PANELFIT

PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Handbook for Journalists

Authors: Iñigo de Miguel Beriain, Lorena Pérez Campillo (UPV/EHU)

Edition: Federico Caruso (OBC Transeuropa)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains This report is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

Table of Content

1. Introduction 4

2. The legal framework regarding freedom of expression and data protection in the EU arena 6

3. The "journalistic exemption" in the GDPR 7

3.1 Introduction and background 7

3.2 The personal scope of the exemption 11

3.3 Processing personal data: the material scope 12

3.4. The condition for the exemption 13

3.5 The material scope of the exception 16

3.6 Applicable regulation 17

4. GDPR applied to journalism 18

4.1 The GDPR in a nutshell 18

4.2 The legal bases for data processing 18

4.3 The special categories of data 19

4.4 The subject's rights and the controller's duties 20

4.5 The main concepts 22

5. The Principles applied to journalism 24

5.1 Introduction 24

5.2 Lawfulness, fairness and transparency 24

5.3 Choosing a legal basis for processing 26

5.4 Purpose limitation 28

5.5 Data minimisation 28

5.6 Accuracy 29

5.6 Storage limitation 30

5.7 Integrity and Confidentiality 30

5.8 Accountability 31

6. Additional issues 33

6.1 Subject access requests 33

6.2 Confidential sources 34

6.3 Minors and vulnerable population 35

6.4 Takeaway points 36

7. Q&As 38

8. Glossary (art. 4 GDPR) 43

Annex I. The balancing test 49

DOs and DON'Ts 53

Further Readings 55

Annex II. Comparative analysis of the regulatory framework at the EU Member states level 56

Austria 56

Belgium 56

Finland 56

France 57

Germany 57

Ireland 57

Italy. 58

The Netherlands 59

Spain 59

Sweden 59

United Kingdom 60

Information related to exemptions and derogations in a nutshell 61

Sources of information 62

Bibliography 62

Documents of the Council of Europe 63

Jurisprudence by the European Court of Human Rights 64

1. Introduction

The world of journalism is a very particular microcosm in terms of data protection. Even though it involves the collection and storage of huge amounts of personal information in the form of interviews, company records, photographs and films, and their dissemination, its regulatory framework has never been so clear. Thus, it is not surprising that when it comes to media activity there are serious concerns related to data protection (Erdos, 2015, p.8). Indeed, publishing information related to an identified or identifiable person might constitute a serious attempt against his or her privacy.

On the other hand, it is undeniable that the work of journalism is essential in building a well-formed public opinion. Indeed, members of the media are often considered to be public watchdogs with a vital role in a democratic society. They have a duty to disseminate information and inform the public regarding all matters of public interest, which the public also has a right to receive (Guidelines on Safeguarding Privacy in the Media, p.6). Thus, mass media have a duty to adequately report events that might be of public interest, even though this may put at risk the rights of some affected by their publication.

Therefore, there are two fundamental rights, freedom of expression and privacy, which sometimes collide. This raises an issue that can only be solved by their proper balancing in each concrete case. When does the right to the protection of personal data prevail against the right to freedom of expression and information and vice versa? This is a question that has already been explored in depth from a legal perspective. However, the approval of the 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 (General Data Protection Regulation, GDPR) and the reinforced protection of data protection rights are opening the gate to new debates. We believe that journalists and mass media organisations should be aware of this situation.

This Handbook is not aimed at focusing on theoretical aspects of this issue, but at providing information professionals – journalists, information editors, media directors,

etc. - with adequate mechanisms to ensure compliance with the minimum legal and ethical standards in terms of data protection, while ensuring an adequate exercise of their profession. Namely, this Handbook is focused on anyone working in a media organisation, since they could all benefit from the exemptions or derogations derived from article 85.2 of the GDPR.

The contents of this Handbook mix several different regulatory frameworks: on the one hand, the EU regulation, mainly the GDPR; on the other hand, the regulation by the Council of Europe through the European Convention of Human Rights and the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108). These sources are complemented by jurisprudence by the ECtHR and the EUCJ. As the Article 29 Working Party stated, "One important element that emerges from the current legislative situation in the Member States is that the media, or at least the press, are bound to respect certain rules which although not part of data protection legislation in a proper sense contribute to the protection of the privacy of individuals. Such legislation and the often rich case-law on the matter confer specific forms of redress which are sometimes considered a substitute for the lack of preventive remedies under data protection law" (A29WP, p. 7). Therefore, the guidance provided in this Handbook is intended to follow the regulation provided by all the institutions mentioned.

The Handbook is divided into several different parts. In its first sections, it exposes the legal framework about journalism and data protection issues in the EU arena. Sections four and five, instead, focus on how to deal with the main ethical issues that must be addressed by a journalist or a media organisation in the framework of the GDPR and the Council of Europe regulations. Finally, the annexes provide detailed information about the balancing test and the regulatory framework at the Member state level.

DISCLAIMER: This document is aimed at helping journalists deal with the data protection regulation. However, its contents do not constitute legal advice, are not intended to be a substitute for legal advice and should not be relied upon as such. You should seek legal advice or other professional advice in relation to any particular matters you or your organisation may have.

2. The legal framework regarding freedom of expression and data protection in the EU arena

The regulatory framework regarding the right to freedom of expression and the regime of data protection in Europe is mainly linked to the Council of Europe and the European Union legal systems. In the case of the Council of Europe, the regulation is twofold. On the one hand, the main rights at stake, right to freedom of expression and right to privacy, are part of the European Convention of Human Rights. Its article 10.1 states that "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". Quite obviously, this right might be limited according to the provisions made by number 2 of this clause. Article 8, instead, focuses on the defence of privacy, by stating that:

> "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 wellbeing 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".

On the other hand, the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108), also approved by the Council of Europe, regulates data protection issues. Indeed, at the present moment it 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, since it is only related to the European Convention of Human Rights.

In the EU context, the right to freedom of expression was included in article 10 of the EU Charter of Fundamental Rights, which reads:

> "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".

Instead, articles 7 and 8 of the Charter included the right to privacy and the right to the protection of personal data concerning him or her. At the present moment, the legal framework for data protection is mainly drawn by the Regulation (EU) 2016/679 of the GDPR. Alleged violations of the EU law are heard by the Court of Justice of the European Union (CJEU). There is no equivalent piece of overarching and comprehensive secondary legislation about free speech and media freedom mostly due to the Commission's position that the EU has no authority to legislate in this area (Biriukova, 6).

The GDPR applies whenever anyone processes (collects, retains, uses, or discloses, for instance) any information about a living person. As the ICO remarks, "it does not prevent responsible journalism, as the main principles are flexible enough to accommodate day-to-day journalistic practices (…) However, the media are not automatically exempt and will need to ensure they give some consideration to the data protection rights of individuals. Legal responsibility usually falls on the relevant media organization rather than individual employees, although freelance journalists are likely to have their own separate obligations". However, it is good to always keep in mind that employees of media organisations need to be aware of their legal responsibilities, particularly day to day adherence, when working for their employer.

3. The "journalistic exemption" in the GDPR

3.1 Introduction and background

The GDPR is the main legal tool regarding data protection issues at the EU level. It contains the general principles and rules that apply to all processing of personal data within the EU or involving EU citizens. Within its provisions, it is possible to find a

specific reference to the issues at stake. We are talking about the so-called "journalistic exemption", as stated by Article 85 of the GDPR, which is shown in the table below.

This clause was included in the GDPR as a solution to alleviate the tensions between freedom of expression and the right to data protection. Indeed, it was aimed at codifying the general need to balance these two fundamental rights. At a glance, it simply left in the hands of the Member States the possibility to exempt those who exercise their freedom of expression for "journalistic purposes" from specific GDPR rules and obligations (Biriukova, 14).

This journalistic exemption was not a novelty in the EU regulation. The article 9 of the Data Protection Directive of 1995, the predecessor of the GDPR, already included a similar provision, which brought some divergence in the regulation of this issue in the EU Member states. A Recommendation by the Article 29 Working Party[1] summarised the situation by dividing the Member states into three main groups:

> "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".

1 However, the Working Party also reported that "The differences between these three models should not however be overestimated. In most cases, independently of any express derogation that may exist, data protection legislation does not apply fully to the media because of the special constitutional status of the rules on freedom of expression and freedom of the press. These rules place a de facto limit on the application of substantive data protection provisions or at least their effective enforcement. On the other hand the ordinary data". See: 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, at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1997/wp1_en.pdf.

The GDPR only introduced minor changes in this scenario. As a matter of fact, article 85 of the GDPR provides a very broad framework for action to the Member States. They are to figure out the scope of the journalistic exemption and the circumstances in which it applies. However, for their regulatory developments to be valid, they must be aligned with the provisions of the GDPR and the European Convention of Human Rights (ECHR). Therefore, one must think about the rules to be followed in the journalistic environment from a double perspective. On the one hand, one must always keep in mind a series of rules that are embedded in the GDPR and/or the ECHR and the jurisprudence by the EUCJ and the ECtHR. These must be strictly followed in the practice of this profession. On the other hand, one must consider that there may be certain differences between Member states, depending on the particular regulatory framework. In any case, they should not be excessive since the principles and rules of the GDPR and the ECHR must always be respected.

Nevertheless, it is important to highlight that some Member states have not fully adhered to these standards. In Bulgaria, for instance, the Constitutional Court has recently declared the national approach towards the implementation of Article 85 unconstitutional. This was due to the inclusion of an article in the Personal Data Protection Act that set out 10 criteria for deciding whether journalists have complied with the balance between the right to information and that to personal data protection. The Court considered that such criteria were too vague and could create a risk of arbitrary interpretations, a circumstance that opened the way for the Commission for Data Protection to have unpredictable power to interpret it not necessarily in the public interest regarding pluralistic information about the policies and activities of government[2].

