotes the main principles of human rights[6]. In 1950, the Council of Europe adopted the European Convention on Human Rights[7] (the Convention or the ECHR), which established the European Court of Human Rights (the Strasbourg Court or the ECtHR). The ECtHR hears cases brought by the applicants on the alleged violations of the rights enshrined in the ECHR, including a right to private life (Article 8) and a right to freedom of expression (Article 10).

In 1981, due to the increasing concerns related to the treatment of personal data and its cross-border sharing, the Council of Europe opened for signature the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108)[8]. To this day, the Convention 108 is the only international legally binding agreement on the data protection law. However, the European Court of Human Rights does not hear cases on the alleged violations of this Convention.

The European Union (EU) has its origin in the European Communities formed in the 1950s as a form of economic cooperation between the European countries. The EU was formally established in 1992 by the Maastricht Treaty. In 2000, the Charter of Fundamental Rights of the European Union (Charter)[9] was adopted, which includes the right to freedom of expression (Article 10), a right to privacy (Article 7), as well as a self-standing right on the protection of personal data (Article 8). Alleged violations of the EU law are heard by the Court of Justice of the European Union (CJEU). Majority of the cases are initiated by the national judges referring questions to the Court.

Since the 1990s, the EU has played an important role in the field of data protection law. The EU-level data protection law harmonization effort resulted in the Data Protection Directive of 1995, which from 2018 is effectively replaced by the

[6] Council of Europe, About the Council of Europe – Overview, https://www.coe.int/en/web/yerevan/the-coe/about-coe/overview.

[7] European Convention on Human Rights, https://www.echr.coe.int/Documents/Convention_ENG.pdf.

[8] Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108), https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37.

[9] https://www.liberties.eu/en/news/politicians-in-romania-use-gdpr-to-intimidate-journalists/16384.

Freedom of expression and freedom of media

Article 10 of the European Convention on Human Rights (CoE):

> 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises .
> 2. The exercise of these freedoms since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary. .

Article 10 of the EU Charter of Fundamental Rights (EU)[12]:

> 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. .
> 2. The freedom and pluralism of the media shall be respected. .

General Data Protection Regulation (GDPR). There is no equivalent piece of overarching and comprehensive secondary legislation in the free speech and media freedom mostly due to the Commission's position that the EU has no authority to legislate in this area.

Freedom of expression is one of the fundamental human rights in a democratic society. Freedom of expression has a special status in comparison with other human rights because it is considered to be not only the outcome of democratic governance but also its basis. Without free debates and the pluralism of expression democracy cannot progress or survive[13].

Freedom of expression includes the right to have and express one's beliefs (opinions), the right not to disclose one's beliefs (opinions) and the right to receive and impart information[14]. As a matter of principle, the protection of freedom of expression extends to all forms of expression through written statements, paintings, films or photographs, disseminated by any individual, group via any type of media, both online and offline[15].

In the ECtHR, jurisprudence media plays an essential role in the exercise of freedom of expression. It serves as a "public watchdog" whose task is to control the conduct of public authorities, disseminate information on political issues and other areas of public interest. In practice if a person demonstrates that they were acting in their journalistic capacity, according to the ECtHR, they should benefit from additional protection afforded to media under Article 10[16].

As the European Court of Human Rights has found in Castells v. Spain case: "(f)reedom of the press affords the public one of the best means of

[12] The rights under Article 11 of the Charter correspond to those of Article 10 ECHR. See Explanations relating to the Charter of fundamental rights, C 303/17, 14 December 2017, p. 5, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0017:0035:en:PDF.

[13] Bitiukova N., Hate Speech in Lithuania: Frequently Asked Questions (FAQ), 2013, http://hrmi.lt/wp-content/uploads/2016/08/Neapykantos_kurstymas_EN.pdf, p. 21.

[14] INTERIGHTS.Freedom of Expression under the European Convention on Human Rights (Article 10). Manual for lawyers, 2009, http://www.interights.org/documentbank/index.htm?id=519, p. 7.

[15] See e.g., EctHR, The Sunday Times v. United Kingdom, 1979 April 26, App No 6538/74 and EctHR, The Sunday Times v. United Kingdom (No. 2), 1991 November 26, App No 13166/87.

[16] See e.g., ECtHR, The Observer and Guardian v. UK, 26 November 1991, Application No. 13585/88, para. 59.

discovering and forming an opinion of the ideas and attitudes of their political leaders. In particular, it gives politicians the opportunity to reflect and comment on the preoccupations of public opinion; it thus enables everyone to participate in the free political debate which is at the very core of the concept of a democratic society"[17].

The Court of Justice of the EU (CJEU) also started very early to see the importance of media pluralism not only for the free movement of services across the EU but also in order to ensure pluralism in views. It accounted expressly for the importance of media pluralism and media freedom for the internal market as well as for democracy in the EU[18].

The right to respect for private life[19] and the right to personal data protection, although closely related, are distinct rights[20]. Both strive to protect similar values, i.e. the autonomy and human dignity of individuals, by granting them personal sphere in which they can freely develop their personalities, think and shape their opinions.

However, the two rights differ in their formulation and scope. The right to respect for private life consists of a general prohibition of interference, subject to some public interest criteria that can justify the interference in some instances. The scope of the right to private life is particularly broad, and it may apply to a variety of circumstances ranging from forced medical treatment, end of life issues to right to a name and identity documents, lawyer-client relationship and so on[21].

A right to privacy and data protection

Article 8 of the European Convention on Human Rights (CoE):

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 7 of the EU Charter of Fundamental Rights (EU):

Everyone has the right to respect for his or her private and family life, home and communications.

Article 8 of the EU Charter of Fundamental Rights (EU):

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

[17] EctHR, Castells v. Spain, 24 April 1992, Application No. 11798/85, 14 EHRR 445, para. 43.

[18] CJEU, Elliniki Radiophonia Tileorassi AE v Dimotiki Etairia Pliroforissis and Sotirios Kouvelas, C-260/89, 18 June 1991, para. 3. The Court held that a Greek broadcasting monopoly was unacceptable not only in the context of the freedom to provide services but also to ensure a range of voices are available to the public.

[19] In this paper, the right to private life is used interchangeably with the right to privacy.

[20] European Union Agency for Fundamental Rights and Council of Europe, Handbook on European data protection law, 2018, https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf, p. 18.

The protection of personal data, on the other hand, is viewed as a modern and active right, putting in place a system of checks and balances to protect individuals whenever their personal data are processed. The processing must comply with the essential components of personal data protection, namely independent supervision and respect for the data subject's rights[22]. While in the Council of Europe legal order, the right to data protection is "derived" from the right to private life under Article 8, the EU law suggests a more nuanced approach and separates these two rights into two distinct articles under the EU Charter (Articles 7 and 8).

As with the freedom of expression, the importance of the right to data protection has been underlined in the jurisprudence of both the ECtHR and the CJEU as analysed below.

Approaches to balancing competing rights

Privacy and freedom of expression have equal weight in the case-law of the European Court of Human Rights. According to the Court, "as a matter of principle these rights deserve equal respect." At the same time, none of the rights is absolute.

The conditions for limiting the right to freedom of expression and the right for private life are listed in Article 8 of the ECHR and Article 52 (1) of the Charter. They have been developed and interpreted through the case-law of the ECtHR and the CJEU[23] (see Table 1 below).

It depends on the circumstances in a particular case which right should prevail. The courts have developed a large body of case law on balancing privacy and freedom of expression. The courts take a nuanced approach, taking all circumstances of a case into account. For example, when determining whether a contested publication about a specific individual transgressed the limits of lawful expression and resulted in the interference with private life, the ECtHR has developed a set of criteria including:

- whether the event that the published article concerned was of general interest;
- whether the person concerned was a public figure;
- how the information was obtained, whether the information was reliable;
- whether or not the expression in question contributes to a debate of general public interest[24].

Thus, by examining each situation case-by-case,

TABLE 1

ECtHR (CoE)	Charter of Fundamental Rights (EU)
Interference with the freedom of expression and a right to private life can be carried out if it: • is in accordance with the law; • pursues a legitimate aim; • respects the essence of the fundamental rights and freedoms; • is necessary and proportionate in a democratic society to achieve a legitimate purpose.	Any limitations on the fundamental rights can be lawful if it: • is in accordance with the law; • respects the essence of the right; • subject to the principle of proportionality, is necessary; and • pursues an objective of general interest recognised by the EU, or the need to protect the rights of others.

[21] ECtHR, Guide on Article 8 of the European Convention on Human Rights. Right to respect for private and family life, home and correspondence, https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf.

[22] European Union Agency for Fundamental Rights and Council of Europe, Handbook on European data protection law, 2018, p. 19.

[23] The table is based on the European Union Agency for Fundamental Rights and Council of Europe, Handbook on European data protection law, 2018, p. 36.

[24] See e.g. ECtHR, Axel Springer AG v. Germany [GC], 7 February 2012, App No 39954/08, paras. 90 and 91 and ECtHR, Mosley v. the United Kingdom, 10 May 2011, App No 48009/08, paras. 129 and 130.

the Court reaches a conclusion taking specific circumstances into account[25].

One of the most notorious and controversial examples of reaching a balance between the freedom of expression and a right to data protection was a Google Spain case, decided by the CJEU. The case concerned removal from Google's search results references to information available in the internet archives of one of the Spanish newspapers. The information regarded outdated financial liabilities of Mr Gonzales and was published at the request of the Spanish authorities in 1998. In this case, the CJEU determined that the individuals have a right to have their Google search results containing personal data about them delisted because "the data subject's privacy and data protection rights override, 'as a rule', the search engine operator's economic interests, and the public's interest in finding information"[26]. However, to ensure that the balance is fair, the court also found a caveat to this general rule. Namely, it stressed that the data subjects' rights should not prevail if the interference with their rights can be justified by the public's interest in accessing information, for example, because of the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life[27]. This approach resembles the approach of the ECtHR when balancing freedom of expression and a right to private life and data protection as explained in the preceding paragraph.

However, freedom of expression and privacy and data protection are not in constant and perpetual conflict. There are instances where the effective protection of data protection and privacy rights guarantees at the same time freedom of expression.

For example, the UK bulk surveillance of electronic communication regime was found to interfere with data protection and privacy rights[28]. At the same time, the ECtHR found that it also negatively affected freedom of expression as it could have discouraged individuals from freely disseminating and receiving information via those means[29]. A similar conclusion was made by the CJEU in the case concerning a Swedish regime for mandatory retention of traffic and location data as well as the metadata of all subscribers and users of electronic communications services. The Court noted that where the data were retained and subsequently used without the subscriber or registered user being informed, it was likely to generate in the minds of the persons concerned the feeling that their private lives were the subject of constant surveillance. This was found to be incompatible with Articles 7, 8 and 11 of the Charter[30].

Despite involving different wording, conditions for lawful limitations on the rights in Article 52 (1) of the Charter are reminiscent of Article 8 (2) of the ECHR concerning the right to respect for private life. In their case law, the CJEU and the ECtHR often reach same conclusions in similar cases and refer to each other's judgments, as a part of the constant dialogue between the two courts to seek a harmonious interpretation of data protection rules[31]. Therefore, when analysing the provisions of the EU law the interpretation of ambiguities can be found in the jurisprudence of the ECtHR, as shown in this paper.

[25] Kulk, S., & Zuiderveen Borgesius, F. (2018). Privacy, Freedom of Expression, and the Right to Be Forgotten in Europe. In E. Selinger, J. Polonetsky, & O. Tene (Eds.), The Cambridge Handbook of Consumer Privacy (pp.301-320). Cambridge: Cambridge University Press, https://pure.uva.nl/ws/files/9113768/Kulk_Zuiderveen_Borgesius_RTBF_chapter_2Feb2017.pdf, p.8.

[26] Kulk, S., & Zuiderveen Borgesius, F. (2018). Privacy, Freedom of Expression, and the Right to Be Forgotten in Europe. In E. Selinger, J. Polonetsky, & O. Tene (Eds.), The Cambridge Handbook of Consumer Privacy (pp.301-320). Cambridge: Cambridge University Press, pp.20-21.

[27] CJEU, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, C-131/12, 13 May 2014, para. 81.

[28] ECtHR, Big Brother Watch and Others v. the United Kingdom, App nos. 58170/13, 62322/14 and 24960/15, 13 September 2018.

[29] Ibid., para. 495.

[30] CJEU, Joined Cases Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v. Watson, C-203/15 and C-698/15, 21 December 2016.

[31] European Union Agency for Fundamental Rights and Council of Europe, Handbook on European data protection law, 2018, p.51.

AN OVERVIEW OF THE GENERAL DATA PROTECTION REGULATION

Since 1995, the rights of data subjects in the EU level were regulated by the Data Protection Directive. Eventually, the legal framework created in the last century was no longer able to meet the expectations of the digital society and cope with new data protection challenges. Data collection and data sharing increased significantly in scope, while economic and social integration led to greater cross-border data traffic.

In order to fully account for these developments, the European Commission launched the so-called Data Protection Reform, the crux of which was the General Data Protection Regulation[32]. The Regulation was finally adopted in April 2016, after nearly four years of negotiations between the European Commission, the Council, the European Parliament and business representatives, non-governmental organizations and other interested parties[33]. The Regulation became effective on 25 May 2018, giving both Member States and businesses time to prepare for its implementation[34].

It is important to note that, unlike the Data Protection Directive, the Regulation has a direct effect. This means that there is no need to transpose its provisions into national law and that it has legal effect from its entry into force. However, the Regulation gives discretion to the Member States in certain areas – that is, they can choose how legal relations shall be regulated. For example, the Regulation provides that Member States may introduce proportional restrictions on data subjects' rights into national law when such restrictions are necessary for the purposes of national security, defence, prevention of crime and the like[35]. It is estimated that the Regulation contains more than fifty such "flexible" provisions[36], and Article 85, which foresees the "journalistic exemption" is one of them.

The scope of the Regulation

Regulation preserves the fundamental provisions of the Directive. Personal data may only be processed if there are lawful grounds for doing so, with these grounds (consent, public interest, legitimate interest, etc.) being essentially the same as before[37]. Data processing must also comply with data processing principles, including transparency, storage limitation, data minimization and others[38]. Importantly, the Regulation introduces the seventh overarching quasi-principle of "accountability", which essentially means that data controller is not only responsible for compliance with the data processing principles, but should also be able to demonstrate it[39].

The notion of personal data is interpreted, as before, broadly, and includes any information about an identified or identifiable individual[40], including the data which was already made public[41]. Importantly, such individual (known as "a data subject" under the GDPR) does not have to be an EU citizen or resident – as long as they are present in the EU when the processing takes place, they can exercise their rights under the GDPR[42].

Personal data "processing" is also understood

[32] European Commission, „Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses", Europa.eu, 25 January 2012, http://europa.eu/rapid/press-release_IP-12-46_lt.htm.

[33] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC.

[34] Article 99(2) of the GDPR.

[35] Article 23 of the GDPR.

[36] EDRi, Proceed with Caution. Flexibilities in the General Data Protection Regulation, https://edri.org/files/GDPR_analysis/EDRi_analysis_gdpr_flexibilities.pdf.

[37] Article 6 of the GDPR.

[38] Article 5 of the GDPR.

[39] Ibid.

[40] Article 4(1) of the GDPR.

[41] Article 9(1)(e) of the GDPR.

[42] Article 3(2) of the GDPR.

broadly and includes any type of automated or semi-automated[43] operation performed on the data, such as data collection, storage, analysis, viewing, deletion and others[44]. There is a limited number of activities that are explicitly outside the scope of the Regulation, but they are mostly applicable to the state institutions. Also, purely personal activities are not regulated by the GDPR (a so-called "household exemption")[45].

The Regulation retains the prohibition on processing special categories of personal data (data about health, sexual orientation, trade union membership, etc.) unless an exception applies. The category of sensitive data has been expanded to include genetic and biometric data[46].

One of the most prominent changes is the expansion of the scope of the Regulation. The Regulation applies to business entities established in any EU country, irrespective of whether the data itself is being processed in EU territory. The big change is that the Regulation provides for the so-called "extraterritorial application" – that is, even business entities that have been established outside the EU (e.g. in the US, Brazil, China) must comply with the Regulation in certain cases.

The duties of controllers and processors

As a general rule, the Regulation applies to all type of legal entities and natural persons, including state institutions, private companies, non-profit organizations, churches and religious associations, media companies, freelance journalists, sole traders and others. There are exceptions from this general rule such as a household exception discussed above or a journalistic exemption which is at the centre of this research.

Where these legal or natural persons are not availed an exception, they should comply with a range of obligations set out in the Regulation. The scope of the obligations will largely depend on their role in the data processing. If they make a decision about "why" and "how" the personal data should be processed, they become data controllers[47] and are fully responsible and liable for the processing operations. Some of the data controller's obligations include:

- Compliance with the data processing principles, carrying out data protection impact assessments, publishing privacy notices, performing legitimate interests assessments, etc.
- Responding to the requests of the data subjects, such as requests for data access, rectification, erasure, etc.
- Implementing appropriate technical and organizational security measures to ensure the security of personal data, such as encryption, anonymization, logging control, etc.
- Notifying supervisory authorities and data subjects, where relevant, about the data breaches.
- Appointing a data protection officer

[43] "Processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system." Article 2(2) of the GDPR.
[44] Article 4(3) of the GDPR.
[45] Article 2(2) of the GDPR.
[46] Article 9 of the GDPR.
[47] European Commission, What is a data controller or a data processor?, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en.

where mandatory or necessary.

If an entity or an individual is instructed to process personal data (e.g., data centres that store personal data on customers' behalf) they would be considered under the GDPR as data processors. They can also be held liable under GDPR for non-compliance with the controller's instructions or their self-standing obligations, such as:

- Entering into a binding contract with the data controller.
- Implementing appropriate technical and organizational security measures to ensure the security of personal data, such as encryption, anonymization, logging control, etc.
- Notifying data controller about personal data breaches.

Media companies and freelance journalists, in the course of their typical activities (investigation and publication of news stories), will be considered DATA controllers with all of the obligations deriving from that status, unless the journalistic exemption under the national law will exempt them from it.

The Regulation lays down significant fines for violations of these rules, which can amount to €20 million or up to 4% of the company's total worldwide annual turnover of the preceding financial year, whichever is higher[48]. Of course, such fines are reserved for exceptionally serious, intentional violations, but it marks a stark contrast to the pre-existing regime in the EU members states, including Lithuania[49]. The Regulation does not set a minimum fine, leaving that to the Member States.

The fines are typically (with the exception of Estonia and Denmark) imposed by the supervisory authorities (state institutions responsible for the enforcement of the GDPR, also known as the data protection authorities). The supervisory authorities also have powers to carry out inspections, impose non-financial sanctions and alike. There is at least one independent authority in each EU Member State, while in some, there are two or more authorities. For instance, in Lithuania, the supervision and enforcement powers are shared between the State Data Protection Inspectorate and the Office of the Inspector for Journalist Ethics. The latter's competence is focused on overseeing the processing of personal data for journalistic purposes and the purposes of academic, artistic or literary expression. When exercising its powers, the Inspector for Journalist Ethics must cooperate with the DPA to ensure the consistent application of the data protection laws[50].

The rights of the data subjects

Notably, the GDPR strengthens the rights of the individuals (data subjects), which now are the following:

- The right to be informed. The principle of fair and transparent processing requires data controllers to provide individuals with information about how their data is being processed[51]. To ensure that individuals are able to effectively enjoy this right, the information should be provided in a "transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child[52].
- The right of access. This right, commonly

[48] Article 83(5) of the Regulation.

[49] For instance, Article 82 of the Code of Administrative Offences of the Republic of Lithuania, which came into force on 1 January 2017, provided that personal data security breaches may be subject to fines up to €3,000. Code of Administrative Offences, 25 June 2015, No. XII-1869, https://www.e-tar.lt/portal/lt/legalAct/4ebe66c0262311e5bf92d6af3f6a2e8b/IJpyIHVrJb.

[50] From Bitiukova N., Lithuania adopts new Law on Legal Protection of Personal Data, 16 July 2018, https://iapp.org/news/a/lithuania-adopts-new-law-on-the-legal-protection-of-personal-data/.

[51] Article 5(1)(a) of the GDPR.

referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why their data is being used and check whether it is done lawfully[53].

- The right to rectification. The Regulation allows individuals to ask the data controller to rectify inaccurate or outdated data.

- The right to erasure. Also known as "a right to be forgotten", this right allows individuals to request deletion of their data held by the data controller where such data is no longer necessary, was collected unlawfully and in other circumstances.

- The right to restrict processing. The Regulation provides for the person's right to temporarily suspend the processing of their data.

- The right to data portability. The new right to data portability gives individuals the right to receive personal data they have provided to a data controller in a structured, commonly used and machine-readable format. It also gives them the right to request that a data controller transmits this data directly to another controller[54].

- The right to object. Individuals can object to the processing of their personal data at any time. This effectively allows individuals to stop or prevent data controllers from processing their personal data.

- Rights in relation to automated decision making and profiling. Where important decisions about a person are made by an algorithm without human intervention, the data controller is required to give individuals specific information about the processing, take steps to prevent errors, bias and discrimination; and give a right to challenge and request a review of the decision.

The data controller must respond to the data subject request related to the exercise of any of the rights outlined above within one month of receipt of the request; that period may be extended by two further months where necessary, taking into account the complexity and number of the requests. Majority of these rights are not absolute, and thus the requests can be overridden by the data controller's or public's interests. For example, the request for erasure will not be satisfied if the data is still necessary for freedom of expression and information purposes, however, in line with the accountability principle, it falls on the data controller to prove that it is the case.

Just like before, if a person believes that his or her rights have been violated (for example, they received no reply from the controller regarding a request to access data), he or she can complain to a supervisory authority.

[52] Article 12(1) of the GDPR.

[53] UK Information Commissioner's Office, Guide of the General Data Protection Regulation. Right to access, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/.

[54] UK Information Commissioner's Office, Guide of the General Data Protection Regulation, Right to data portability, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/.

A CLOSER LOOK AT ARTICLE 85 OF THE GDPR

Legislative history

The primary aim of the "journalistic exemption" under the data protection law is to address the tension between freedom of speech and a right to data protection and to codify the general need to balance these two fundamental rights – an approach embedded in the CoE and EU law and followed by both the ECtHR and the CJEU. It essentially creates a possibility for the Member States to exempt those who exercise their freedom of speech for "journalistic purposes" from specific GDPR rules and obligations discussed above, meaning that they would not need to comply with these rules.

"Journalistic exemption" is not a new concept in the EU data protection law. The Data Protection Directive of 1995[55], the predecessor of the GDPR, also included a similar provision, which the Regulation subsequently grandfathered, albeit with some changes.

The Member States had transposed Article 9 of the Directive into the national law in considerably diverging ways. As summarized by the Working Party 29 in 1997:

> **a)** In some cases data protection legislation does not contain any express exemption from the application of its provisions to the media. This is the current situation in Belgium, Spain, Portugal, Sweden and the United Kingdom.
>
> **b)** In other cases the media are exempted from the application of several provisions of data protection legislation. This is the current situation in the case of Germany, France, The Netherlands, Austria and Finland. Similar derogations are envisaged by the draft Italian legislation.
>
> **c)** In other cases the media are exempted from general data protection legislation and regulated by specific data protection provisions. This is the case in Denmark for all media and in Germany in relation to public broadcasters, which are not covered by federal or Länder data protection laws, but are subject to specific data protection provisions in the inter-Länder treaties which regulate them[57].

Naturally, this mosaic of transposition approaches coupled with differing historical backgrounds in the Member States resulted in the supervisory authorities, charged with the

Article 9 of the Data Protection Directive (Processing of personal data and freedom of expression)

Member States shall provide for exemptions or derogations from the provisions of this Chapter (general rules on the lawfulness of the processing of personal data)[56], Chapter IV (transfer of personal data to third countries) and Chapter VI (supervisory authorities) for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

[55] On the legislative history of Article 9 of the Directive see Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Data protection law and media, Recommendation 1/97, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1997/wp1_en.pdf, pp.5-6.