Furthermore, in Romania, the data protection regulator has been criticised for using the GDPR to silence the critical voices in the national media. In November 2018, a case was reported in Romania that might serve well to reflect the tension between data protection and freedom of speech. It was related to an article about a corruption scandal involving a politician and his close relationship to a company being investigated for fraud that was published on the Bucharest-based Rise Project Facebook page. Some

2 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/#:~:text=Bulgaria's%20Constitutional%20Court%20has%20ruled,that%20of%20personal%20data%20protection.

time after the publication, the Romanian data protection authority (ANSPDCP) sent a series of questions to the journalists who authored the article.

In theory, this was due to the necessity to ensure a balance between the right to the protection of personal data, freedom of expression and the right to information. The authority held that that Rise journalists had violated the GDPR by publishing the videos, photos, and documents – in essence, the private data of Romanian citizens – to support the reporters' allegations. The journalists were asked for information which could reveal the article's sources, under the advertisement that if they did not cooperate, they could have to face a penalty of up to 20 million Euros (Warner, 2019).

A group of twelve human rights and media organisations reacted to this request by sending an open letter to ANSPDCP that called for ANSPDCP to carefully analyse GDPR cases that might endanger freedom of expression. It also demanded an urgent and transparent mechanism to be put in place for assessing claims involving data processing operations for journalistic purposes. At the same time, sixteen digital rights NGOs sent a letter to the European Data Protection Board, with ANSPDCP and the European Commission in copy, asking for the GDPR not to be misused in order to threaten media freedom in Romania (Benezic, 2018). Later on, some MEPs in Brussels criticised the case against the Rise Project and disputed the Romanian interpretation of GDPR enforcement. Finally, all this led to warnings from the European Commission (Nielsen, 2018). However, at the present moment it is hard to know what might finally happen, since the case is currently ongoing.

There are, however, some other Member states that have taken the opposite way. For instance, Sweden considered that article 85 of the GDPR gave a larger space for exemptions to member States than the Data Protection Directive did, not least because it does not require that the processing shall be carried out "solely" for journalistic purposes (a wording that was included in the Directive). Moreover, the Swedish Government put forth that recital 153 of the GDPR states that the concept of freedom of expression has to be interpreted broadly. On this basis, the new Data Protection Act is including wider exemptions or derogations than the Personal Data Act of 1998 (McCullagh, 45).

3.2 The personal scope of the exemption

What does "journalistic purposes" mean? What does "journalism" mean? There is nothing similar to a definition of journalism in the Regulation, since it was removed from the first drafts of the GDPR[3]. Some of the Member states have created their own definitions. Most of them are quite open, with the main exception of Austria, which reserved the exemption exclusively to "media undertakings, media services and their employees" (Cullagh, 2019, p.5).

However, it seems quite clear that the GDPR opts for an open, inclusive meaning of the term, which might be applicable even though the national regulation does not reflect it. Indeed, in the Buivids case[4], the CJEU accepted that the journalist exception was applicable to a citizen who published a video recording on Youtube, proved that the object of the recording and publication thereof was the disclosure of information, opinions or ideas to the public. Similarly, in the Satamedia case[5] the CJEU ruled that data collection and dissemination activities could also be considered "journalistic", if their aim was to disclose to the public information, opinions or ideas, no matter the means employed. The fact that the controller was a non-media organisation for profit-making purposes was considered irrelevant to these purposes.

It is not clear what would happen if an Austrian organisation that could be considered as a media undertaking or a media service implements any of the derogations or exceptions provided by article 85. Somehow, this would create a conflict between the Austrian regulation and the GDPR, which explicitly begs for a broad extension of the concept of journalism. In our opinion, it is likely that the interpretation by the GDPR would prevail.

Keeping this in mind, it seems that a broad definition of journalism makes much more sense than a narrow one. Natalija Bitiukova has written that "journalism refers to the

3 Indeed, the draft read: "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 medium 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" (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).

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

5 CJEU, Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy, C-73/07, 16 December 2008

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" (Bitiukova, p.4). Her wording works perfectly well with the GDPR, in our opinion.

Journalism, thus, must be defined as an activity that covers all output on news, current affairs, consumer affairs or sports[6]. This is because the exemption covers information processed only for journalism. The concept can also include publisher and editors of Internet blogs or web pages since comments made on these platforms should be considered as a manifestation of their own freedom of expression. Of course, this does not mean that every blog or comment posted online will be journalism, since some bloggers simply intend to take part in common social interactions or other recreational Internet use. Moreover, search engines are expressly excluded from the concept and therefore, from the exception[7].

3.3 Processing personal data: the material scope

As shown, article 85 specifies that exemptions or derogations might be applicable to everyone who aims at disclosing to the public information, opinions or ideas. However, what type of data could be considered as such? Which personal data can be processed for journalistic purposes without having to comply with the GDPR? Again, there is not a simple answer to this question. In principle, Member states have a say on the material scope of the journalist exemption and their policies are not always the same. For instance, article 7 of the Romanian law no. 190/2018, which introduces derogations for the processing of personal data for journalistic purposes, offers only three alternative scenarios under which personal data can be processed for journalistic purposes[8]:

1) if it concerns personal data which were clearly made public by the data subject;

6 According to the ICO, "Taken together with art and literature, we consider it is likely to cover everything published in a newspaper or magazine, or broadcast on radio or television – in other words, the entire output of the print and broadcast media, with the exception of paid-for advertising (…) It would involve a wide range of activities, loosely grouped into production (including collecting, writing and verifying material), editorial, publication or broadcast, and management of standards (including staff training, management and supervision). In short, the exemption can potentially cover almost all information collected or created as part of the day to day output of the press and broadcast media, and comparable online news or current affairs outlets. However, advertising revenue, property management, financial debt, circulation, or public relations would not usually be considered as journalism" (ICO, 29).

7 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, par. 81

8 Complaint to the EU Commission by The Association for Technology and Internet (ApTI), 2018, at: https://www.apti.ro/sites/default/files/Complaint%20on%20Romanian%20implementation%20of%20the%20GDPR%20-%20ApTI.pdf

2) if the personal data were tightly connected to the data subject's quality as a public person; or

3) if the personal data are tightly connected to the public character of the acts in which the data subject is involved. If any of these three situations applies, the GDPR (except for the Sanctions chapter) is entirely excluded from application.

These three alternative scenarios are extremely limited compared to the current jurisprudence of both the European Court of Justice and the European Court of Human Rights. Both courts consider that there are several factors that need to be weighed in before an analysis, the most important ones being the contribution to a debate of public interest on the one hand and the damage to data subjects' private life on the other. Therefore, the Romanian law does not seem to perform an adequate reconciliation between the right to the protection of personal data and the right to freedom of expression and information.

The United Kingdom adopted a totally different approach. Its Data Protection Act 2018 considers that the journalist exception applies to personal data processing where three cumulative conditions are met:

- the data in question must be processed with a view to the publication of journalistic material,
- the data controller must reasonably believe that, with particular regard 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.

This approach seems much more in line with the regulatory framework.

3.4. The condition for the exemption

The exemptions or derogations foreseen by article 85 are only applicable "if they are necessary to reconcile the right to the protection of personal data with the freedom of

expression and information". When does this necessity apply? Recital 153 provides valuable insight to answer this question:

> *Member States law should reconcile the rules governing freedom of expression and information, including journalistic, academic, artistic and or literary expression with the right to the protection of personal data pursuant to this Regulation. The processing of personal data solely for journalistic purposes, or for the purposes of academic, artistic or literary expression should be subject to derogations or exemptions from certain provisions of this Regulation if necessary to reconcile the right to the protection of personal data with the right to freedom of expression and information, as enshrined in Article 11 of the Charter. This should apply in particular to the processing of personal data in the audiovisual field and in news archives and press libraries. Therefore, Member States should adopt legislative measures which lay down the exemptions and derogations necessary for the purpose of balancing those fundamental rights.*

Thus, the GDPR is willing to ensure an adequate balance between data protection and the right to freedom of expression and information, as enshrined in Article 11 of the Charter[9]. This is why *derogations or exemptions from certain provisions of the GDPR* only apply *if necessary to reconcile the right to the protection of personal data with the right to freedom of expression and information*. This idea of balancing both rights has been endorsed by 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 such rights. The key point, however, is how to proceed to do so. The ICO states that in order to do this adequately, organisations should take into account:

- the general public interest in freedom of expression,
- any specific public interest in the subject matter,
- the level of intrusion into an individual's private life, including whether the story could be pursued and published in a less intrusive manner, and

9 Article 11. Freedom of expression and information

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.

- the potential harm that could be caused to individuals. Existing guidance set out in industry codes of practice can help organisations think about what is in the public interest[10].

In this context, the notion of public interest is particularly relevant, according to the jurisprudence by the Court of Justice of the EU or the European Court of Human Rights, as mentioned in cases such as Buivids[11] or Satakunnan v. Finland[12]. However, it is hard to define. Indeed, the ECtHR has historically refrained from providing a definition of "public interest". Nevertheless, it declared, in the context of the Von Hannover cases[13], that "an initial essential criterion is the contribution made by photos or articles in the press to a debate of general interest. Thus, it seems that this notion covers "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" (Biriukova, 21).