[56] Information in square brackets added by the author.

[57] Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Data protection law and media, Recommendation 1/97, pp. 6-7.

monitoring and enforcement of the data protection laws, holding sometimes conflicting views as to how these provisions should be applied to scenarios relevant for media professionals.

These inconsistencies were well documented in the 2013 survey carried among 75% of the EU/EEA supervisory authorities. Consider, for instance, the responses provided by the regulators to the first question of "whether an individual who was the subject of a journalistic investigation by a media entity had the right to access the data held by that entity in the context of the investigation"[58] (see Figure 1).

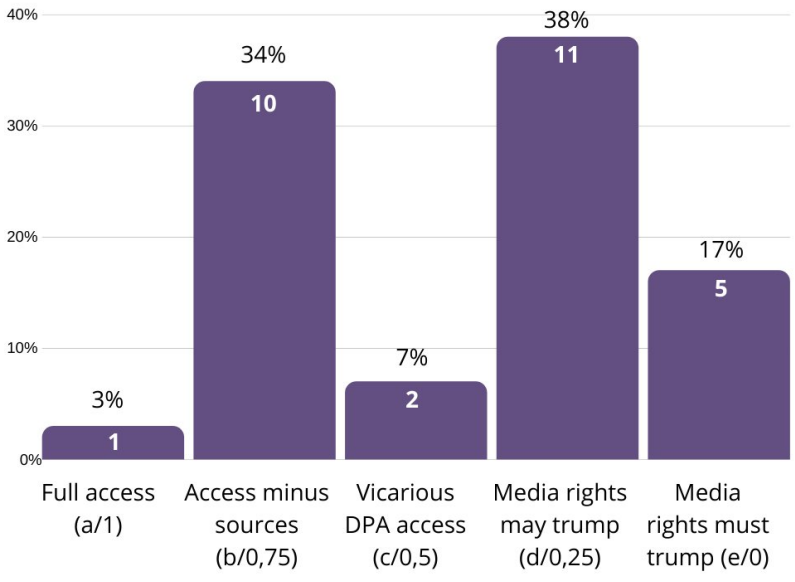
Below (see Table 2) there are comparable interpretation suggested by the regulators with the statutory law provisions.

The majority (eleven) of the regulators stated that a person would be able to access all the information except for the journalist's sources, while ten held that, whilst an individual had a right to make a subject access request, it might nevertheless be outweighed by the media's rights including to freedom of expression. Five authorities held the strictest view that a data subject won't be able to access information in the media context, while one DPA had a completely opposite view – that subject access would apply without any distinction to the media, as it applies to other data controllers. Two regulators suggested that a modified procedure could apply whereby the authority itself would access the data on behalf of the data subject[60].

Although seemingly all but one authority made attempts to balance freedom of expression and data protection (even if this was not prescribed by the national laws), these attempts were "both incomplete and imperfect"[62]. This is troublesome especially given the nature of the scenario

FIGURE 1

Subject Access and Journalism — DPA Standardized Responses (n = 29)[59]



[58] Erdos D., European Regulatory Interpretation of the Interface between Data Protection and Journalistic Freedom: An Incomplete and Imperfect Balancing Act? (October 29, 2015). A revised version of this paper is in Public Law (2016 Forthcoming); University of Cambridge Faculty of Law Research Paper No. 61/2015, p. 14.

[59] Ibid., p. 16.

[60] Ibid., p. 15.

TABLE 2

Subject Access and Journalism: Statutory Law vs DPA Interpretation[61]

Statutory law (n=30)> DPA Interp. (n= 29)v	Full access (a/1) 7 (23%)	Access minus sources (b/0,75) 3 (10%)	Vicarious DPA access (c/0,5) 2 (7%)	Media righte may trump (d/0,25) 9 (30%)	Media rights may or must trump (de/ 0,125) 5 (17%)	Vicarious DPA access (c/0,5) 2 (7%
Full access (a/1) 1 (3%)	- Cyprus					
Access minus sources (b/0,75) 10 (34%)	- Greece - Slovakia - Slovenia	- Italy - Bulgaria		- Belgium - Estonia - Malta - Gibraltar	- Germany / Schleswig-Holstein	
Vicarious DPA access (c/0,5) 2 (7%)			- Luxembourg - Portugal			
Media righte may trump (d/0,25) 11 (38%)	- Czech Republic - Latvia - Spain / Catalonia	- Hungary		- Ireland - Liechtenstein - Poland	- Germany Federal - Germany Brandenburg - Germany Mecklenburg-Vorpommern	- Lithuania
Media rights may or must trump (de/ 0,125) 5 (17%)				- France	- Germany Rhineland-Palatinate	- Austria - Finland - Sweden
Free-text (1 response outside formal calculations)				- United Kingdom		

presented to the authorities — it is likely that the media professionals receive access requests quite often and thus it is paramount for them to have clear guidance on how to respond to the individuals.

Comparative analysis

As mentioned above, although the primary aim of the GDPR is to harmonise the data protection law across the EU, it also gives discretion to the Member States to independently determine how certain areas (historically falling in the area of the Member States competence) should be regulated. In addition to "journalistic purposes," such areas include employment, functioning of religious associations, archiving and research purpose, and so on[63].

Under GDPR, the "journalistic exemption" is codified in Article 85 and is based mainly on Article 9 of the Directive, discussed previously[64].

The first and the most apparent difference between Article 9 of the Directive and Article 85 of the GDPR[65] is in the wording of the exemption:

[61] Ibid., p. 17.

[62] Ibid., p. 34.

[63] It should be noted, however, that not all "flexible" provisions are worded in the identical manner. For instance, Article 85 is formulated as an imperative directive ("shall by law reconcile" and "shall provide for exemptions or derogations") to the Member states to provide exemptions from the GDPR when the data processing takes place for journalistic and other enumerated purposes. Conversely, Article 88, providing for a margin of flexibility to regulate data processing in the employment context, is worded as a non-binding option ("may, by law or by collective agreements, provide for more specific rules").

[64] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Explanatory Memorandum, COM(2012) 11 final, 25 January 2012, https://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf, p. 15.

Article 85 of the GDPR. Processing and freedom of expression and information

1. Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.
2. For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.
3. Each Member State shall notify to the Commission the provisions of its law which it has adopted pursuant to paragraph 2 and, without delay, any subsequent amendment law or amendment affecting them.

while Article 9 spoke of "processing of personal data carried out solely for journalistic purposes", Article 85 talks of "processing carried out for journalistic purposes". In other words, the word "solely" is no longer present. Legally speaking, this could point towards an objective of the broader interpretation of the "journalistic purposes" concept. For instance, this was a position which the Swedish government had taken during the national discussions on the implementation of Article 85, which resulted in carving out particularly broad exemptions from the application of the GDPR — something that had been criticized by the Swedish data protection authority[66]. This question will be revisited when discussing the material scope of the exemption later in the paper.

Secondly, the third part of Article 85 introduces a new obligation to notify the Commission about the legislation adopted on the national "without delay"[67]. However, this obligation was reflected in the general Article 32 of the Directive, which required the Member States to transpose the Directive and inform the Commission about the adopted domestic laws, and thus, this difference is immaterial.

Lastly, although it may seem that the Regulation had broadened the areas where the exception applies by including more chapters, in fact, the areas remain mutatis mutandis the same as were previously outlined in the Directive.

Overall, the GDPR maintained a significant margin of the flexibility of the Member States as to how they interpret Article 85 and strike the right balance between data protection and freedom of expression in their national legislations, without any additional guidance on the reconciliation of these rights.

Such an approach runs contrary to the underlying objective of the Regulation — the establishment of "a strong and more coherent data protection framework in the Union"[68]. Especially

[65] Differences between the articles unrelated to journalism are not discussed in this paper.

[66] Cullagh K. et al, National adaptations of the GDPR, Luxembourg: Blogdroiteuropéen, 17 February 2019, https://blogdroiteuropeen.files.wordpress.com/2019/02/national-adaptations-of-the-gdpr-final-version-27-february-1.pdf, p. 47.

[67] Notably, not all "flexible" provisions carry such an obligation. Other provisions in Chapter IX of the GDPR include Article 88 (processing in the employment context) and Article 90 (Obligation of secrecy). Conversely, e.g. Article 86, which includes a possibility for the Member States to regulate processing and public access to official documents, does not carry an obligation to notify the Commission about such as law.

so, given the uneven national implementation of Article 9 discussed above. The differences in the national implementation may also create practical difficulties to ensure the legal compliance for the media outlets or individual journalists operating across several member states. While in one EU Member State they may be exempted from the requirements to comply with some of the data protection rules, in other Member State such an exemption will apply. The same is valid from the data subjects' perspective – if the same piece of information is published across outlets operating in different Member States, the individuals would have considerable difficulty understanding media obligations with respect to protection of their personal data.

But this is not only a question of legal certainty. Given the current state of the rule of law in Europe, such a broad margin of appreciation may also serve as a leeway for less democratic regimes to swing the balance in favor of extremely broad interpretation of the right to data protection, by creating barriers for the public watchdogs to operate. For example, if not exempted from Chapter III of the GDPR on the rights and freedoms of data subjects, the investigative journalists could be placed under the obligation to inform those they investigate about the ongoing investigation and grant them the right to access their data. A failure to do so would result in the million-euro fines – even if not imposed, the harshness of potential punishment may in itself create a "chilling effect", thereby discouraging the journalists, especially those not belonging to the institutional media outlets, from undertaking investigations into the ruling majority.

THE BOUNDARIES OF A "JOURNALISTIC EXEMPTION"

To better understand Article 85 of the GDPR, it should be read along with a corresponding Recital 153 of the GDPR. The latter requires the Member States "to take account of the importance of the right to freedom of expression in every democratic society" and "to interpret notions relating to that freedom, such as journalism, broadly"[69]. Arguably, these statements come across as rather vague. Although the recitals are not meant to have and do not have any autonomous legal effect, they are particularly valuable as interpretative tools in the EU legal order and providing guidance when it comes to the implementation of the operative provisions[70]. For this reason, it would have been valuable to have more extensive guidance included in the text of the law.

In fairness to the GDPR drafters, Recital 121 in the Commission's proposal for the GDPR, included important clarifications as to the scope of the provision:

> (...) In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly. Member States should classify activities as "journalistic" for the purpose of the exemptions and derogations to be laid down under this Regulation if the object of these activities is the disclosure to the public of information, opinions or ideas, irrespective of the me-

[65] Recital 7 of the GDPR.

[69] Recital 153 of the GDPR.

[70] Baratta R., Complexity of EU law in the domestic implementing process, 19th quality of legislation seminar, 'EU Legislative Drafting: Views from those applying EU law in the Member States', 3 July 2014, https://ec.europa.eu/dgs/legal_service/seminars/20140703_baratta_speech.pdf, p. 9.

> dium which is used to transmit them. They should not be limited to media undertakings and may be undertaken for profit-making or for non-profit making purposes[71].

However, following the trialogues, the last two sentences were removed from the corresponding Recital 153, which merely states that the notions related to freedom of expression, including journalism, should be interpreted broadly. This, of course, does not mean that the omitted text is wrong but rather indicates that, at that particular point in time, the agreement between the stakeholders has not been reached on it.

To understand the scope of the "journalistic exemption" embedded in Article 85 (read together with Recital 153), three questions have to be answered:

1. Who can rely on the exemption or, in other words, what is its personal scope;
2. What activities are exempted or what is the material scope;
3. Which rules do not apply as a result of the exemption or the nature of the derogations.

Personal scope or who can rely on the exemption

The national implementation of Article 85 varies (for the overview of implementation in the selected EU Member States, see Annex I of this paper) and the first notable point of departure is the definition of the personal scope of the exemption's application.

In the majority of the analysed jurisdictions, the national data protection law refrains from defining precisely who can benefit from the exemption[72]. In this respect, Austria appears to be an outlier as it reserves the exemption exclusively to "media undertakings, media services and their employees". Reportedly:

> (t)he original version of the DPA 2018 had outlined the role of media undertakings, media services and their employees, but treated them like everyone else exercising their right to freedom of expression and information. The special treatment was inserted by the Amendment. Interestingly, even data secrecy does not apply to employees of media undertakings and media services – it did apply in the original version of the DPA 2018[73].