To sum up, there are some variables that shall be surely present in the definition of public interest, which must involve "an element of proportionality – it cannot be in the public interest to disproportionately or unthinkingly interfere with an individual's fundamental privacy and data protection rights. If the method of investigation or the details to be published are particularly intrusive or damaging to an individual, a stronger and more case-specific public interest argument will be required to justify that, over and above the general public interest in freedom of expression" (ICO, 33). Indeed, public interest cannot be reduced to the public's thirst for information about the private life of others or to the reader's wish for sensationalism or even voyeurism, like publishing details of the sexual activities of a public figure. If the sole aim of an article is to satisfy curiosity of the readership regarding details of a person's private life, it cannot be deemed to contribute to any debate of general interest to society (Guidelines on Safeguarding Privacy in the Media, 12). For instance, in the Standard Verlags GmbH v. Austria (No.2) case, it was judged that a newspaper had violated the privacy of the

10 ICO, p. 34

11 CJEU, Sergejs Buivids v. Datu valsts inspekcija, C–345/17, 14 February 2019, par. 60-61.

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

13 ECtHR, Von Hannover v. Germany (No. 2), App Nos. 40660/08 and 60641/08, 7 February 2012, par. 109.

persons concerned when it published an article commenting on rumours that the wife of the then Austrian President sought to divorce him and was maintaining close contacts with another politician. In the opinion of the Court, journalists can not report pointless gossip about politicians' marriages. The Guidelines on Safeguarding Privacy in the Media highlight that "in determining whether a person is a public figure, it is of little importance for journalists whether a certain person is actually known to the public. Journalists cannot be limited by the claims of concerned persons that they are not actually known to the public. What matters is whether the person has entered the public arena by participating in a public debate, by being active in a field of public concern or in public debate" (Guidelines on Safeguarding Privacy in the Media, 12-20). A set of examples of sentences produced by the ECtHR and gathered in the Guidelines has been incorporated in the next table (full references are included in the Sources of Information section at the end of this Handbook).

These considerations open the gate to a more extensive debate on how to balance public interest against the right to privacy. This will be analysed in the section of this Handbook devoted to legitimate interest as a legal ground for personal data processing.

3.5 The material scope of the exception

Article 85 draws a broad scope for the exceptions and derogations, since it mentions 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). Therefore, exceptions and derogations might cover *general principles, the rights of the data subject, the controller and the processor, the transfer of personal data to third countries or international organisations, the independent supervisory authorities, cooperation and consistency, and specific data-processing situations.*

However, it is essential to notice that this broad scope will not necessarily apply to all EU Member states. The clause explicitly states that Member states shall provide for exemptions or derogations, but it does not list those exceptions. It only declares that they *shall* by law reconcile the right to the protection of personal data pursuant with the

right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.

Therefore, the decision about the concrete measures to be adopted belongs to the Member states. They are supposed to develop such a regulatory framework and notify to the Commission the provisions adopted regarding exemptions or derogations and, without delay, any subsequent amendment law or amendment affecting them. At the present moment (November 2020), not all Member states have developed such a legal framework. In Annex II we included information about the regulation incorporated by EU Member states, including the data in which the modification was introduced. However, it might happen that some countries have changed their legal framework afterwards.

3.6 Applicable regulation

In general, journalists should try to avoid sending personal data outside the European Economic Area (EEA) without adequate protection. What counts as 'adequate protection' will depend "on the nature of the information, the purpose of the transfer and the legal position at the other end, among other things. This principle will not prevent online publication, even if this makes information available outside the EEA. If publication complies with the DPA in other respects (or is exempt as being in the public interest), it will be appropriate to publish it to the world at large" (ICO, 26).

What if journalists are based in a Member state but wish to publish contents in other countries or in the web space? The GDPR states that "where such exemptions or derogations differ from one Member State to another, the law of the Member State to which the controller is subject should apply". This might cause weird consequences. For instance, it seems that a publication by a Spanish-based publisher (or blogger) could benefit from relatively lax rules on privacy of "celebrities" there, even if the publication in question would be barred if published by a French publisher and even though the Spanish publication is easily (and online directly) accessible from France. Furthermore, they could even benefit from being based in Spain even if the publication was in French and directed at a French audience. This brief suggestion on applicable law is insufficient for the online environment. Unless this is more specifically addressed in the successor

to the e-Privacy Directive, it might make the legal environment for free speech very unclear, particularly in the online digital environment (EDRI, 51).

4. GDPR applied to journalism

4.1 The GDPR in a nutshell

The GDPR is intended to stimulate the creation of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons (Recital 2). It is aimed at guaranteeing an adequate balance between data protection and privacy and some other fundamental rights, such as freedom of speech, for instance.

The Regulation is mainly focused on the processing of personal data, that is, "any information about an identifiable living person which is (or will be) stored on a computer or other digital device, or filed in an organized filing system where it can be easily found" (ICO, 2). Therefore, it focuses on structured data that reveal information about a living person. Handwritten notes are not considered personal data, for example. However, if someone transfers those notes to a computer and organises them, they will become personal data.

Similarly, anonymised information is not personal data, but it should not be confused with pseudonymised information, that is, information that might be linked to a person (see the conceptualisation below). Information that refers to deceased people is not protected by the GDPR too, even though its publication may generate problems related to the right to honour or public image. On the other hand, the fact that a piece of data is public or private does not change its nature as personal data. It may, however, have consequences for the lawfulness of its processing.

4.2 The legal bases for data processing

In general, no personal data can be processed unless on a legal basis. Article 6 of the Regulation sets forth up to six legal grounds that legitimate processing, namely:

1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes
2. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
3. processing is necessary for compliance with a legal obligation to which the controller is subject
4. processing is necessary in order to protect the vital interests of the data subject or of another natural person
5. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
6. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

There are three legal bases for processing that usually apply for journalists. These are consent, public interest, and legitimate interest. They will be explored in detail in section 5.3.

4.3 The special categories of data

Some data are specially protected by the GDPR and journalists must be extremely careful if they are willing to process them. These special categories comprise: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

A controller can only process such data if he or she has a legal ground to proceed according to article 6 of the GDPR and any of the circumstances that alleviate the ban introduced to their processing by article 9.1 applies. The circumstances are listed in article 9.2 of the GDPR. In principle, explicit consent by the subject who provides the

information or public disclosure by the people with whom the information relates seem the most promising circumstances. Anyway, the controller must always consider that, since these types of data are particularly sensitive, he or she should only disclose them if a substantial public interest applies. In the following table you can find a compilation of the ECtHR provided by the Guidelines on Safeguarding Privacy in the Media, which gathers the jurisprudence by the ECtHR

Regarding this issue, the ICO has stated that "if the information is 'sensitive personal data' organisations must also meet one of the following conditions:

- the person has given their explicit consent
- the information has already been made public as a result of steps that a person has deliberately taken. It is not enough that it is already in the public domain – it must be the person concerned who took the steps which made it public" (ICO, 41).

4.4 The subject's rights and the controller's duties

Finally, it is essential to mention that the GDPR provides data subject with some essential rights that must be respected, unless derogations and exceptions are applicable. These include:

- the right to access. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and information regarding issues such as the purposes of the processing, the categories of personal data concerned, the recipients or categories of recipient to whom the personal data have been or will be disclosed, etc. (see article 15 of the GDPR).

- The right to rectification. The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the

data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

- Right to erasure ('right to be forgotten'). The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay when the circumstances listed in article 17 of the GDPR apply.

- Right to restriction of processing. The data subject shall have the right to obtain from the controller restriction of processing where the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data; or the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; or the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; or the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

- Right to data portability. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format.

Furthermore, there are two essential duties that the controller must take care of according to the GDPR:

- duty to provide the data subject with information no matter if collected from them or not. This includes information about the identity and the contact details of the controller and, where applicable, of the controller's representative, the contact details of the data protection officer, where applicable, the purposes of the processing for which the personal data are intended as well as the legal basis

for the processing, etc (see articles 13 and 14 of the GDPR)

- notification obligation regarding rectification or erasure of personal data or restriction of processing. The controller shall communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

4.5 The main concepts

There are several concepts that are particularly relevant in the context of the GDPR and journalists must be aware of their meaning. These are:

- 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

- 'pseudonymisation' means that the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational

measures to ensure that the personal data are not attributed to an identified or identifiable natural person,

- ‘filing system’ means any structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis,

- ‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for their nomination may be provided for by Union or Member State law,

- ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

- ‘recipient’ means a natural or legal person, public authority, agency or another body to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing

- ‘third party’ means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data

- ‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a

statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

5. The Principles applied to journalism

5.1 Introduction

This section aims to provide some concrete tips for journalists to deal with their day-to-day activities. It uses an easy to understand, plain language, that might be understood by a non-expert. It is structured on the grounds of the principles set by the GDPR. This is due to a simple fact: processing must always respect those principles, which are the core of the GDPR. This means that even though you have a legal ground to process personal data, you must respect these fundamental principles. Otherwise, your processing would not be lawful.

In the following pages, we show these principles and provide advice on how to deal with them from the perspective of a journalist. This advice incorporates the recommendations made by the Council of Europe in its Guidelines on Safeguarding Privacy in the Media approved jointly in June 2018 by the Steering Committee on Media and Information Society (CDMSI) and the Committee of Convention 108 (Council of Europe Data Protection Convention). These Guidelines comprise a collection of standards of the Council of Europe (the Council/CoE) and the European Court of Human Rights (the Court) concerning the protection of privacy of public figures and private individuals in the media. **Please, always keep in mind that this part of the Handbook mainly provides guidance on how to deal with the principles adopted by the GDPR from an ethical perspective. In order to ensure adequate legal compliance, you must follow the regulation produced by the corresponding Member state.**

5.2 Lawfulness, fairness and transparency

According to article 5.1 (a) of the GDPR, "Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject". This principle includes three different requirements.

- Lawfulness. Data processing is only lawful if a basis of legitimacy allows it (see section 3.1). Most of the information that a journalist collects is personal data. Thus, obtaining information often means data processing and, therefore, should follow the principles settled by the GDPR. This means that you need to have a legal basis to process the data and you need to justify the reasons why you collect them.

- Fairness. The concept of fairness is difficult to define. It refers to the fact that processing must be in accordance with the spirit of the GDPR, not only with its literacy. In this way, it allows for the introduction into the application of the RGPD of the provisions of other regulations of particular importance when it comes to defining what is considered as "fair" within the EU and its Member States, such as the EU Charter of Fundamental Rights. In general, however, one could state that fairness implies that you process the information in a way that satisfies the rational expectations of the data subjects. The ICO has stated that fairness means that “wherever possible the media should collect and use information about people fairly and lawfully, and not cause any unjustified harm. Journalists will often be able to collect information without the subject’s knowledge or consent, but it will be unfair to actively mislead people about the journalist’s identity or intentions” (ICO, 40).

- Transparency. The principle of transparency seeks to ensure that all interested parties are aware of each processing of their personal data and that they can access essential information about their specific content. In general, you should also tell the person you are collecting the information from, and the person the information is about (that is, the data subject), who you are, and what you are doing with their information. If they provide you with the information for a concrete aim, you should not use if for another aim. Sometimes, notifying data subjects about data processing could undermine the journalistic activity. Sometimes, you use intrusive covert methods to get a story, such as surveillance. All these circumstances might be acceptable, as long as you had no alternative more compliant with data protection principles and the story is of public interest. Indeed, this is the key point: you can avoid notifying the data subject

about the processing if and only in so far as it would make the exercise of journalism impossible. In other words, you must communicate the processing to the data subjects unless you consider that by doing so you would be unable to build the story. Once this no longer applies, you should proceed with the obligations settled by the GDPR. As the ICO stated, "in the context of journalism, we accept that it will not generally be practicable for journalists to make contact with everyone about whom they collect information. It will often be fair to collect information on matters of potential journalistic interest without the subject's knowledge. However, there will be cases where fairness may require some direct contact with the subject of a major investigation, to offer them the opportunity to put forward their side of the story" (ICO, 40).

5.3 Choosing a legal basis for processing

There are three legal bases for processing that usually apply for journalism. These are consent, public interest and legitimate interest.

Consent. Data can be processed if the people who are the subject of the information have given consent. If the information refers to several people, consent should be given by all of them. Consent must be freely given, specific and informed. We must highlight that the mere fact that someone has published personal data in a public site, such as his or her Facebook profile, does not mean that this data can be used without his or her consent or another legal basis. Consent must cover the purposes of the data processing. Therefore, if you want to use the data for a purpose other than the one originally sought by the data subject, you need a legal basis. There might be exceptions to this rule, especially if the data subject is a public figure but, in such circumstances, you should process the data under the legitimate interest basis, instead of consent. According to the Guidelines on Safeguarding Privacy in the Media, "journalists should, in principle, secure the consent of the person concerned at the time the picture is taken and not simply if and when it is published. Otherwise an essential attribute of personality (the image) is dependent on third parties and the person concerned has no control over it" (p. 20).

Public interest. Data can be processed if it is necessary for the performance of a task carried out in the public interest. Indeed, this is the most recommendable legal basis if

you are part of a public institution that is acting as such (if consent is not applicable). If you are a private actor or if you are a public institution that is working as a private actor, the legitimate interest basis is more recommendable. This is due to the fact that public interest cannot legitimate processing if we do not consider the interests of the data subject, since information is not an absolute right or duty. However, if this is the case, legitimate interest and balancing test are concepts that work very well with processing. Thus, it is recommendable to use legitimate interest as a legal basis for processing.

Legitimate interest. The processing is necessary for 'legitimate interests', provided that it will not cause unwarranted harm to the person concerned. "Legitimate interests will include a media organization's commercial and journalistic interests in gathering and publishing material, as well as the public interest in freedom of expression and the right to know". Thus, it is a wide legal basis that comprises public interest but not only public interest. In order to balance all interest involved, you should follow a procedure able to ensure that the legitimate interest serves as a legal basis processing includes three main phases (Detrekői):

- first, you must identify a legitimate interest test (why the story serves the public interest)
- second, you must perform a necessity test (how the publication of names and personal data is needed to make the article informative)
- finally, you need to carry out a balancing test aimed at demonstrating that the interest of the public to know about the topic covered in the story exceeds the individual's interest to keep their personal data hidden from the public eye. The greater the information value for the public, the more the interest of a person in being protected against the publication has to yield, and vice versa (Guidelines on Safeguarding Privacy in the Media, p.11).

An extensive description of a balancing test is included in Annex I of this document. The jurisprudence of the ECtHR is quite extensive on the balance between public interest and privacy (See Right to the protection of One's Image, at: https://www.echr.coe.int/documents/fs_own_image_eng.pdf). An excellent summary of its position was included in the Kaboğlu and Oran V. Turkey Case: "In several of its

judgments the Court has summarised the relevant criteria for balancing the right to respect for private life and the right to freedom of expression as follows: contribution to a public-interest debate, whether the person concerned is well-known, the subject of the report, the prior conduct of the person concerned, the content, form and consequences of the publication, as well as, if appropriate, the circumstances of the case (see *Von Hannover* (no.2) [GC], cited above, §§ 108-113, and *Axel Springer AG*, cited above, §§ 89-95; see also *Couderc and Hachette Filipacchi Associés*, cited above, § 93). If the two rights in question have been balanced in a manner consistent with the criteria established by the Court's case-law, the Court would require strong reasons to substitute its view for that of the domestic courts (see *Palomo Sánchez and Others v. Spain* [GC], nos. 28955/06, 28957/06, 28959/06 and 28964/06, § 57, ECHR 2011)".

5.4 Purpose limitation

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. By virtue of this, the data can only be processed for certain purposes, which must be explicitly stated when justifying the processing. Therefore, you should always keep in mind, for instance, that you cannot use the data that you keep in your records for purposes other than those that justified their processing, unless you have a basis that serves as a ground for the new processing.

5.5 Data minimisation

Personal data shall be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". This principle implies that "you must have enough information to do the job, but shouldn't have anything you really don't need. Note that this principle takes account of your purpose. As the nature of journalism requires the collection and cross-referencing of large volumes of information, we accept that information without immediate relevance to a current story can be justifiably retained for future use if it relates to a person or subject of more general journalistic interest" (ICO, 25).

5.6 Accuracy

According to article 5.1(d), "personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay".

Accuracy is both an essential principle of the GDPR and a key value of journalism. Therefore, journalists should pay special attention to ensure that the information published is accurate. For this purpose, you must check the facts. It can be argued that only accurate information works well with the idea of promoting public interest. Therefore, article 85 exemptions and derogations will only apply if the information is accurate. "However, the exemption may be available if, for example, the story is urgently in the public interest and the short deadline makes a complete accuracy check very difficult. As with any use of the exemption, you will still need to show that proper thought was given by someone at an appropriate level to what checks might be possible, whether publication could be delayed for further checks, the nature of the public interest at stake and that the decision to publish was, therefore, reasonable" (ICO, 14).

Furthermore, accuracy implies that very reasonable steps must be taken to ensure that personal data that are inaccurate are erased or rectified without delay. This is essential, since published information might seriously compromise someone's public image or private life. According to the Article 29 WP, "the right to reply and the possibility to have false information corrected, the professional obligations of journalists and the special self-regulatory procedures attached to them, together with the law protecting honour (criminal and civil provisions concerning libel) must be taken into consideration when evaluating how privacy is protected in relation to the media" (A29WP, p. 7).

Therefore, journalists must be particularly careful and change the information if it is shown not to faithfully reflect reality. This, of course, must be especially considered if the people requesting the rectification are the data subjects, in accordance with their right to rectification. Finally, you should always declare whether you are expressing an opinion or informing about a fact. This is crucial for the audience not to misinterpret the information.

5.6 Storage limitation

The principle of storage limitation means that data are "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed" (art. 5 GDPR). In the context of journalism, this means that, once you have your information, you have to make some decisions regarding whether you would like to storage it and for how long. Data are very valuable assets for journalist, since they could often serve as background materials. Contact details are also a very important resource and journalist usually wish to keep them. In principle, you can keep these data for long periods or indefinitely. The GDPR does not impose a time limit on how long you can retain personal data. The 'storage limitation' principle only imposes that there is a good reason to keep the data. Assuming this is the case, they can be kept indefinitely.

However, as the ICO states (ICO, 12), "you should review your retained information from time to time to ensure that the details are still up to date, relevant and not excessive for your needs, and you should delete any details which you no longer need (e.g. if a contact has changed their number). Furthermore, the way you retain the information or how you review it should be set out in organisational policies.

5.7 Integrity and Confidentiality

Data must be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures" (art. 5 GDPR). This principle is aimed at avoiding unauthorised or unlawful processing and accidental loss, destruction or damage of the data.

The data you are storing are sensitive material. Therefore, you must do your best to avoid their being lost, stolen or misused. Try to keep them safe by paying attention to the procedures and security protocols established by your organisation. Indeed, all employees of a media company should be aware of, and follow, the organisation's policies and procedures. Information should be locked, password protected and

encrypted where possible. You must be particularly aware of security when out of the office with documents, phones or laptops containing personal data.

The range of security needed is not set. In principle, security measures might be appropriate to ensure that no unlawful access happens or to avoid accidental loss, destruction or damage. Journalists should consider how sensitive or confidential the information they hold is, the harm that might result from its loss or improper use, the technology available, and the costs involved. They do not have to have state-of-the-art security, but it should fit the level of risk. Organisations need to consider technical (electronic) and physical security measures, policies and procedures, and staff training and supervision. These should cover staff working both in and outside of the office. In any case, organisations should be able to justify the level of security adopted (ICO, 43).

5.8 Accountability

According to article 5.2 of the GDPR, "The controller shall be responsible for, and be able to demonstrate compliance with paragraph 1". This clause rules that the data controller is not only responsible for compliance with the GDPR, but should also be able to demonstrate this compliance. Therefore, the controller carries the burden of proof for compliance with the GDPR. In the case of journalism, it might happen that, in fact, an exemption to the subject's rights has been implemented. In such cases, organisations or journalists should be able to explain why complying with the relevant provisions was not compatible with the purposes of journalism. To this purpose, they should often demonstrate that they have performed a balancing test, considering the different interest at stake. Stating that compliance is not standard industry practice would not be enough in any case. Keeping an audit trail in cases that are controversial or particularly likely to prove contentious could be an appropriate tool to demonstrate accountability.

As Biriukova stated, "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 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 priori 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" (Biriukova, 22).