Such a narrow approach to the personal scope can be criticized from the EU law perspective. For instance, in Buivids case[74], the CJEU has adopted a functional approach to the notion of "journalism", essentially saying that even if the person is not recognized as a journalist under the national law, he or she can still benefit from the exemption, provided that the sole purpose of the data processing is the disclosure of information, opinion or comments to the public. In Buivids case, the Court accepted that Mr Buivids, who was not a journalist or otherwise related to media, could potentially rely on the exemption for the video he recorded and posted on Youtube of him making a statement in a Latvian police

[71] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM/2012/011, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52012PC0011.

[72] Other sectoral national laws could provide such a definition, but this question was not in scope of the current analysis.

[73] Cullagh K. et al, National adaptations of the GDPR, Luxembourg: Blogdroiteuropéen, 17 February 2019, p. 5.

[74] CJEU, Sergejs Buivids v. Datu valsts inspekcija, C–345/17, 14 February 2019.

station with the alleged aim to expose police malpractice.

In Markkinapörssi and Satamedia cases[75], the CJEU ruled that tax data collection and dissemination activities, even undertaken by a non-media organization for profit-making purposes[76] could also be considered "journalistic", provided that their aim was to disclose to the public information, opinions or ideas. Even more, in Google Spain case[77], the Court put forward an idea that essentially any publisher of a webpage with information about an individual could, depending on the purposes of the publication, legitimately fall within the scope of "journalistic purposes". At the same time, the Court was very specific to explicitly state that operators of the search engines, such as Google, cannot rely on this derogation.

Thus, at least from the standpoint of the EU law, the personal scope of the exemption is broad and could include essentially any individual or undertaking, whether professionally affiliated with the journalistic community or not, to the extent that they process personal data to disclose information, opinion or comments to the public, even if this implies providing for-profit services. The only type of service providers explicitly excluded from the scope are operators of the search engines[78]. Therefore, any national laws a priori limiting the application of Article 85 to the professional journalists or media outlets may be considered at odds with the EU law.

At the same time, such an approach, endorsed by the CJEU, appears to capture almost any publication available, including those produced by social media "influencers", data registers, employers publishing employee data on the company websites, and alike. As this is unlikely to have been the intention of the Court[79] or the legislator, the question then turns to the material scope of the exemption, i.e. determination which activities are considered to be carried out for "journalistic purposes".

Material scope or what activities are exempted

Similarly to the personal scope of the derogation, it's material scope has not been thoroughly fleshed out in the national law of the EU Member States. Majority of the analyzed national laws repeated the wording Article 85 of the GDPR, without including any additional explanation. However, Romanian and the UK laws in this respect deserve a closer look.

The Romanian data protection law comes across as particularly restrictive as it includes only three alternative scenarios in which personal data can be processed for journalistic purposes without having to comply with the GDPR[80]:

- if it concerns personal data which was clearly made public by the data subject;
- if the personal data is tightly connected to the data subject's quality as a public person;
- if the personal data is tightly connected

[75] CJEU, Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy, C-73/07, 16 December 2008.

[76] According to the Court, "[E]very undertaking will seek to generate a profit from its activities. A degree of commercial success may even be essential to professional journalistic activity. . ." (bid., para. 59).

[77] CJEU, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, C-131/12, 13 May 2014, para. 81.

[78] So far, only Google search engine was considered by the Court.

[79] As a matter of fact, in Buivids case, the CJEU has said that "the view cannot be taken that all information published on the internet, involving personal data, comes under the concept of 'journalistic activities" (CJEU, Sergejs Buivids v. Datu valsts inspekcija, C–345/17, 14 February 2019, para. 58).

[80] The whole GDPR, except for the Sanctions chapter, is excluded from the application (The Association for Technology and Internet (ApTI), Complaint to the European Commission on the infringement of the EU law, https://www.apti.ro/sites/default/files/Complaint%20on%20Romanian%20implementation%20of%20the%20GDPR%20-%20ApTI.pdf,p.3).

> to the public character of the acts in which the data subject is involved.

Many cases of investigative journalism would not precisely fit any of the three scenarios, as they may include many non-public actors and substantive amount of non-public information. At the same time, the first scenario – personal data which was made clearly public – seems to be stripped of any protection under in Romania, which, in the context of the GDPR as a whole (and Article 9(2)(e) in particular) could not have been the regulator's intention.

In contrast, the UK Data Protection Act 2018[81] offers a more nuanced take on the boundaries of the exemption, suggesting that some of the GDPR provisions would not apply to data processing where three cumulative conditions are met[82]:

- the data in question must be being processed with a view to the publication of journalistic material,
- the data controller must reasonably believe that, having regard in particular to the special importance of the public interest in freedom of expression, publication would be in the public interest, and
- the data controller must reasonably believe that the application of the listed GDPR provision would be incompatible with its journalistic purpose.

The UK ICO advises to consider the second condition – "public interest" – on case-to-case basis taking into consider existing codes of conduct[83] and balancing the public interest in the subject-matter with the level of intrusion into the private life of an individual.

It is not surprising to see "public interest" included as one of the criteria as it features prominently in the jurisprudence of the ECtHR (see the section "Approaches to balancing competing rights"). Although the ECtHR refrained from providing a definition of the "public interest", it recognized this notion to cover the public, political and historic debate, issues related to the politicians, behavior of the public servants, large corporations, governments, crime-related matters. However, other, less apparent matters may also be considered as meeting public or general interest. As explained by the Court:

> An initial essential criterion is the contribution made by photos or articles in the press to a debate of general interest. The definition of what constitutes a subject of general interest will depend on the circumstances of the case. The Court nevertheless considers it useful to point out that it has recognised the existence of such an interest not only where the publication concerned political issues or crimes, but also where it concerned sporting issues or performing artists[84].

This is essentially similar to the CJEU position in Buivids case, where the Court held that processing of personal data may be considered to be for "journalistic purposes" if "the video in question was published on an internet site to draw to the

[81] The UK Data Protection Act 2018, Schedule 2, Part 5, para 26, http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/part/5/enacted.

[82] Cain N. And Cowper-Coles, R., GDPR and the Data Protection Act 2018 – how do they impact publishers?, 25May 2018, https://www.rpc.co.uk/perspectives/data-and-privacy/gdpr-and-the-data-protection-act-2018/.

[83] Also see Schedule 2, Part 5, paras 26(4)-(6) of the UK Data Protection Act 2018.

[84] ECtHR, Von Hannover v. Germany (No. 2), App Nos. 40660/08 and 60641/08, 7 February 2012, para. 109.

attention of society alleged police malpractice". Importantly, the Court did not find it important whether, at the end of the day, such malpractice was established, as long as the author genuinely believe that it had taken place[85].

However, not all publications fall within the scope of public or general interest. According to the ECtHR, the matters which are simply meant to satisfy the curiosity of the readers and serve no real interest, do not deserve special protection. For instance, the publication of the photos of Caroline, Princess of Hanover, involving her daily life activities, in the tabloid press were found not to serve any legitimate interest of the public[86]. The ECtHR was also sceptical about the publication of taxation data on 1.2 million persons by a Finnish magazine. According to the Court, there was no public interest in the bulk dissemination of such raw data by the newspapers, in unaltered form and without any analytical input. The information on taxation might have enabled curious members of the public to categorise individuals according to their economic status and satisfy the public's thirst for information about the private lives of others. This could not be regarded as contributing to a debate of public interest[87].

As to the last criteria advanced by the UK ICO, it requires the data controller to identify "a clear argument that the provision in question presents an obstacle to responsible journalism" and is impossible to comply with[88].

From the theoretical perspective, the UK approach seems to be aligned with the ECtHR and CJEU jurisprudence and overall appears to be more balanced then, e.g. Romanian data protection law. The issues may arise when it comes to its practical application. Firstly, the media undertaking, a journalist or essentially anyone who would like to rely on the exemption would need to establish the public interest of the intended publication, and, secondly, to understand which data protection obligations would, in that case, conflict with the journalistic purposes. Perhaps, when it comes to a journalistic investigation into the governmental corruption a refusal to disclose information source could be easily defended, however, other, less black and white scenarios (e.g., breach notifications), may create compliance conundrums. At the same time, it is difficult to conceive that, e.g. a citizen journalist would a prior carry out such a balancing exercise. Unless more detailed guidance, codes of practices or conduct are provided, such a nuanced approach is at risk of remaining largely theoretical and non-operational.

Notably, on the 15 November 2019, the Bulgarian Constitutional Court has found Article 25z of the Bulgarian Personal Data Protection Act 2019 to be unconstitutional[89]. This national law provision was essentially meant to define the material scope of the exemption, by establishing ten criteria for balancing freedom of expression and a right to personal data. The criteria were as follows[90]:

1. The nature of personal data.
2. The impact of personal data's (public)

[85] CJEU, Sergejs Buivids v. Datu valsts inspekcija, C–345/17, 14 February 2019, paras 60-61.

[86] ECtHR, Von Hannover v. Germany, App No 59320/00, 24 June 2004, para. 76.

[87] ECtHR, Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, App no 931/13, 21 July 2015.

[88] The UK Information Commissioner's Office, Data protection and journalism: a guide for the Media, 2014, https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf, p.35.

[89] Constitutional Court of the Republic of Bulgaria, Decision No 8, 15 November 2019, http://constcourt.bg/bg/Acts/GetHtmlContent/865e35ff-b1b2-4a3c-8c50-449a4d887bf1.

[90] The criteria are not reproduced entirely verbatim. For the original wording, please consult the Bulgarian Personal Data Protection Act 2019, Article 25z(1) and (2), https://www.cpdp.bg/userfiles/file/ZZLD/ZZLD_26_02_2019.pdf.

disclosure on the rights and freedoms of the data subject.

3. The circumstances in which the data became known to the data controller.

4. The nature and characteristics of the statement through which (freedom of journalistic expression is exercised).

5. The importance of personal data's (public) disclosure for the matters of the public interest.

6. The role of the data subject in the public life or his position as a public person under applicable national laws related to anti-corruption and anti-money-laundering.

7. The data subject's contribution towards the disclosure of personal data or information about his private and family life

8. The purpose, content, form and consequences of the statement through which (freedom of journalistic expression is exercised).

9. Whether the statement through which (freedom of journalistic expression is exercised) is in line with the fundamental or human rights.

10. Other circumstances relevant for the case.

Where, based on the outcome of the application of these criteria, the processing was considered to be carried out for "journalistic purposes", the data controller was exempted from certain GDPR rules (e.g., lawfulness of process, international data transfer rules, etc.)[91], which would otherwise apply to him.

The Bulgarian Constitutional Court has noted that the Directive and the Regulation have not established similar non-exhaustive lists of mandatory criteria for balancing fundamental rights, and neither has the EU legislator explicitly instructed the national authorities to establish them. According to the Court, such a list amounts to a state interference with freedom of (journalistic) expression and is contrary to the case-law of the ECtHR and the CJEU which requires a balancing act to be carried out on case-by-case basis whenever there is a real conflict between the two rights. The Court further criticized the vague and ambiguous wording of individual criteria (e.g., a "nature of personal data"), which, collectively, lead to "self-censorship" of the media and journalists. The Court was particularly critical about the fact that by introducing these "unnecessary" (according to the Court) criteria the legislative arm defined the legal restrictions of the constitutional rights – something that is considered to be a prerogative of the judiciary– which amounted "to a step towards the establishment of a hierarchical order of fundamental rights". In the Court opinions, the current jurisprudence already outlined all the necessary means to reconcile the fundamental rights, while the measures which could be legitimately pursued should be related to strengthening of self-regulation by the media organizations, through the adoption of the codes of conduct also envisioned in the GDPR. The Court concluded that:

> Due to the fact that Article 25z, paragraph 2 of the PDPA introduces unclear criteria, it creates unpredictability, legal uncertainty and

[91] Ibid., Article 25z(3) and (4).