We should also keep always in mind that, in general, the data controller is not an isolated journalist, but the organisation he or she works in. Therefore, the organisation is responsible for implementing organisational measures and policies about data processing and responsibility. Indeed, the organisation must be able to prove that the processing of the data was the final result of a decision-making process that considered all issues at stake. Procedures might vary considerably, depending on the type of organisation and information, but there should be a kind of structured procedure in each organisation. Furthermore, it would be good to develop some codes of conducts in the framework of the journalist profession in every Member state. Indeed, the Article 29 Working Party stated that "evaluating whether exemptions or derogations are proportionate, attention must be paid to the existing ethic and professional obligations of journalists as well as to the self regulatory forms of supervision provided by the profession" (A29WP, p.8).

As the ICO states, "in many day-to-day stories it may well be appropriate for the journalist to use his or her own judgement, but more high-profile, intrusive or damaging stories are likely to require more editorial involvement and a more formal consideration of the public interest. Organisational policies should be used to explain when greater editorial involvement is required. Our view is that it is the belief at the time of the processing that is important. The data controller must be able to demonstrate that it had a belief about the public interest, i.e. that the issue of public interest was actually considered. It should also be able to show that it was considered at the time of the relevant processing of personal data and not just after the event. If a journalist initially considers that a story will be in the public interest, but in the end the organisation decides not to publish it, the exemption can still cover all journalistic activities undertaken up to that point.

Secondly, the exemption only requires a reasonable belief. This gives much more leeway than other exemptions and reflects the importance of a free and independent media (ICO, 35). The following table shows some measures included in the Guidelines on Safeguarding Privacy in the Media that might serve well to organisations seeking to ensure compliance with data protection.

6. Additional issues

6.1 Subject access requests

Accessing the information stored by journalists can be very important, both for the subjects they cover and for other people. The former, however, have a right of access that others do not have. Article 85, however, allows Member States to limit that right. In this section we will introduce some considerations on how this limitation is usually formulated. In doing so, we will focus on both the right of access and the right not to disclose the sources of information, which are widely acknowledged in Europe.

According to article 15 of the GDPR, the data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and information regarding the purposes of the processing, the categories of data concerned, the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations, the envisaged period for which the personal data will be stored, etc.

On this basis, a journalist should provide the data subjects with the information that he or she holds about them, unless he or she considers that by doing so he or she would be unable to build the story. Under such circumstances the exceptions and derogations of article 85 would prevail against their right to access. Needless to say, this would only happen under the assumption that the story is of public interest. The higher the interest is, the stronger the right not to disclose the information to the data subject. Quite often, it might happen that you could provide access to some of the information about the processing or the personal data used without causing damage to the aims of your investigation. If this is the case, you should proceed without delay.

The denial to provide the information requested might perfectly be justified even after the story is published. If you have strong reasons to consider that this might be against public interest, if you are able to explain why responding would undermine future investigations or publications, or journalistic activities more generally, you could refuse the request. But you will always have to give a good reason to oppose it. Finally, do not forget that you must not include any information about other people unless they have consented, or it is reasonable to supply it without their consent.

6.2 Confidential sources

Sources of information are sacred to journalists. Several international instruments ensure their adequate protection, including the Resolution on Journalistic Freedoms and Human Rights, adopted at the 4th European Ministerial Conference on Mass Media Policy (Prague, 7-8 December 1994) and the Resolution on the Confidentiality of Journalists' Sources by the European Parliament (18 January 1994, Official Journal of the European Communities No. C 44/34). Moreover, Recommendation No. R(2000) 7 on the right of journalists not to disclose their sources of information was adopted by the Committee of Ministers of the Council of Europe on 8 March 2000. Moreover, in general domestic law and practice in member States provide for explicit and clear protection of the right of journalists not to disclose information identifying a source in accordance with Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms.

Thus, there is a legal framework that allows journalists to keep their sources undisclosed. This right can only be limited under the conditions mentioned by Principle 3(b) of Recommendation No. R(2000) 7, namely:

> "i. reasonable alternative measures to the disclosure do not exist or have been exhausted by the persons or public authorities that seek the disclosure, and
>
> ii. the legitimate interest in the disclosure clearly outweighs the public interest in the non-disclosure, bearing in mind that:
>
> -an overriding requirement of the need for disclosure is proved,

-the circumstances are of a sufficiently vital and serious nature,

-the necessity of the disclosure is identified as responding to a pressing social need, and

-member States enjoy a certain margin of appreciation in assessing this need, but this margin goes hand in hand with the supervision by the European Court of Human Rights.

c.The above requirements should be applied at all stages of any proceedings where the right of non-disclosure might be invoked".

Finally, we must not forget that revealing a source also implies data processing. And that the source is also a data subject that has the rights conferred by the GDPR. Therefore, if the source is an individual, you will probably be able to preserve his or her identity on the basis of the GDPR. Indeed, if the subject of a story makes a subject access request and this could only be satisfied by disclosing the identity of your sources, you can only proceed if the source consents, or if it is reasonable to do so, all circumstances considered. If the source is an organisation, circumstances change since organisations do not have personal data. So, journalists need to rely upon the journalism exemption to withhold the source's identity if they are not willing to reveal their name or if it is not appropriate to disclose it.

6.3 Minors and vulnerable population

You must be especially careful if you are willing to process data concerning minors or vulnerable populations. First, the legal basis for such processing might be feeble. Consent of a minor will only be valid if such minor can provide it according to the Member state legal framework. The GDPR establishes a minimum age, but Member states are empowered to raise it. Therefore, you must get informed about this. If the minor or the vulnerable person is unable to consent, their legal representatives should provide consent.

If you cannot obtain an informed consent, then processing should be based on the legitimate interest basis. However, the legitimate interest pursued by the controller

does not apply "where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child". Therefore, it is highly improbable that the balancing test allows for the processing of personal data corresponding to minors. In our opinion, similar thoughts are applicable to vulnerable populations.

The Guidelines on Safeguarding Privacy in the Media include a summary of two cases related to minors.

- "In Kahn v. Germany, pictures of two children of Oliver Kahn, a former goalkeeper of the German national football team, and his wife were featured in a magazine. The journalists were fined because they had violated the family's right to privacy. All the photos showed the children in the company of their parents or on holiday, though the subject of the reports had not been the children themselves, but rather their parents' relationship and Oliver Kahn's career.
- In Reklos and Davourlis v. Greece, taking pictures of a new-born baby without the consent of his parents (in the intensive unit to which only hospital staff should have had access) was considered to be a violation of the right to privacy even though the pictures were not published".

Notice that this last sentence is particularly relevant, since it focuses on the need to have a legal basis for data processing at the moment when the photographs are made. The decision of not publishing them only avoids a subsequent unlawful processing (publication), but does not mend the previous infringement of the right to privacy.

6.4 Takeaway points

There are some tips that might serve as a summary of the things that you must know about data protection compliance. In general, you should always keep in mind that:

- publication of personal data means data processing. Therefore, you must be sure that you are allowed to show these data before proceeding to do so. At that moment you must have a legal basis that allows processing. Otherwise, it would be unlawful.

- If the personal data is processed in order to serve the public interest ("journalistic purposes"), it is likely that the processing will not have to comply with some or all GDPR articles. Conversely, this means that if personal data is collected, analysed or otherwise processed for other reasons, the GDPR will apply in full.

- Publishing sensitive information might cause considerable harm to private life of the data subject. You must be sure that benefits to public interest justify such harm. To this purpose, you should balance the interests at stake, considering different levels of intrusion into the private life of the data subject. Only when public interest considerations clearly prevail against their privacy are you allowed to publish this information.

- The intervention of senior editorial or the use of expert input might be of great help to ensure that this requirement applies. Never forget that usually the interested journalists are not so objective while balancing the different interests involved.

- Always remember that you should only gather data that are relevant to your investigation and might of public interest. If, for instance, you are investigating a politician on the basis of a possible corruption practice and you discover sensitive information about his or her sexual orientation, you should not process it, provided that it is not relevant for the issue at stake. This is an essential requirement of the minimisation principle, a key concept in the GDPR.

- In particularly contentious cases, where it is not entirely clear whether 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 and consultation from the lead supervisory authority should be sought (Biriukova, p.30)

- Special precautions must be adopted where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs,

trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures.

- Data concerning the vulnerable population and especially minors should only be processed if strong reasons justify it. You must be absolutely sure that they apply to the concrete processing before proceeding.

7. Q&As

What about the secondary use of data?

The answer to this question depends on some key issues. First, if data were collected on the basis of legitimate interest, a contract or vital interests, it can be used for another purpose, as long as the new purpose is compatible with the original one. According to Article 6.4 of the GDPR, one should take into account, inter alia:

a. any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
b. the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
c. the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
d. the possible consequences of the intended further processing for data subjects;
e. the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If one would like to use the data for statistics or scientific research, it is not necessary to run the compatibility test. These new uses are compatible with the original purpose, according to Article 5.2 (b) of the GDPR.

If one processes the data on the basis of the data subjects' consent or following a legal requirement, no further processing beyond what is covered by the original consent or

the provisions of the law is possible. Further processing would require obtaining new consent or a new legal basis.

I'd like to get a focus about the subjects involved in commercialisation of personal data, an economic evaluation of the amount of this global trafficking system

In principle, data commercialization is only possible if no personal data are involved. In the event that a dataset mixes both types of data, the GDPR is applicable. Thus, commercialization of data would not be acceptable. Personal data are related to rights. They are not commodities and cannot be bought or sold. See the part of the PANELFIT Guidelines devoted to datasets and our Critical Analysis for further data.

Data retention/storage, right to be forgotten

In general, data should not be retained any longer than strictly needed for the purposes they were collected. If the controller considers that they might be useful in the future, they should justify this assortment. In any case, they should be stored in a way that works well with the minimization and storage limitation principles. Thus, they should be anonymized or, at least, pseudonymized whenever possible.