> disproportionate restrictions to the right to freedom of expression and information, in the context of a journalistic expression, in light of the aim pursued, the Constitutional Court finds this provision to be unconstitutional on the grounds of its contradiction to Article 4 paragraph 1 of the Constitution[92].

The decision of the Bulgarian Constitutional Court invalidated the ten criteria for balancing the freedom of expression and the right to data protection, which means that in Bulgaria, for a time being, only a general rule under Article 25(1) will apply establishing the need to balance competing rights, and any potential conflicts will be resolved on case-by-case basis. The Court seemed to look particularly unfavorably at the initiative to establish by law, a priori, any set of criteria which could help the media organizations to determine whether or not the expression falls within the material scope of a "journalistic exemption". Applying the logic of the judgment, the criteria established in the Romanian or the UK laws could be criticized on the same grounds, however, it is not a given that all the courts across the EU will necessarily share the views of the Bulgarian highest court.

Nature of derogations or what rules do not apply

Where the speech falls within both personal and material scope of "journalistic purposes", the application of the "journalistic exemption" does not immediately mean that the whole Regulation seizes to data processing in question. It is up for each Member State to determine the scope of the derogations, necessary to reconcile protection of personal data with freedom of expression. The GDPR allows establishing derogations in all or any of these areas:

- principles (lawfulness, transparency, purpose limitation, etc.);
- rights of the data subject (right to access, right to be forgotten, etc.);
- controller and processor obligations (appointment of the data protection officer, carrying out data processing agreements, notifying about data breaches, etc.);
- transfer of personal data to third countries or international organisations (concluding standard contractual clauses, relying on consent to transfer data to non-adequate jurisdictions, etc.);
- independent supervisory authorities (tasks and powers of the supervisory authorities, etc.);
- cooperation and consistency (powers of the European data protection board, etc.);
- specific data-processing situations (data processing for employment purposes, etc.);

In fact, the only Chapters of the GDPR which cannot be derogated from is Chapter I on general provisions such as definitions and scope of the law, Chapter VIII on remedies, liability and penalties (imposition of fines, remedies of the data subjects, judicial oversight, etc.), and Chapters X-XI on administrative provisions. Thus, at least in

[92] IAuthor's translation. For the original wording see the decision of the Constitutional Court referenced above. Article 4 paragraph 1 of the Bulgarian Constitution reads as follows: (1) The Republic of Bulgaria shall be a State governed by the rule of law. It shall be governed by the Constitution and the laws of the country. The Constitution of the Republic of Bulgaria, https://www.parliament.bg/en/const.

theory, almost all key GDPR rules could seize to apply to those who process data for "journalistic purposes".

Again, there are considerable differences in how the Member States approached this. Some (such as Austria and the Netherlands) decided to fully exempt[93] those exercising their freedom of speech for journalistic purpose from the national data protection law, meaning that such laws would not apply to them in their entirety. Others have taken a more granular approach and enumerated specific provisions which will seize to apply, meaning that all the other rules and obligations will continue applying. Further examines approaches of the Member States to the selected obligations under the GDPR.

As evidenced from the Table 3. below and Annex I, there is really no uniformity across the Member States as to which exactly GDPR obligations apply or do not apply to the processing undertaken for "journalistic purposes".

TABLE 3

The scope of the "Journalistic exemption" under the national law of the selected Member States

GDPR Article	Explanation of the Article	Sweden	United Kingdom	Lithuania	Romania
Article 5(1)(f)	Principle of integrity and confidentiality, which means that a data controller (e.g., a media undertaking) must put in place technical and organizational measures to ensure that the personal data it processes is protection from unauthorized disclosure, accidental loss, damage,etc.	Partially exempted[94] ***	Not exempted**	Not exempted	Exempted
Article 6	Lawfulness of processing, which means that each processing operation can only be considered lawful if a data controller can identify a lawful basis for it (consent, contract, public interest, etc.).	Exempted*	Exempted	Not exempted	Exempted
Articles 12-23	Rights of data subjects, meaning that the data controller should provide individuals with information about processing and respond to their requests.	Exempted	Partially exempted[95]	Exempted	Exempted
Article 28	Processor, which means that where a media undertaking outsources data processing to another entity (e.g., a data centre or a data analytics company), they must have a data processing agreement in place with it.	Exempted	Not exempted	Not exempted	Exempted

* **Not exempted** – the controller (a media undertaking, a journalist or another person processing personal data for "journalistic purposes") **has to comply with the rule** the content of which is explained in the second column.

** **Exempted** – the controller (a media undertaking, a journalist or another person processing personal data for "journalistic purposes") **does not have to comply with the rule** the content of which is explained in the second column.

*** **Partially exempted** – the controller (a media undertaking, a journalist or another person processing personal data for "journalistic purposes") **has to comply only with the certain aspects of the rule** the content of which is explained in the second column and in the relevant footnote.

[93] Note that even if the processing is exempted from compliance with the data protection law, it is subjected to other legislation and self-regulation, including codes of conduct for journalists.

[94] Article 32 of the GDPR on the security of processing continues applying.

[95] Exempted for all rights, except for the ones related to automated individual decision-making including profiling (Articles 21 and 22 of the GDPR).

While some of the approaches are understandable (exempting controllers from providing collected data to the data subjects), others are surprising. For instance, it is unclear why some of the Member States would decide to exempt the media undertakings or journalists from an obligation to ensure the security of personal data. The rationale behind the "journalistic exemption" is to reconcile freedom of expression and data protection where there is a tension between two rights –ensuring that the data is stored securely and protected against unauthorized disclosure does not really speak to such tension, as this is both in the interest of the media entities as well as the data subjects.

Blurring boundaries and grey zones

When it comes to the application of the "journalistic exemption", the ultimate criteria of whether or not data processing should be exempted from all or some of the GDPR rules is the purpose of processing. As a rule of thumb, if the personal data is collected, analyzed and published to satisfy the public interest ("journalistic purposes"), it is likely that these processing operations (data collection, analysis and publication) will not have to comply with some or all GDPR articles. Conversely, this means that if personal data is collected, analyzed or otherwise processed for other reasons, the GDPR will apply in full.

A natural question which arises is what these "other reasons" are and how integral to the news making the process the data processing operation should be to be considered as carried out for "journalistic purposes").

The Guidelines on safeguarding privacy in the media issued by the Council of Europe Committee on Media and Information Society and the Consultative Committee of Convention offer such a wording:

> The "media exemption" is necessary but is strictly limited to the editorial and journalistic content. This exemption does not apply to the other activities of media outlets, for instance when they process personal data for commercial or administrative purposes[96].

The national law in the Member States summarized in Annex I does not really give a clear answer as to what is considered "necessary" and "limited to the editorial content", but national practices offer some guidance. For example, as explained by the Information Commissioner's Office (UK ICO), the UK data protection authority, "journalistic purposes" should be interpreted as applying to the background information collected, used, created and retained as part of journalistic day-to-day activities in preparation to the story, even if all the information would not be published in the final piece[97]. The same authority, however, states that information created in response to a complaint about a particular story after publication is unlikely to be processed with a view to publication[98] and thus would not fall within the exemption.

One may also assume that data processing activities carried out for administrative reasons, such as HR management and financial management of the media organization, will unlikely meet the requirement of the "public interest" and thus will have to comply with the GDPR in full. In 1997, the European regulators suggested that "processing

[96] Council of Europe Committee on Media and Information Society and the Consultative Committee of Convention, Guidelines on safeguarding privacy in the media, June 2018, https://rm.coe.int/guidelines-on-safeguarding-privacy-in-the-media-additions-after-adopti/16808d05a0, p. 34.

[97] The UK Information Commissioner's Office, Data protection and journalism: a guide for the Media, 2014, https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf, p. 31.

[98] The UK Information Commissioner's Office, Data protection and journalism: a guide for the Media, 2014, https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf, p. 32.

of subscriber's data for billing purposes or processing for Direct Marketing purposes (including the processing of data on media use for profiling purposes) fall under the ordinary data protection regime", meaning that the journalistic exemption does not apply here[99].

Apart from these relatively clear-cut scenarios, there is an issue of data re-purposing or using the same personal data for multiple purposes, especially in the social media context. Assuming that a journalistic exemption could apply to personal data in the political news piece published on the website of a media outlet, it is not clear whether, under the current regime, it will also extend to its further publications on e.g. outlet's social media website. Strictly speaking, processing of personal data of both the persons mentioned in the news piece as well as the social media users is not strictly necessary for "journalistic purposes". At the same time, it is clear that to reach its intended audience, the news organization needs to disseminate the information via the contemporary mediums. We are, however, looking at the situation where the personal data within the same publication will be processed for both journalistic and, potentially, non-journalistic purposes.

Another case to consider is data sharing with the law enforcement organizations post-publication. Again, such processing does not strictly fit within the boundaries of the "journalistic exemption", as discussed in the preceding sections. It may thus create a scenario where "the media potentially faced losing the protection of the exemption if they assisted the police in connection with a criminal investigation"[100].

This also is likely to be a case for the non-media entities, such as think-tanks or public interest organizations, undertaking their own investigations and publishing media articles, often exposing pressing social concerns. As explained by the UK ICO:

> (...) the focus here is on what the specific information in question is being used for, rather than the purposes of the organisation as a whole. The exemption can still apply if the particular data is collected and used with the exclusive aim of disseminating some information, opinions or ideas to the public. However, if it is also used for the organisation's other purposes – eg in political lobbying or in fundraising campaigns – the exemption will not apply[101].

Overall, in reality, the scope of the "journalistic exemption" is much narrower as it may seem on its face. In the course of its usual activities, an average media organization will be processing personal data for both journalistic and non-journalistic purposes, and, depending on the jurisdiction, it is looking at a fair share of legal conundrums to address before understanding to what extent GDPR provisions apply to what data processing.

[99] Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Data protection law and media, Recommendation 1/97, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1997/wp1_en.pdf, p. 8.

[100] Cain N. And Cowper-Coles, R., GDPR and the Data Protection Act 2018 – how do they impact publishers?, 25 May 2018, https://www.rpc.co.uk/perspectives/data-and-privacy/gdpr-and-the-data-protection-act-2018/.

[101] The UK Information Commissioner's Office, Data protection and journalism: a guide for the Media, 2014, https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf, p. 31.

CONCLUSIONS AND RECOMMENDATIONS

1. In principle, any EU/EEA entity or person who collects, analyzes, uses, shares, publishes, stores and otherwise processing personal data has to comply with the European data protection law, with the centrepiece of such law being the General Data Protection Regulation (GDPR). This general obligation applies to media entities, journalists, non-profit organizations, and the rest.

2. In the jurisprudence of the European Court of Human Rights, the media play an essential role in the exercise of freedom of expression. They serve as a "public watchdog" whose task is to control the conduct of public authorities, disseminate information on political issues and on other areas of public interest. If the persons demonstrate that they were acting in their journalistic capacity, according to the ECtHR, they should benefit from additional protection afforded to media under Article 10.

3. The primary aim of the "journalistic exemption" under the European data protection law is to address the tension between freedom of speech and a right to data protection and to codify the general need to balance these two fundamental rights.

4. The "journalistic exemption" is embedded in Article 85 of the GDPR, and largely follows the wording of Article 9 of the Data Protection Directive (a predecessor of the GDPR). It essentially creates a possibility for the Member States to exempt those who exercise their freedom of speech for "journalistic purposes" from specific GDPR rules and obligations, meaning that they would not need to comply with these rules. However, the boundaries of the exemption are not clearly outlined in the GDPR and are left to be defined by the Member States.

5. There are fundamental differences in how the Member States approach the definition and scope of the "journalistic exemption" across three dimensions:

5.a. Personal scope. In the majority of the analysed jurisdictions, the national data protection law refrains from defining precisely who can benefit from the exemption. In this respect, Austria appears to be an outlier as it reserves the exemption to "media undertakings, media services and their employees". The latter position is at odds with the CJEU jurisprudence which essentially considers that the exemption can be relied on by any individual or undertaking, whether professionally affiliated with the journalistic community or not, to the extent they process personal data to disclose information, opinion or comments to the public, even if this implies providing for-profit services.

5.b. Material scope. Majority of the analysed national laws repeat the wording Article 85 of the GDPR, without including any additional explanation. However, the Romanian data protection law comes across as particularly restrictive as it includes only three alternative scenarios in which personal data can be processed for journalistic purposes. Conversely, the UK data protection law offers a more nuanced approach which centres

around the question of whether the publication is being produced in the "public interest". While the latter position is largely aligned with the decisions of the CJEU and the ECtHR, the Bulgarian Constitutional Court has recently found a legislative practice of establishing criteria for balancing freedom of expression and a right to data protection, unconstitutional.

5.c. Nature of derogations. Here, the differences across the Member States are the most considerable. As an example, some of the analysed laws provide exemptions from the rules related to the security of personal data and breach notification, others apply these provisions in full to the processing undertaken for "journalistic purposes".

6. Such diverging approaches to the scope of the exemption create legal compliance challenges for those exercising freedom of expression, data subjects and, ultimately, are at odds with the primary goal of the GDPR - the establishment of "more coherent data protection framework in the Union". .

7. The inherent risk of leaving the "journalistic exemption" for the national authorities to regulate is that given the current state of the rule of law in Europe, such a broad margin of appreciation may also serve as a leeway for less democratic regimes to swing the balance in favour of extremely broad interpretation of the right to data protection, by creating barriers for the public watchdogs to operate.

To address the challenges identified above, the following actions could be considered:

A. The Member States should act conscientiously to ensure that the national laws are revised to effectively balance data protection with journalistic freedom of expression by providing for more clarity as to the scope of the journalistic exemption across three dimensions outlined above. The legislative proposals should be informed by an extensive consultations with the key stakeholders.

B. The European Data Protection Board (EDPB) should revisit the Opinion on the data protection and media, issued by its predecessor – the Working Party 29 – in 1997. The EDPB should issue guidelines on the scope and application of Article 85 of the GDPR, in order to provide the Member States, the national supervisory authorities, as well as the data controller and data processors, clear guidance and best practices on the consistent and effective implementation of this provision.

C. Meanwhile, the national supervisory authorities should adopt clear guidelines on the wording and application of the national provisions implementing Article 85 of the GDPR. These guidelines should be adopted following a consultation with the key stakeholders and should be supported by dedicated training and awareness-raising activities. A good practice example of such effort is the UK Information Commissioner's Office call for views on a data protection and journalism code of practice[102].

[102] See https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-call-for-views-on-a-data-protection-and-journalism-code-of-practice/.

D. Under Article 97(1) of the GDPR, the Commission is tasked with the evaluation and review of the GDPR. The first report is due to be submitted to the European Parliament and to the Council on 25 May 2020. The interest groups, including the journalist associations, think tanks, freedom of speech and privacy non-profit organizations and other stakeholders should actively participate in the GDPR review by bringing to the Commission's attention practical issues related to the implementation of "journalistic exemption" and jointly proposing solutions to address the ongoing challenges.

E. Organizations processing data for, inter alia, journalistic purposes, should take active steps to understand its processes, data sets and purposes they process the data for. They should then distinguish between processing operations carried for journalist purposes and where "journalistic exemption" may apply and those which have to comply with the GDPR in full. This process and decision-making involved therein should be documented and promoted through the dedicated organizational measures (policies, procedures, training) across the entity. In particularly contentious cases, where it is not entirely clear if or to what extent the "journalistic exemption" applies to data processing, an audit trail should be kept in order to explain the data protection considerations, as well as the consultation from the lead supervisory authority, should be sought.

F. Associations of journalists or media organizations could consider making use of Article 40 of the GDPR and drawing up national or pan-European codes of conduct which are voluntary accountability tools, enabling the sector to resolve key data protection challenges pertaining to the scope of the "journalistic exemption". Such code(s) will be reviewed by the data protection authorities, providing assurance to the sector that the rules outlined in the code area appropriate. If adopted, such code(s) could potentially reduce compliance burdens and allow the sector to address its needs collectively, as opposed to each entity having to create its own solution to a global problem. ■

ANNEX I. AN OVERVIEW OF ARTICLE 85 IMPLEMENTATION IN THE SELECTED EU MEMBER STATES[103]

COUNTRY	IMPLEMENTATION
Austria[104]	Section 9 of the Data Protection Act 2018 exempts processing of personal data through media undertakings, media services and their employees for journalistic purposes from the scope of the GDPR and the DPA 2018.
Sweden[105]	The Data Protection Act contains states that "(n)either the GDPR nor this Act shall apply so far that they will infringe upon the Freedom of the Press Act or the Freedom of expression Act." The Act exempts processing of personal data for journalistic purposes and the purposes of academic, artistic or literary expression from having to comply with the following GDPR provisions: • Articles 5-30 • Articles 35-50 • Chapters 2 and 5 of the Data Protection Act
The Netherlands[106]	The Netherlands has chosen to provide a specific provision in the Implementation Bill, Article 43, which is similar to a provision that existed under the Dutch Data Protection Act. The provision states that the GDPR Implementation Act does not apply to exclusive journalistic purposes. At the request of the Senate, the Government confirmed this will include the preparatory work a journalist needs to do before a publication. Also, it was confirmed this is considered to be a broad exception, in order to allow the free press to do their work
Belgium[107]	Under the Belgian Framework Law of 30 July 2018, the notion of journalistic activities is defined broadly and includes all sorts of

[103] Please note that the information summarized in the table has been collected from both primary and secondary sources, as indicated in the footnotes. Where information has been collected from the secondary source, please consult the primary source before re-using the information.

[104] Cullagh K. et al, National adaptations of the GDPR, Luxembourg: Blogdroiteuropéen, 17 February 2019, https://blogdroiteuropeen.files.wordpress.com/2019/02/national-adaptations-of-the-gdpr-final-version-27-february-1.pdf .

[105] Ibid.

[106] Ibid.

[107] Drechsler L., The GDPR and Journalism. Protecting Privacy or a Break on Democratic Accountability? , 18 September 2018, https://brusselsprivacyhub.eu/publications/ws21.html.

	writings, video, investigations or blogging. It does not matter whether the person claiming the exception for journalistic purposes is a certified or registered journalist. However, every one undertaking journalistic activities is then obliged to follow the Belgian deontological rules for journalists and is under the jurisdiction of the Belgian Council for journalists. Once it is established that there is a journalistic activity (or processing for journalistic purposes in data protection terms), many rules of the GDPR become inapplicable, as for example nearly all data subject rights though the obligation to respond to a data subject rights request to use a data subject right remains. This means journalists relying on the exception will have to explain to the data subject why he or she cannot use their rights. The proof of journalistic activity has to be established by the party wanting to rely on the exception. The exceptions to the GDPR granted to journalistic purposes by Belgian law, do not exclude the application of all GDPR rules. Main principles, such as that processing needs to be lawful, fair and transparent will still apply. All penalties introduced by the GDPR also remain applicable.
The United Kingdom[108]	Schedule 2, Part 5, para 26 of the UK Data Protection Act 2018 lists GDPR provisions which do not apply if the three cumulative conditions are met:[109] • the data in question must be being processed with a view to the publication of journalistic material, • the data controller must reasonably believe that having regard in particular to the special importance of the public interest in freedom of expression, publication would be in the public interest, and • the data controller must reasonably believe that the application of the listed GDPR provision would be incompatible with its journalistic purpose. Where these conditions are met (and it is for the controller to explain how they are met) the exemption from these obligations can be lawfully relied on.[110]

[108] The UK Data Protection Act 2018, Schedule 2, Part 5, para 26, http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/part/5/enacted.

[109] Cain N. And Cowper-Coles, R., GDPR and the Data Protection Act 2018 – how do they impact publishers?, 25 May 2018, https://www.rpc.co.uk/perspectives/data-and-privacy/gdpr-and-the-data-protection-act-2018/.

[110] The UK Information Commissioner's Office, Data protection and journalism: a guide for the Media, 2014, https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf, p. 31.

	• all the principles, except the security and accountability principles; • the lawful bases; • the conditions for consent; • children's consent; • the conditions for processing special categories of personal data and data about criminal convictions and offences; • processing not requiring identification; • the right to be informed; • all the other individual rights, except rights related to automated individual decision-making including profiling; • the communication of personal data breaches to individuals; • consultation with the ICO for high-risk processing; • international transfers of personal data; and • cooperation and consistency between supervisory authorities.
Lithuania[111]	According to Article 4 of the Law on Legal Protection of Personal Data, the following provisions of the GDPR do not apply in their entirety when personal data is processed for journalistic purposes and the purposes of academic, artistic or literary expression: • Article 8 (child's consent), • Articles 12-23 (rights of data subjects),[112] • Article 25 (data protection by design and by default), • Article 30 (records of processing activities), • Articles 33-39 (breach notifications, DPIA and DPO), • Articles 41-50 (monitoring of code of conduct, certification and international transfers), • Articles 88-91 (processing in the employment context, for the purposes of public interest, obligation of secrecy and data protection rules of churches) The definition of "journalistic purposes" is not provided in the Law. In practice, the Courts interpret it based on the definitions of "public

[111] The UK Data Protection Act 2018, Schedule 2, Part 5, para 26, http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/part/5/enacted.

[112] Cain N. And Cowper-Coles, R., GDPR and the Data Protection Act 2018 – how do they impact publishers?, 25 May 2018, https://www.rpc.co.uk/perspectives/data-and-privacy/gdpr-and-the-data-protection-act-2018/.

	information" and "public information outlet" provided for in the Law on the Public's Information.[113]
Romania[114]	Article 7 of the Romanian Law no. 190/2018 includes three alternative scenarios in which personal data can be processed for journalistic purposes without having to comply with the GDPR provisions enumerated in Article 85 of the Regulation: • if it concerns personal data which was clearly made public by the data subject; • if the personal data is tightly connected to the data subject's quality as a public person; • if the personal data is tightly connected to the public character of the acts in which the data subject is involved.

ANNEX II. CŒ GUIDELINES ON SAFEGUARDING PRIVACY IN THE MEDIA (EXCERPTS)

In June 2018, the Council of Europe Committee on Media and Information Society and the Consultative Committee of Convention 108 jointly approved Guidelines on safeguarding privacy in the media (Guidelines). These Guidelines are largely based on the case-law of the European Court of Human Rights and aim to be an instrument of practical advice to journalists. They do not introduce new standards and will be open for feedback, updates and additions.

The excerpts below are limited to the Section 7 of the Guidelines entitled "Data Protection Principles". This section is reproduced below in full[115].

7 DATA PROTECTION PRINCIPLES

7.1 The rights of individuals

a.

Media outlets will need to comply with their obligations, under the Constitution and under the Convention, to ensure the privacy of individuals.

Moreover, under Article 9 of Convention 108, derogations from basic data protection principles may be allowed, for instance to ensure the freedom of expression, only when such derogations are provided for by the law of the Party to the Convention, and constitute necessary measures in a democratic society in the interests of protecting the data subject or the rights and freedoms of others.

Journalists will then need to assess, on a case by case basis, if they are allowed to derogate to the basic data protection principles in specific circumstances.

As a result, data protection key principles may to some extent apply also to media processing personal data for their journalistic activities.

[113] Vilnius district administrative court, decided on 2 April 2019, Case No EI-1485-821/2019, https://eteismai.lt/byla/36176409154589/eI-1485-821/2019.

[114] Privacy International et al., Data protection law is not a tool to undermine freedom of the media, 21 November 2018, https://privacyinternational.org/advocacy-briefing/2455/data-protection-law-not-tool-undermine-freedom-media.

[115] See https://rm.coe.int/guidelines-on-safeguarding-privacy-in-the-media-additions-after-adopti/16808d05a0.

Concerning the rights of the individual, under Article 8 of Convention 108, individuals have the right (where no derogations under Article 9 apply) to:

- establish the existence of an automated personal data file, its main purposes, as well as the identity and usual residence or principal place of business of the controller of the file;
- obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him/her of such data in an intelligible form;
- obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic data protection principles;
- have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure is not complied with.

Under the new European Union's legislative framework, with the General Data Protection Regulation, the rights of the individuals will even be strengthened and individuals will receive more comprehensive information at the time of the collection and will have, for instance, the right to have information erased ("right to be forgotten"), the right to the portability of their personal data, etc.