The right to be forgotten is regulated by Article 17 GDPR. If the conditions set forth in Article 17.1 GDPR are met, the controller shall "have the obligation to delete personal data without undue delay". Nonetheless, this is not an absolute right. The exemptions of Article 17.3 GDPR identify cases in which this obligation does not apply. One of these conditions is that the right "shall not apply to the extent that processing is necessary (…) for exercising the right of freedom of expression and information" (Article 17.3 (a)). How could we balance both rights and interests –right to erasure and right of freedom of expression and information? According to what it was explained by the CJEU in its Google 2 judgment, Article 17.3.a GDPR is "an expression of the fact that the right to protection of personal data is not an absolute right but (…) must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality".[14] The Court "expressly lays down the requirement to strike a balance between the fundamental rights to privacy and protection of personal data guaranteed by Articles 7 and 8 of the Charter, on the one

14 CJEU, Case C-136/17, judgment of 24 September 2019, paragraph 57.

hand, and the fundamental right of freedom of information guaranteed by Article 11 of the Charter, on the other."[15] On the other hand, the ECHR indicated in the judgment "M.L. and W.W. vs Germany" of June 28th, 2018, the that the balancing of the interests could hardly be resolved in favor of a request for erasure brought against the original publisher whose activity is at the heart of what freedom of expression aims to protect.[16] Thus, in general the right to be forgotten does not apply if it impedes the exercise of the right to information.

Data collection in investigations, data storage, handling of data from confidential sources

Professional secrecy is a fundamental value that should not be broken on the basis of data protection. Most probably, your Member State has adopted specific rules to set out the powers of the supervisory authorities laid down in points (e) and (f) of Article 58(1) in relation to controllers or processors that are subject, under Union or Member State law or rules established by national competent bodies, to an obligation of professional secrecy or other equivalent obligations of secrecy where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy (See Article 90 of the GDPR). Those rules, however, shall apply only with regard to personal data which the controller or processor has received as a result of or has obtained in an activity covered by that obligation of secrecy.

Forensic research/investigation with machine learning and false outputs of such approaches that affect citizens

Journalists are supposed to check the accuracy of their information carefully. Inferred data are personal data, since it provides information about an identifiable person. All rights and duties settled by the GDPR are applicable to them.

Specific tools that might make the data processing more manageable

PANELFIT Handbook for Journalists and Guidelines might be quite useful for these purposes.

15 CJEU, Case C-136/17, judgment of 24 September 2019, paragraph 59.

16 European Court of Human Rights (ECHR), "M.L. and W.W. vs Germany", 28 June 2018.

The lifecycle of handling data. If you can keep data or e.g. interview recordings, when should you delete them? Best practices for separating what can be kept indefinitely and what should be deleted, and about taking the time to actually delete relevant stuff from backup locations after x number of years

There is nothing like an objective standard of adequate storage time in the GDPR. It totally depends on whether storage makes sense or not. If you can prove that storing such data is needed for the purpose of the processing, you can keep them indefinitely. In any case, they should be stored in a way that works well with the minimization and storage limitation principles. Thus, they should be anonymized or, at least, pseudonymized whenever possible.

Regulation about health information

"Personal data that are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms" (Recital 51 GDPR). Data concerning health are considered special categories of personal data. According to Article 9.1, they cannot be processed unless an exception that allows for such processing occurs. Exceptions are listed in Article 9.2.

Protection about images

Images are personal data. Therefore, one needs a legal basis to process such data. If the images correspond to several people, the legal basis should apply to all data subjects. For instance, if the data basis is consent, you should have the consent of all people who are pictured in the photograph or video. Of course, public interest might be an excellent legal basis to allow processing, but you should carefully balance the rights, freedoms and interest at stake. For example, if you could avoid identification of those people who are not essential to the information, you should do it, especially if those are minors.

How to handle data that is publicly available in a non-structured format with the purpose of compiling a new dataset that could possibly lead to valuable information, but also harm vulnerable people (e.g. scraping [public] personal data from a social media)?

In general, you should always find a suitable legal basis for data processing. As previously mentioned, legitimate interest is, in the absence of consent, the most suitable one. If we are talking about the vulnerable population, this should be included prominently in the balancing test. Processing would only be lawful if public interest is so strong that it overwhelms the data subject interest.

Scraping as such does not introduce novelties in this basic rule. Even thought some data might be public, this does not mean that you can use them as you wish. In the case of data that are expressed in a social network, you should also take into account that you are also a user of that network. Thus, the Terms of Service are applicable to you. This should not in principle mean too much, but you should keep it in mind.

Detailed information about this is available here:

Moreno Mancosu, Federico Vegetti, What You Can Scrape and *What Is Right to Scrape: A Proposal for a Tool to Collect Public Facebook Data, Social media + Society*, Volume: 6 issue: 3, Article first published online: July 31, 2020; Issue published: July 1, 2020, at: https://journals.sagepub.com/doi/full/10.1177/2056305120940703

How to behave when you want to send a press release to another journalist's professional email address (assuming you did not have any prior contact). Should you ask for permission beforehand (and how, if not by email) or should you presume they have an interest in being informed, so you send them your press release and give them the possibility to opt-out? And what about follow-up emails?

In general, you can send emails to people's professional addresses, provided that:

- you have a good reason to think that the recipient can benefit from the information provided by the press release.
- you should inform the recipient of what personal data you are processing, for what purpose, and how they can remove their data from your mailing list, or change them, in case this list exists.
- Furthermore, you should not process the addressees' personal data (storage, for instance) for longer than necessary.

Sending follow-ups does not violate GDPR if it meets the three requirements described in the answer above. Data processing in case of a follow-up message should follow the same rules as a preliminary message.

8. Glossary (art. 4 GDPR)

(1) **'personal data'** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(2) **'processing'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(3) **'restriction of processing'** means the marking of stored personal data with the aim of limiting their processing in the future;

(4) **'profiling'** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

(5) **'pseudonymisation'** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

(6) **'filing system'** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

(7) **'controller'** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(8) **'processor'** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

(9) **'recipient**' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

(10) **'third party'** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

(11) **'consent'** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

(12) **'personal data breach'** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(13) **'genetic data'** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

(14) **'biometric data'** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

(15) **'data concerning health'** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

(16) **'main establishment'** means:

(a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

(b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

(17) **'representative'** means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;

(18) **'enterprise'** means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

(19) **'group of undertakings'** means a controlling undertaking and its controlled undertakings;

(20) **'binding corporate rules'** means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

(21) **'supervisory authority'** means an independent public authority which is established by a Member State pursuant to Article 51;

(22) **'supervisory authority concerned'** means a supervisory authority which is concerned by the processing of personal data because:

(a) the controller or processor is established on the territory of the Member State of that supervisory authority;

(b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or

(c) a complaint has been lodged with that supervisory authority;

(23) **'cross-border processing'** means either:

(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

(24) **'relevant and reasoned objection'** means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;

(25) **'information society service'** means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council (19);

(26) **'international organisation'** means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

Annex I. The balancing test

Introduction: The balancing test in the context of legitimate interest as a legal basis for processing

Legitimate interest is one of six legal bases for the processing of personal data stated in Article 6(1) of the GDPR. This legal basis requires that the legitimate interests of the controller or any third parties to whom the data are disclosed prevail over the interests, fundamental rights and freedoms of the data subjects (Article 6(1)(f). To verify that this is indeed the case, controllers can make use of a tool called balancing test, which was recommended by the Article 29 Working Party, for instance[17]. This tool is aimed at ensuring that the legitimate interests of the controller or any third parties to whom the data are disclosed prevail over the interests and fundamental rights and freedoms of the data subjects.

When do fundamental rights and freedoms of the person concerned by the data protection not take precedence?

Carrying out a balancing test involves considering several key factors that are decisive in determining which interests, freedoms or rights prevail, namely[18]:

- the **nature and source of the legitimate interest** – whether the data processing is necessary for the exercise of a fundamental right, is otherwise in the public interest, or benefits from recognition in the community concerned. Evaluating the possible prejudice suffered by the controller, by third parties or the broader community if the data processing does not take place is compulsory.
- The **power and status of the two parties** (controller or third party and data subject). For instance, an employer intending to process the data of an employee is in a stronger position than the employee. If the data subject is a minor his/her interests, rights or freedoms should be overweighted.

17 A29WP, Opinion 06/2014 on the notion of legitimate interests of the controller under Article 7 of Directive 95/46/EC. April 2014, p.24. At: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Accessed 05 January 2020

18 A29WP, Opinion 06/2014 on the notion of legitimate interests of the controller under Article 7 of Directive 95/46/EC. April 2014, p.24. At: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Accessed 05 January 2020.

- The **nature of the data**. Special categories data, for instance, should be given greater weight. Similarly, data that people are likely to consider particularly 'private' (for example financial data), children's data or data relating to other vulnerable individuals should be adequately weighed.

- The **impact of the processing on the data subjects**. To this purpose, controllers should consider whether processing might result in a high risk to individuals' rights and freedoms. If this is the case, they must perform a DPIA.

- The data subjects' **reasonable expectations** about what will happen to their data. Controllers should be able to demonstrate that a reasonable person would expect the processing in light of the particular circumstances applicable. If the purpose and method of processing is not immediately obvious and there is the potential for a range of reasonable opinions about whether people would expect it, controllers may wish to carry out some form of consultation, focus group or market research with individuals to demonstrate expectations and support their position. If there are pre-existing studies in regard to reasonable expectations in a particular context, controllers may be able to draw on these as part of their determination of what individuals may or may not expect[19].

- The **way data are processed** (large scale, data mining, profiling, disclosure to a large number of people or publication);

- The **additional safeguards** which could limit undue impact on the data subject, such as data minimisation (e.g. strict limitations on the collection of data, or immediate deletion of data after use) – technical and organisational measures to ensure that the data cannot be used to take decisions or other actions with respect to individuals ('functional separation') – wide use of anonymisation techniques, aggregation of data, privacy-enhancing technologies, privacy by design, privacy and data protection impact assessments; increased transparency,

19 ICO, How do we apply legitimate interests in practice? At: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/ Accessed: 15 January 2020

general and unconditional right to object (opt-out), data portability and related measures to empower data subjects, etc.

The issue of additional safeguard

The Article 29 Working Party considers that mitigation measures and safeguards, such as organisational or technical measures adopted by the controller for the protection of the data subject rights should be included in the balancing test. There is, however, an alternative approach, which considers that article 6(1)(f) asks for a balancing test between two values, the legitimate interests of the controller (or a third party) and the interests, rights and freedoms of the data subject. Mitigation measures and safeguards do not fit well with any of these values. Therefore, they should not be considered. Otherwise, they would outweigh the controllers' side since they would undermine the importance of the possible harm to be caused to the data subject interests, rights and freedoms. Kamara and De Hert have made some convincing statements on this concrete issue, by stating that[20]

> *"including mitigation measures in the assessment would lead to a representation of the actual expected impact of the processing to the data subjects' rights, and would still allow the legitimate interests to prevail. This approach does not 'punish' the controller that takes mitigation measures and safeguards, by not including them in the balancing test. On the contrary it encourages the controller to do so. On the other hand, one should keep in mind that the weight of future safeguards and mitigation measures is always relevant to their realisation and effectiveness. Such measures therefore should be considered, but not play a significant role in determining to which side the scale leans."*

Some examples of balancing test

Example 1[21]

20 Kamara, Irene and De Hert, Paul, "Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach, Brussels Privacy Hub, Working paper, vol. 4, nº 12, 2018, p.17. At: https://brusselsprivacyhub.eu/BPH-Working-Paper-VOL4-N12.pdf Accessed: 17 January 2020

21 Source: A29WP, Opinion 06/2014 on the notion of legitimate interests of the controller under Article 7 of Directive 95/46/EC. April 2014, p.63. At: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Accessed 05 January 2020

Case: Newspaper Z is considering the publication of some photographs that show X, an actor, after being arrested for cocaine possession at a public parade. X is a famous public figure in his country as he plays a policeman in a TV series. Furthermore, he has conceded several interviews providing data about his private life publicly.

Balancing test: the data concerns the individual's private life rather than professional life. Sharing the data might contribute to significant harm to the individual. However, there is a public interest in sharing this information. The actor's expectation that their privacy will be effectively protected has been reduced by the fact that he has disclosed data from his private life in several interviews. The outcome for the company having considered all the relevant factors must be that the famous actor interests do not outweigh its legitimate interests in publishing the photographs, and processing is lawful on the basis of these legitimate interests.

See: Axel Springer AG vs. Alemania

Example 2[22]

Case: An employer monitors Internet use during working hours by employees to check they are not making excessive personal use of the company's IT. The data collected include temporary files and cookies generated on the employees' computers, showing websites visited and downloads performed during working hours. The data is processed without prior consultation of data subjects and the trade union representatives/ work council in the company. There is also insufficient information provided to the individuals concerned about these practices.

Balancing test: The amount and nature of the data collected is a significant intrusion into the private life of the employees. In addition to proportionality issues, transparency about the practices, closely linked to the reasonable expectations of the data subjects, is also an important factor to be considered. Even if the employer has a legitimate interest in limiting the time spent by the employees visiting websites not directly relevant to their work, the methods used do not meet the balancing test of Article 7(f). The employer should use less intrusive methods (e.g. limiting accessibility of certain sites),

22 Source: ICO. How do we apply legitimate interests in practice? At: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/ Accessed: 15 January 2020

which are, as best practice, discussed and agreed with employees' representatives, and communicated to the employees in a transparent way.

DOs and DON'Ts

DOs

- Check the nature of the data processed and take extra care about protecting children's interests, rights and freedoms if they are at stake
- Consider the reasonable expectations of the data subjects
- Perform a DPIA if circumstances recommend it

DON'Ts

- Don't process children's data if it is not absolutely necessary to reach the pursued interest
- Don't process the data if the balancing test is inconclusive
- Don't hesitate to introduce adequate safeguards to minimise prejudice to data subjects interests, rights and freedoms

Check List

- The controllers have made sure that the individual's interests do not override legitimate interests of the controller or third parties.
- The controllers use individuals' data in ways they would reasonably expect.
- The controllers are not using people's data in a very intrusive way or in a way which could cause them harm, unless they have a particularly good reason.
- The controllers do not process children's data, or, if they do, they have taken extra care to make sure they protect their interests.
- The controllers have considered safeguards to reduce the impact where possible.
- The controllers have considered whether they need to conduct a DPIA.

Further Readings

- Additional examples of balancing test were provided by the Article 29WP and can be found in their Opinion 06/2014 on the notion of legitimate interests of the controller under Article 7 of Directive 95/46/EC

- A29WP, Opinion 06/2014 on the notion of legitimate interests of the controller under Article 7 of Directive 95/46/EC. April 2014, p. 24. At: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

- EDPS, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, 11 april 2017, at: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en.pdf. Accessed 5 May 2020

- ICO, How do we apply legitimate interests in practice? At: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/

- ICO, What is the 'legitimate interests' basis? https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/. Accessed 05 May 2020.

- Kamara, Irene and De Hert, Paul, "Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach, Brussels Privacy Hub, Working paper, vol. 4, nº 12, 2018, p.17. At: https://brusselsprivacyhub.eu/BPH-Working-Paper-VOL4-N12.pdf

Annex II. Comparative analysis of the regulatory framework at the EU Member states level

The main source for the information gathered is the Bird&Bird comparative analysis, except where otherwise indicated.

Austria

Last Reviewed: 05.06.2018

Sec 9 ADPA provides special provisions concerning the processing of personal data in the context of freedom of expression and information. According to these provisions, several regulations of the GDPR (especially its principles and rights of data subjects) do not apply to the processing of personal data for journalistic purposes as well as for scientific, artistic or literary purposes.

Belgium

Last Reviewed: 13.09.2018

Section 16 of the DPA allows processing of personal data carried out by adequate means for journalistic purposes or for purposes of academic, artistic or literary expression. Sections 17 et seq. stipulate exceptions to information obligations (Section 17), protection of source and content of information (Section 18), exceptions to right to restriction of processing (Section 19), information about rectification and erasure (Section 20), and limitation of the right to object (Section 21).

Finland

Last Reviewed: 13.11.2018

According to Section 27 of the Data Protection Act only limited provisions of the GDPR apply to the processing of personal data for the purposes of journalism or academic,

artistic or literary expression. This approach upholds the situation as it was under the abrogated Personal Data Act.

France

Last Reviewed: 11.02.2019

According to the French regulatory framework, when personal data is processed for journalistic, artistic or literary expression purposes, provisions regarding information notice, data transfers, data subject rights data, retention and the processing of special categories of data do not apply.

Germany

Last Reviewed: 23.05.2018

§ 35 of the new German Federal Data Protection Act ('FDPA') exempts the controller from the obligation to erase personal data where the erasure is, in case of non-automatic data processing, impossible, or only possible with disproportionately high effort and the data subject has a minor interest for erasure. § 27(2) FDPA restricts the data subjects' rights subject to certain further requirements.

Ireland

Last Reviewed: 07.06.2018

Under section 43(1) of the Act, the processing of personal data for the purpose of exercising the right to freedom of expression and information, including processing for journalistic purposes or for the purposes of academic, artistic or literary expression, shall be exempt from compliance with certain provisions of the GDPR where, having regard to the importance of the right of freedom of expression and information in a democratic society, compliance with such provisions would be incompatible with such purposes. The Data Protection Commission may refer any question of law which involves consideration of whether processing of personal data is exempt under section 43(1) to the High Court for its determination.

Italy.

Last Reviewed: 25.10.2018

IDPA title XII - sections 136-137-138-139. The code of practice on the processing of personal data & journalistic activities (Annex A.1 of IDPA) remains in force. The compatibility of this code with the GDPR will be reassessed by the Italian Data Protection Authority (hereinafter, the "Authority"). The Authority should review it before the end of the calendar. Furthermore, Italy incorporated some principles regarding the journalistic exemption through a code of ethics, namely

a) the requirement to avoid any kind of prior censorship

b) the exemption of the right to information in the collection of data when the professional exercise requires it

c) the journalist's duty to rectify errors and inaccuracies without delay

d) the need to be particularly careful when the processing affects specially protected data. In such circumstances, processing shall be limited to facts of undisputed public interest. Moreover, it shall be limited to the essential aspects of the information and avoid references to persons not related to them. Even in the case of matters that the interested party may have made public, or which are appreciated in public behaviour, the right to be protected is reserved

e) it is suggested that the "essentiality" of the information be sought, the proportionality of what is made public, so that it is limited to what is essential in relation to the case

f) when a news item relating to health is referred to, the dignity, decorum and private life of the affected person shall be respected, especially when serious or terminal illnesses are involved, abstaining from publishing analytical data or data of strictly clinical interest. However, an exception may be made to this requirement where, in accordance with the principle of proportionality, if the person concerned is in a position of particular public importance. The same applies to information on sex life.

The Netherlands

Last Reviewed: 17.09.2018

Article 41 GDPR Execution Act provides that the GDPR Execution order does not apply where personal data are processed exclusively for journalistic purposes or for the purposes of academic, artistic or literary expressions. In addition it sums up a list of chapters and articles in the GDPR that are also not applicable for these purposes: (a) article 7(3), 11(2);(b) chapter III; (c) chapter IV (with the exception of articles 24, 25, 28, 29 and 32); (d) chapter V; (e) chapter VI; and (f) chapter VII. "Art. 41 UAVG limits the scope of certain obligations in connection with (compelling) general interests in alignment with art 23 GDPR. Therefore, it provides for exceptions to the rights of the data subject and the duties of the controller. The GDPR partially (art. 12-21 and 34 GDPR) does not apply (insofar appropriate and proportionate) to data processing in view of – inter alia – important public interest objectives, public security, the protection of the data subject or of the rights and freedoms of others; and/or the collection of civil claims.