Derogations to these rights are allowed only if they are provided for by the law of the Party and constitute a necessary measure in a democratic society in the interests of protecting the data subject or the rights and freedoms of others.

b.

In general, and subject to the requirements of national law, individuals have the right to obtain information about the data stored by the responsible media outlet.

Such request may be declined if the disclosure of the information would impair the journalistic activities (revelation of the sources, of an undergoing investigation, etc.), would infringe the rights of third parties or would affect in a disproportionate manner the freedom of expression.

Procedures to handle access request should be adopted by media outlets. In case of refusal to comply with a request, the media outlets should record the reasons of this decision and communicate them to the person concerned.

c.

Published news or assertions, which subsequently turn out to be incorrect, should be promptly rectified in an appropriate manner by the editor.

The correction publishing the true facts should refer to the incorrect article. The true facts should be published even if the error has been admitted in another form. In the case of online publication, the rectification should be linked to the original content. If the publication is made within the original publication itself, it should be marked as such.

The correction, retraction or refutation should be stored together with the original publication and

for the same period of time.

Media should have procedures to ensure the exercise of the right to reply and the right to obtain rectification of false information after publication, which are even more crucial in cases where the rights of access and to rectification have been limited prior to the publication (Cf. Article 29 Working Party, Recommendation 1/97, "Data protection law and the media", 25 February 1997).

d.

Personal data gathered in violation of the rights of the persons concerned should be blocked in the first place and eventually deleted by the editor.

e.

Every person should be entitled to bring a complaint and to have an effective remedy in case of violation of their right to data protection, having been informed about their rights so that remedies are efficient in practice and do not remain purely theoretical.

The persons concerned should be able to address their complaints directly to the reporting media, to a self-regulatory body and eventually to the data protection authority or the courts.

They should also be entitled to a proper compensation proportionate to the violation and its consequences.

In Avram and others v. Moldova the applicants, five women, complained about the broadcasting on national television on 10 May 2003 of intimate video footage of them in a sauna with five men, four of whom were police officers. The footage was used in a programme about corruption in journalism, and notably in the newspaper Accente. The Court noted that the interference with the applicant' right to privacy was not in dispute. It had been acknowledged by the national courts and the applicants awarded compensation. In its ruling, the Court considered that the amounts awarded at national level had been too low to be proportionate to such a serious interference with the applicants' right to respect for their private life as was a broadcast of intimate video footage of them on national television. The Court took into account the dramatic effect on the applicants' private, family and social lives and awarded an additional compensation.

7.2 Security measures

Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss, as well as against unauthorised access, alteration or dissemination.

Media outlets should take appropriate and reasonable steps to store personal data securely and prevent them from being purposely or by negligence stolen, lost or misused. They should protect the technical devices (strong password policy, log-on controls, encryption, suitable back-up, antivirus and firewall, etc.) used inside and outside the organisation (USB, smartphones, laptops, etc.).

Media should at the same time adopt physical security measures and policies (locks, alarms, limited access to the facilities, etc.). Management and organisational measures should be adopted, for instance to regulate the relations with processors and subcontractors, to define a limited number of persons who will be able to access personal data or to organise a strict separation of journalistic and non-editorial activities.

7.3 Processing of non-editorial content

a.

The scope of the data protection legislation is extremely wide and media should keep in mind that data protection principles are fully applicable concerning the noneditorial content.

The "media exemption" is necessary but is strictly limited to the editorial and journalistic content. This exemption does not apply to the other activities of media outlets, for instance when they process personal data for commercial or administrative purposes.

In the latter case, media outlets should be considered as "traditional" data controllers and fully comply with data protection requirements.

For instance, media should fully apply data protection principles when they process personal data about their subscribers (for instance for advertising purposes) or about their employees. When processing personal data, the press should thus establish a clear distinction between editorial and commercial or administrative purposes.

b.

Personal data collected for non-editorial purposes shall be only processed if there is a legal ground for the processing. Principles of data protection shall be respected at any time. The existence of legal ground for data processing is a precondition for the legitimacy of the processing itself.

Along with the existence of legal ground for data processing, media outlets shall take into account the following data processing principles:

- data must be processed fairly and lawfully, without impinging on the dignity of a data subject;
- data may be processed only for specific, clearly defined and legitimate purposes. Further processing of data for purposes that are incompatible with the original purpose shall be inadmissible;
- data may be processed only to the extent necessary to achieve the respective legitimate purpose. The data must be adequate and proportionate to the purpose for which it is processed;
- data must be valid, accurate, and kept up to date, if necessary. Data collected without legal ground and irrelevant to the processing purpose must be blocked, deleted or destroyed;
- data may be kept only for the period necessary to achieve the purpose of data processing. After achievement of purpose it must be blocked, deleted or destroyed, or stored in a form that excludes identification of a person, unless otherwise determined by Law.

All data protection principles shall be considered simultaneously.

7.4 Best practices to ensure and demonstrate compliance

As a matter of good practice, media outlets should take all the necessary measures to ensure compliance with data protection requirements and demonstrate this compliance.

One may mention for instance the usefulness of the following "accountability" tools:

- appointment of a data protection officer;
- establishment of a register of data protection processing activities;
- elaboration of a privacy policy;
- internal procedures to consider the data protection implications at key stages of a journalistic activity and to adopt swift decisions in cases of ethical difficulties;
- internal procedures to draft information notices, to handle complaints of individuals, to alert the management of the organisation, to contact the data protection authority, to deal with cases of security breaches, etc.;
- elaboration of a privacy impact assessment in case of risks for the individuals;
- regular audits to verify and ensure compliance;
- review the contracts and relations with processors and subcontractors;
- basic data protection and privacy training for journalists and for the staff members;
- awareness raising activities (clear information for the individuals, dedicated data protection and privacy page on the website or on the intranet; etc.). The relevant "accountability tools" may be adapted to the size and resources of the media outlets.

ANNEX III. SUMMARY IN LITHUANIAN

Asmens duomenų tvarkymo išimtys žurnalistikoje: nacionaliniai sprendimai Europos Sąjungos masto dilemai*

Natalija Bitiukova**
2019 m. lapkričio 24 d.

Lapkričio 15 d. Bulgarijos Konstitucinis Teismas priėmė istorinį sprendimą byloje dėl saviraiškos laisvės žurnalistikoje ribų. Teismas pripažino Bulgarijos duomenų apsaugos įstatymo nuostatą, numatačią dešimt kriterijų, kuriais turi būti vadovaujamasi sprendžiant, ar konkreti publikacija yra parengta „žurnalistikos tikslais" ir dėl to jai neturi būti taikomos tam tikros duomenų apsaugos taisyklės, prieštaraujančia Bulgarijos Respublikos Konstitucijai.

Konstitucinis Teismas nurodė, kad „neaiškūs ir dviprasmiški" a priori kriterijai, numatyti nacionaliniame teisės akte, prieštarauja Europos žmogaus teisių teismo ir Europos Sąjungos Teisingumo Teismo suformuotai jurisprudencijai, reikalaujančiai kiekvienu atveju atskirai spręsti konfliktus tarp asmens duomenų apsaugos ir žodžio laisvės, pasitelkiant teismų praktikoje nustatytus vertybių balansavimo testus. Bulgarijos duomenų apsaugos įstatyme įtvirtintas teisinis reguliavimas, anot Teismo, gali vesti prie žiniasklaidos savicenzūros, yra neproporcingas, nekonkretus bei prieštaraujantis teisės viršenybės principui, įtvirtintam Bulgarijos Konstitucijoje.

Sprendimo priešistorė ir iš BDAR kylantys reikalavimai

Bulgarijos Konstitucinio Teismo sprendimas yra pirmasis išsamus Europos Sąjungos valstybių narių konstitucinio lygio teismo paskelbtas išaiškinimas dėl to, kaip duomenų apsaugos taisyklės turėtų būti taikomos žurnalistams ir kitiems, skleidžiantiems informaciją „žurnalistikos tikslais".

Nors teisiškai bylą inicijavo Bulgarijos parlamento narių grupė, faktiškai diskusijos šalyje prasidėjo dar 2019 m. pradžioje, po to, kai parlamentas, neorganizavęs klausymų, priėmė Bulgarijos duomenų apsaugos įstatymo pakeitimo paketą, kuriuo ir buvo įtvirtinti minėti dešimt kriterijų.

Anot įstatymų leidžiamosios valdžios, šiais pakeitimais buvo siekiama įgyvendinti Bendrojo duomenų apsaugos reglamento (BDAR) 85-ąjį straipsnį, reiklalaujantį ES valstybes nares suderinti „duomenų apsaugą pagal šį reglamentą (...) su teise į saviraiškos ir informacijos laisvę, įskaitant duomenų tvarkymą žurnalistikos tikslais“. Tuo tikslu BDAR rengėjai leido valstybėms narėms, kai tai yra būtina, netaikyti žiniasklaidos priemonėms tam tikrų BDAR reikalavimų, pvz. susijusių su tvarkymo teisėtumo pagrindimu, atsakymu į duomenų subjektų užklausas ir prašymus, duomenų perdavimo į trečiąsias valstybes apribojimais ir pan. Kokios konkrečiai duomenų apsaugos taisyklės nebūtų taikomos ir kokiais atvejais ši išimtis galiotų, buvo palikta nuspręsti pačioms valstybėms narėms, nepateikiant konkrečių gairių.

Minėtu pakeitimu Bulgarijos parlamentas numatė dešimt kriterijų (publikacijos turinys, asmens duomenų pobūdis, asmens duomenų atskeidimo poveikis individų teisėms ir laisvėms, asmens duomenų gavimo aplinkybės ir kt.), kuriais būtų vadovaujamasi sprendžiant, ar publikacija yra parengta žurnalistikos tikslais. Jeigu sprendimas yra teigiamas, duomenų valdytojas (pvz., žiniasklaidos priemonė ar individualus žurnalistas) būtų atleidžiamas nuo pareigos laikytis aukščiau minėtų BDAR nuostatų, tvarkant asmens duomenis publikacijos rengimo konkteste.

Šis pakeitimas nebuvo palankiai sutiktas Bulgarijos žurnalistų bendruomenės, o Bulgarijos nevyriausybinė organizacija „Prieigos prie informacijos programa“ įvertino minėtus kriterijus kaip „subjektyvius” ir „darančius nepagrįstą spaudimą žurnalistams”. Savo išplatintame pranešime organizacija kvietė panaikinti visus kriterijus, paliekant įstatyme bendrą principą, teigiantį, kad asmens duomenų tvarkymas žurnalistikos tikslais yra teisėtas, kai juo yra siekiama įgyvendinti žodžio ir informacijos laisvę, gerbiant teisę į privatumą.

Problema išspręsta ar tik atidėta?

Bulgarijos Konstituciniam teismu pripažinus teisės akto nuostatą, įtvirtinančią dešimt minėtų kriterijų, prieštaraujačia Konstitucijai, de facto buvo įgyvendintas Bulgarijos nevyriausybinės organizacijos pasiūlymas. Nors iš konstitucinės teisės perspektyvos toks sprendimas atrodytų logiškas, iš praktinės pusės esminiai klausimai liko neatsakyti:

- Ką reiškia duomenų tvarkymas „žurnalistikos tikslais“?
- Kokiais atvejais, tvarkant asmens duomenis „žurnalistikos tikslais“, nėra taikomos duomenų apsaugos taiksyklės?

Bulgarijos Konstitucinis teismas savo sprendime neskyrė daug dėmesio atsakymui į pirmąjį klausimą, tuo tarpu atsakymo į antrąjį pasiūlė ieškoti kiekvienu atveju atskirai, kilus konkrečiam konfliktui tarp teisės į saviraiškos laisvę ir teisės į asmens duomenų apsaugą. Toks požiūris nėra unikalus Bulgarijai. Pavyzdžiui, Lietuvos Asmens duomenų teisinės apsaugos įstatyme irgi yra tik lakoniškai nurodyta, kad BDAR galioja ne visa apimtimi, kuomet asmens duomenys yra tvarkomi „žurnalistikos (...) tikslais”. Kol kas dar negausioje teismų praktikoje ši sąvoka yra interpretuojama atsižvelgiant į „visuomenės informavimo“ ir „visuomenės informavimo priemonės“ apibrėžimus, įtvirtintus Visuomenės informavimo įstatyme. Panašus reguliavimas yra Austrijoje, Švedijoje, Olandijoje ir Belgijoje.