Spain

Last Reviewed: 05.03.2019

The SDPA does not include any legal precept that conciliates freedom of expression with data protection. There is only a reference to freedom of expression in article 85 regarding the right to freedom of expression in Internet that everyone has.

Sweden

Last Reviewed: 06.09.2018

Data Protection Act paragraph 1:7: the GDPR and the Data Protection Act shall not be applied to the extent that it would breach the laws on freedom of expression. The Data Protection Act provides that articles 5-30 and 35-50 of the GDPR shall not be applicable to the processing of personal data for journalistic purposes or for purposes of academic, artistic or literary expressions.

United Kingdom

Last Reviewed: 23.05.2018

The UK Data Protection Act 2018[23] 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 (Cain, 2018):

- the data in question must be 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 consideration existing codes of conduct 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. Although the ECtHR refrained from providing a definition of the "public interest", it recognised this notion to cover the public, political and historic debate, issues related to the politicians, behaviour 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 (Bitiukowa, 21).

23 Vid. The UK Data Protection Act 2018, Schedule 2, Part 5, par. 26, http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/part/5/enacted.

Information related to exemptions and derogations in a nutshell

The following table (Bitiukowa, 25) includes an updated comparison between several EU Member states regarding the regulation of the exceptions.

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.

Sources of information

Bibliography

Article 29 Working Party, RECOMMENDATION 1/97 Data protection law and the media. Adopted by the Working Party on 25 February 1997, at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1997/wp1_en.pdf. Last visited: 17/10/2020.

BIRD & BIRD, Personal data and freedom of expression, At: https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/personal-data-and-freedom-of-expression. Last visited: 17/10/2020.

BENEZIC, Dollores, Romania May Be Using GDPR to Intimidate Journalists, Liberties, 2018, At: https://www.liberties.eu/en/news/politicians-in-romania-use-gdpr-to-intimidate-journalists/16384. Last visited: 17/10/2020.

BITIUKOVA, Natalija, Journalistic exemption under the european data protection law, Vilnius Institute for Policy Analysis, 2020, at: https://vilniusinstitute.lt/wp-content/uploads/2020/01/VIPA_Bitiukova_2020_v4_f.pdf. Last visited: 17/10/2020.

CAIN N. and COWPER-COLES, R., GDPR and the Data Protection Act 2018 – how do they impact publishers?, 25 May 2018, https://www.lexology.com/library/detail.aspx?g=b26433e1-0548-4a9d-8351-f720e737f811. Last visited: 17/10/2020.

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. Last visited: 17/10/2020.

DETREKŐI, Zsuzsa, GDPR in Hungary: A Road to Hell?, At: https://medium.com/center-for-media-data-and-society/gdpr-in-hungary-a-road-to-hell-3b60718a0281. Last visited: 17/10/2020.

DRECHSLER L., The GDPR and Journalism. Protecting Privacy or a Break on Democratic Accountability?, 18 September 2018, https://brusselsprivacyhub.eu/publications/ws21.html. Last visited: 17/10/2020.

ECtHR, Guide on Article 8 of the European Convention on Human Rights, August 2020, at: https://www.echr.coe.int/documents/guide_art_8_eng.pdf. Last visited: 17/10/2020.

EDRI, Proceed with caution, at: https://edri.org/files/GDPR_analysis/EDRi_analysis_gdpr_flexibilities.pdf. Last visited: 17/10/2020.

NIELSEN, Nikolaj. EU Warns Romania Not to Abuse GDPR Against Press, EU Observer (Nov. 12, 2018

REVENTLOW, Nani Jansen, Symposium on the GDPR and international law. Can the GDPR and freedom of expression coexist? At: https://www.researchgate.net/publication/338407067_Can_the_GDPR_and_Freedom_of_Expression_Coexist. Last visited: 17/10/2020.

The UK Information Commissioner's Office, Data protection and journalism: a guide for the Media, 2014, at: https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf. Last visited: 17/10/2020.

WARNER, Bernhard, Online-Privacy Laws Come With a Downside, The Atlantic, 2019, at: https://www.theatlantic.com/ideas/archive/2019/06/europes-gdpr-elevated-privacy-over-press-freedom/590845/. Last visited: 17/10/2020.

Documents of the Council of Europe

Convention for the protection of individuals with regard to the processing of personal data

Recommendation CM/Rec(2018)1 of the Committee of Ministers to member States on media pluralism and transparency of media ownership

Recommendation CM/Rec(2016)4 of the Committee of Ministers to member States on the protection of journalism and safety of journalists and other media actors

Recommendation CM/Rec(2011)7 of the Committee of Ministers to member states on a new notion of media

Declaration by the Committee of Ministers on the protection and promotion of investigative journalism (26 September 2007)

Resolution 2066 (2015), Media responsibility and ethics in a changing media environment, Parliamentary Assembly

Resolution 1843 (2011), The protection of privacy and personal data on the Internet and online media, Parliamentary Assembly

Resolution 1165 (1998), Right to privacy, Parliamentary Assembly

Resolution 1003 (1993), Ethics of Journalism, Parliamentary Assembly

Jurisprudence by the European Court of Human Rights

- A v. Norway, No. 28070/06, 9 April 2009
- Ageyev v. Russia, No. 7075/10, 18 April 2013
- Alkaya v. Turkey, No. 42811/06, 9 October 2012
- Armonienė v. Lithuania, No. 36919/02, 25 November 2008
- Axel Springer Ag v. Germany [GC], No. 39954/08, 7 February 2012
- Bédat v. Switzerland [GC], No. 56925/08, 29 March 2016
- Biriuk v. Lithuania, No. 23373/03, 25 November 2008 Björk Eiðsdóttir v. Iceland, No. 46443/09, 10 July 2012
- Bladet Tromsø and Stensaas v. Norway, No. 21980/93, 20 May 1999
- Bodrožić v. Serbia, No. 32550/05, 23 June 2009 Bohlen v. Germany No. 53495/09 and Ernst August von Hannover v. Germany No. 53649/09, 19 February 2015
- Couderc and Hachette Filipacchi Associés v. France [GC], No. 40454/07, 10 November 2015

- Dorothea Sihler-Jauch against Germany and Günther Jauch v. Germany, Nos. 68273/10 and 34194/11, 24 May 2016 (decision)
- Egeland and Hanseid v. Norway, No. 34438/04, 15 April 2009
- Erla Hlynsdóttir (No.2), No. 54125/10, 21 October 2014
- Feldek v. Slovakia, No. 29032/95, 12 July 2001 Flinkkilä and Others v. Finland, No. 25576/04, 6 April 2010
- Fürst-Pfeifer v. Austria, Nos. 33677/10 and 52340/10, 17 May 2016
- Guseva v. Bulgaria, No. 6987/07, 17 February 2015
- Hachette Filipacchi Associés v. France, No. 71111/01, 14 June 2007
- Hachette Filipacchi Associés v. France [GC], No. 40454/07, 10 November 2015
- Hachette Filipacchi Associés ("Ici Paris") v. France, No. 12268/03, 23 July 2009
- Haldimann and Others v. Switzerland, No. 21830/09, 24 February 2015
- Janowski v. Poland, No. 25716/94, 21 January 1999
- Khan v. Germany, No. 38030/12, 21 September 2016
- Khmel v. Russia, No. 20383/04, 12 December 2012
- Khuzhin and Others v. Russia, No. 13470/02, 23 October 2008
- Krone Verlag GmbH & Co. KG v. Austria, No. 34315/96, 26 February 2002
- Krone Verlag GmbH & Co KG and Krone Multimedia GmbH & Co KG v. Austria, No. 33497/07, 17 January 2012
- Leempoel & S.A. ED. Ciné Revue v. Belgium, No. 64772/01, 9 November 2006
- Lillo-Stenberg and Sæther v. Norway, No. 13258/09, 16 January 2014 Mitkus v. Latvia, No. 7259/03, 2 October 2012
- MGN Limited v. the United Kingdom, No. 39401/04, 18 January 2011
- Mosley v. the United Kingdom, No. 48009/08, 10 May 2011
- Müller v. Germany (Dec.), No. 43829/07, 14 September 2010
- Österreichischer Rundfunk v. Austria, No. 35841/02, 7 December 2006 Guidelines on Safeguarding Privacy in the Media 38
- Peck. V. United Kingdom, No. 44647/98, 28 January 2003 Pentikäinen v. Finland [GC], No. 11882/10, 20 October 2015 Reklos and Davourlis v. Greece, No. 1234/05, 15 January 2009 Renaud v. France, No. 13290/07, 25 February 2010
- Salihu and Others v. Sweden, No. 33628/15, 10 May 2016 (decision)
- Schweizerische Radio- und Fernsehgesellschaft SRG v. Switzerland, No. 34124/06, 21 June 2012

- Selistö v. Finland, No. 56767/00, 16 November 2004
- Standard Verlags GmbH v. Austria (No.2), No. 21277/05, 4 June 2009
- Standard Verlags GmbH v. Austria (No. 3), No. 34702/07, 10 January 2012
- Toma v. Romania, No. 42716/02, 24 February 2009
- Verlagsgruppe News GmbH v. Austria, No. 10520/02, 14 December 2006
- Von Hannover v. Germany, No. 59320/00, 24 June 2004
- Von Hannover v. Germany (No.2) [GC], Nos. 40660/08 and 60641/08, 7 February 2012
- White v. Sweden, No. 42435/02, 19 September 2006
- Wirtschafts-Trend Zeitschriften-Verlagsgesellschaft mbH v. Austria (no.2), No. 62746/00, 14 November 2002 (decision)
- Y v. Switzerland, No. 22998/13, 06 June 2017
- Zvagulis v. Lithuania, No. 8619/09, 26 January 2017 (decision)