Visgi tarp ES valstybių narių galima rasti ir tokių, kurios, kaip Bulgarija, savo nacionaliniuose teisės

aktuose siekė sukonkretinti BDAR nuostatą ir dėl to juose numatė sąlygas, kurioms esant „žurnalistiniais tikslais“ platinamai informacijai nebūtų taikomos duomenų apsaugos taisyklės. Iš tokių valstybių galima išskirti Rumuniją, kurios duomenų apsaugos akte numatytos sąlygos yra ypač siauros ir dėl to jau sulaukė kritikos, ir galbūt taps Europos Komisijos tyrimo objektu. Tuo tarpu istoriškai labiausiai nusistovėjusios sąlygos yra numatytos Jungtinės Karalystės Duomenų apsaugos įstatyme (į 2018 m. įstatymo versiją jos iš esmės buvo perkeltos iš 1998 m. įstatymo):

- Asmens duomenys turi būti tvarkomi žurnalistinės medžiagos paskelbimo tikslu,
- Duomenų valdytojas turi pagrįstai manyti, kad žurnalistine publikacija būtų siekiama patenkinti viešąjį interesą,
- Duomenų valdytojas turi pagrįstai manyti, kad BDAR nuostatų taikymas neleis pasiekti žurnalistinių tikslų.

Esant šioms trims sąlygoms, žiniasklaidos priemonė neturi pareigos laikytis kai kurių BDAR nuostatų. Jungtinės Karalystės duomenų apsaugos priežiūros institucija yra parengusi išsamias gaires dėl šių kriterijų taikymo. Šias gaires ji planuoja greitu metu atnaujinti, pasikonsultavusi su žurnalistų bendruomene ir kitais suinteresuotais asmenimis.

Kaip matyti, nors ir esant tam pačiam tikslui – įgyvendinti BDAR, taikomo vienodai visoms valstybėms narėms, 85-ajį straipsnį, – priemonės, kurias kiekviena valstybė parinko, yra pakankamai skirtingos. Viena grupė pasirinko teisiškai jokių kriterijų nenumatyti ir palikti tai, kas yra ir kas nėra „žurnalistikos veikla“ vertinimus a posteriori, greičiausiai tam metui, kai bus nagrinėjamas konkretus konfliktas tarp žurnalistų ir duomenų subjektų (nors, kaip parodė 2013 m. tyrimas, tokių konfliktų sprendimo procesas ir jo rezultatai yra ypač subjektyvūs).

Kita valstybių grupė nuėjo kiek kitokiu keliu, pasirinkdama savo teisinėje sistemoje įtvirtinti konkrečius kriterijus ir sąlygas, kuriems esant asmens duomenų tvarkymui nebūtų taikomos BDAR nuostatos. Nors pastarosios sistemos kritika jau buvo aptarta nagrinėjant Bulgarijos Konstitucinio Teismo sprendimą, panašiais pagrindais būtų galima kritikuoti ir pirmąją grupę – konkrečių apibrėžimų ir vertinamųjų kriterijų nebuvimas sukuria tokią pat neaiškumo situaciją ir palieka plačią erdvę subjektyviam vertinimui. Be to, atsižvelgiant į tai, kad duomenų tvarkymas pagal BDAR reikalauja proaktyvių, sistemingų ir kompleksiškų žingsnių, nėra iki galo aišku, kaip žiniasklaidos priemonė galės šiuos reikalavimus įgyvendinti, jeigu sprendimas dėl to, ar konkrečiu atveju jai bus ar nebus taikomos Reglamento nuostatos, faktiškai bus priimtas tik įvykus konfliktinei situacijai.

Išimties „žurnalistikos tikslais“ ribos ir paribiai

Kitas įdomus klausimas, kuris nebuvo aptartas Bulgarijos Konstitucinio teismo sprendime, yra BDAR išimčių ribos, t.y:

- Kokios konkrečiai duomenų apsaugos taisyklės nėra taikomos, kai duomenys yra tvarkomi „žurnalistikos tikslais“?

BDAR šiuo atveju numato tam tikrą taisyklių „meniu”, iš kurio valstybės narės gali pasirinkti, kurias taikyti duomenų tvarkymui „žurnalistikos tikslais“, o kurių ne. Šiuo atveju konsensusą tarp valstybių narių atrasti yra irgi sudėtinga.

Pavyzdžiui, žiniasklaidos priemonės, tvarkančios asmens duomenis „žurnalistikos tikslais“ galėtų potencialiai nesilaikyti įpareigojimo numatyti teisėtą duomenų tvarkymo pagrindą Bulgarijoje, Rumunijoje, Švedijoje ir Jungtinėje Karalystėje, tuo tarpu jis būtų pilna apimtimi taikomas Lietuvoje. Žiniasklaidos priemonės Bulgarijoje, Jungtinėje Karalystėje ir Lietuvoje turėtų įgyvendinti technines ir organizacines priemones duomenų

saugumui užtikrinti, tuo tarpu tai nebūtų privaloma žurnalistams Švedijoje ir Rumunijoje. Jeigu žiniasklaidos priemonė pasitelktų duomenų tvarkytoją tam tikriems veiksmams atlikti, ji turėtų su juo sudaryti sutartį ir užtikrinti kitų reikalavimų laikymąsi Bulgarijoje, Jungtinėje Karalystėje ir Lietuvoje, bet ne Švedijoje ar Rumunijoje.

Tokia skirtingų nacionalinių sprendimų mozaika iš esmės nesutampa su pamatiniu BDAR priėmimo tikslu, kuris pačiame Reglamente yra apibūdintas kaip „tvirtos ir geriau suderintos duomenų apsaugos sistemos, paremtos griežtu vykdymo užtikrinimu“ siekis, kuriuo „turėtų būti užtikrintas didesnis teisinis ir praktinis tikrumas fiziniams asmenims, ekonominės veiklos vykdytojams ir valdžios institucijoms“. Teisinis tikrumas ir vienodamas teisės taikymas ES yra ypač aktualus toms žiniasklaidos priemonėms ar žurnalistams, kurie vykdo veiklą keliose ES valstybėse narėse, o taip pat ir duomenų subjektams, siekiantiems pasinaudoti jiems BDAR suteiktomis teisėmis.

Europos Sąjungos lygio sprendimo beieškant

BDAR yra taikomas visiems juridiniams ir fiziniams asmenims vykdantiems profesinę veiklą ES teritorijoje, kai jie renka, saugo, analizuoja ar kitaip tvarko asmens duomenis. Reglamentas numato skirtingas taisykles, skirtas įgyvendinti pamatinius duomenų tvarkymo principus, tokius kaip duomenų tvarkymo teisėtumas, skaidrumas, duomenų kiekio mažinimas, duomenų saugumas ir kt.

Šios taisyklės gali būti netaikomos tik tais atvejais, kai BDAR aiškiai numato jų išimtis ir tos išimtys yra įgyvendinamos nacionalinėje teisėje, pavyzdžiui, išimtys gali būti skirtos duomenų tvarkymui archyvavimo, mokslinių ar istorinių tyrimų tikslais, o taip pat ir duomenų tvarkymui „žurnalistikos tikslais“. Imant žiniasklaidos priemonės kaip duomenų valdytojo pavyzdį, jai BDAR būtų visapusiškai taikomas tais atvejais, kai jos administracija ar darbuotojai tvarko asmens duomenis žmogiškųjų išteklių valdymo, finansiniais ar kitais administraciniais tikslais, tačiau tose srityse, kuriose duomenys yra tvarkomi „žurnalistikos tikslais“ (pvz. medžiagos, reikalingos publikacijai surinkimas, jos apibendrinimas, analizė, publikacijos viešinimas), BDAR nuostatos galėtų būti visiškai ar iš dalies netaikomos.

Nors iš pirmo žvilgsnio toks taisyklės ir išimties santykis atrodo pakankamai aiškus, taikant šią sistemą praktikoje, ir ypač tais atvejais, kai priemonė veikia keliose valstybėse narėse, kyla nemažai klausimų. Žinoma, vienas iš būdų geriau suprasti šios sistemos ribas ir paribius yra sulaukti, kol susiformuos daugiau ir įvairesnės priežiūros institucijų, nacionalinių teismų ir Liuksemburgo teismo praktikos. Kitas būdas yra įsitraukti į nuoseklios sistemos kūrimą ir užtikrinti efektyvesnį žiniasklaidos, interesų grupių ir priežiūros institucijų bendradabiavimą. Savo sprendime, Bulgarijos konstitucinis teismas rekomendavo susitelkti ties duomenų tvarkymo elgesio kodeksu, numatytų BDAR, kūrimu žiniasklaidos ir žurnalistinės veiklos srityje. Tai reikalautų aktyvių žingsnių tiek iš žurnalistų bendruomenės, tiek iš nacionalinės priežiūros institucjos.

Šiuo atveju svarbus vaidmuo tenka ir Europos duomenų apsaugos valdybai, kurioje dalyvauja visos nacionalinės priežiūros institucijos. Paskutinė ES lygio nuomonė žurnalistinės veiklos klausimu buvo publikuota 1997 m. ir nuo to laiko jokių gairių, ar tuo labiau 85 str. išaiškinimų, nebuvo paskelbta, nors Valdyba turi prerogatyvą tokias nuomones skelbti. Tikėtina, kad vienas rimčiausių pokyčių šioje srityje gali įvykti po to, kai Europos Komisija atliks periodinį BDAR nuostatų vertinimą ir pateiks šio vertinimo rezultatus Europos Parlamentui ir Tarybai (tai bus padaryta iki 2020 m. gegužės 25 d.). Ar šiame vertinime atsispindės aukščiau aptartos problemos ir kokie šių problemų sprendimai bus pasiūlyti, iš dalies

priklausys nuo žiniasklaidos ir kitų suinteresuotų grupių įsitraukimo į jau vykstantį vertinimo procesą.

* Šis straipnis yra parengtas 2019 m. autorės tyrimo „Journalistic exemption under the European data protection law" pagrindu. Tyrimas ir straipsnis buvo paremti Vilniaus politikos analizės instituto, Žiniasklaidos būklės tyrimų konkurso rėmuose.

** Natalija Bitiukova yra teisininkė, besispecializuojanti duomenų apsaugos srityje. Natalija yra Europos Tarybos duomenų apsaugos srities mokymų Lietuvos teisininkams lektorė ir bendravedėja, Europos Komisijos 2019 m. tyrimo apie skaitmeninę dezinformaciją bendraautorė, Žmogaus teisių stebėjimo instituto (ŽTSI) ir Vokietijoje įsikūrusios Pilietinių laisvių platformos valdybų narė. Prieš pradėdama darbą privačiame sektoriuje Natalija dirbo Europos Duomenų apsaugos priežiūros pareigūno (EDPS) būstinėje, o prieš tai ėjo ŽTSI direktoriaus pavaduotojos teisės klausimais pareigas. ■

ABOUT THE AUTHOR

Natalija Bitiukova is a data protection lawyer currently working in Denmark. She also serves on the boards of the Lithuania-based watchdog Human Rights Monitoring Institute (HRMI) and Berlin-based non-profit Civil Liberties Union for Europe. Natalija researches the implications of online manipulation and data misuse for democratic processes and has recently co-authored the study commissioned by the European Parliament (LIBE) on the impact of propaganda on the functioning of the rule of law in the EU. Before that, Natalija completed a traineeship with the European Data Protection Supervisor where she contributed to the Supervisor's Opinion on Online Manipulation and Personal Data and held a position of the Deputy Director of the Human Rights Monitoring Institute where she led legal work in the areas of digital rights, rule of law and criminal justice.

Vilnius
institute
for policy analysis

Vilnius Institute for Policy Analysis
Didžioji g. 5, LT-01128 Vilnius
Tel. +370 612 25727
info@vilniusinstitute.lt
www.vilniusinstitute.lt