Special, Personal and Broad Expression: Exploring Freedom of Expression Norms under the General Data Protection Regulation

David Erdos

Abstract: The interface between data protection and freedom of expression is increasingly crucial and the General Data Protection Regulation (GDPR) solidifies a bipartite or potentially even tripartite conceptualization of this relationship. Whilst the GDPR’s personal exemption can play some role in governing individual expression, it must be construed narrowly so as to only exclude innocuous publication that is not liable to infringe other’s fundamental rights. The special expression derogation remains central and encompasses not just journalism but also other forms of special expression (academic, artistic, literary) which, when published, are objectively orientated towards a collective public. Whilst Member States do retain considerable discretion given the wide diversity of national constitutional norms in this area, a strict balancing between fundamental rights should still be ensured. Freedom of expression is also distinctly furthered by, inter alia, self-expression on social networking sites and the facilitation of a range of expressive purposes by search engines. As shown in GC and Others v CNIL, the stricter reconciliation of rights here must retain a direct role for data protection’s core substance including its legal grounds and principles and is thereby substantially (albeit not completely) harmonized across the EU.

I. Introduction

Although approximately half of the world’s jurisdictions now have data protection laws, Europe was the ‘cradle’ of this framework and since the adoption of

1 See G Greenleaf, ‘Global data privacy laws 2019: 132 national laws and many bills’ (2019) 157 Privacy Law and Business International Report, 14.

2 F Hondius, A Decade of International Data Protection (1983) 30 Netherlands International Law Review 103, 104. Indeed, even at the time of the adoption Data Protection Directive 95/46 in the mid-1990s only two countries outside Europe – Israel and New Zealand – had adopted
Data Protection Directive 95/46 (DPD), including its transborder ‘adequacy’ regime, the European Union (EU) has assumed a position of the leading norm entrepreneur in this area. Moreover, the ground-breaking judgment of the Court of Justice of the EU (CJEU) in *Google Spain* (2014), which applied data protection to search engine indexing, confirmed that this was also the case in relation to the increasingly crucial interface between data protection and freedom of expression including its sub-right, the freedom of information. With the adoption of the General Data Protection Regulation 2016/679 (GDPR), including its formalization of a ‘right to be forgotten’ as a crucial mechanism for promoting greater ‘information self-determination’, the EU aims to solidify what it considers to be a ‘digital gold standard’ here over the coming decades. It is, therefore, important to explore what precise understanding of the relationship between data protection and freedom of expression the GDPR in fact furthers. To do so effectively, it is also necessary to look back much further into this framework’s history. Although it was only with *Google Spain* that this was brought to general worldwide public visibility, recognition of an interface with freedom of expression goes back to the very beginning of European data protection law. Building on the Explanatory Report of the Council of Europe Data Protection Convention of 1981, the DPD conceived this in essentially dichotomous terms. In sum, the need for a reconciliation between these rights was only explicitly acknowledged when processing was solely for journalistic, artistic, or literary purposes. However, subsequent CJEU case law increasingly came to recognize the significantly more variegated nature of this interface. The GDPR has comprehensive data protection law. See Israel, Protection of Privacy Law, 5741-1981 and New Zealand, Privacy Act 1993.

5 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281/31.

4 Ibid, Arts 25–26. The EU’s ‘adequacy’ exercised a powerful *de facto* extraterritorial effect and continues to constitute a key driver behind its global influence here (see Greenleaf (n 1), 18).

5 Case 131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzáles v AEPD*, ECLI:EU:C:2014:317.

6 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) OJ L 119/1.

7 Ibid, Art. 17.

8 O Lynskey, ‘Deconstructing data protection: the “added-value” of a right to data protection in the eu legal order’ (2014) 63 *International and Comparative Law Quarterly*, 569, 597.

9 G Buttarelli, ‘The EU GDPR as a clarion call for a new global digital gold standard’ (2016) 6 *International Data Privacy Law*, 77, 78.

10 This interface also has considerably more salience than is commonly recognized in other jurisdictions internationally. See D Erdos, ‘The “right to be forgotten” beyond the EU; an analysis of wider G20 regulatory action and potential next steps’ (2021/forthcoming) 13 *Journal of Media Law*, doi.org/10.1080/17577632.2021.1884947.

11 Council of Europe, Convention for the protection of individuals with regard to automatic processing of personal data (1981) ETS 108 (Data Protection Convention).

12 Ibid, Art. 9.
powerfully furthered this trend through what is best understood as a tripartite conceptualization of freedom of expression. In sum, alongside a broader conceptualization of journalistic and other forms of special expression, the GDPR recognized a broad expression area where data protection also has to be reconciled with freedom of expression (and its sub-right, freedom of information). A clear case falling within the latter area is search engine indexing, as highlighted not only in *Google Spain* itself but also in the recent Grand Chamber judgments of *GC and Others v CNIL* (2019) and *Google v CNIL* (2019). Special expression benefits from an overarching rights balancing test based on a strict necessity standard and, as the German Constitutional Court has recently emphasized in *Right to be Forgotten I*, is overseen principally by individual EU Member States. In contrast, broad expression continues to fall inside many of EU data protection’s core provisions including, at the least, the data protection principles in and of themselves and the legal grounds for processing. Finally, although the personal or household exemption has historically been strictly confined to ‘activities which are carried out in the course of private or family life of individuals’, the GDPR hints that it could play a limited role in reconciling data protection with certain personal expressions including in the area of ‘social networking’. Nevertheless, given the overriding need to ensure ‘effective and complete protection of data subjects’ and the fact that this operates as a full exemption, this role would need to be confined to activities which clearly pose a low risk to a data subject’s rights including, in particular, their privacy, reputation, and human dignity.

Drawing especially on CJEU case law, the GDPR text, its *travaux préparatoires*, and national implementing legislation, this article provides a detailed exploration of the evolving nature of the data protection–freedom of expression interface within the EU in the GDPR-era. For reasons of analytical clarity and space, the article does not explore the allocation of responsibility for compliance where different online operators, including individual users, cloud providers, social networking platforms, and internet search engines may be variously characterized as sole controllers, co-controllers, or joint controllers of personal data or perhaps simply processors operating entirely on behalf of another actor. These complexities will be further explored in future work. Instead, the article focuses on the more basic question of which substantive data protection norms are and should be applicable to which activities as a

---

13 Ibid, Art. 85(2).
14 Ibid, Art. 85(1).
15 Case 136/17 *GC and Others v Commission National de l’Informatique et des Libertés*, ECLI:EU:C:2019:773.
16 Case 507/17 *Google LLC v Commission Nationale de l’Informatique et des Libertés (CNIL)*, EU:C:2019:772.
17 BVerfG, 6 November 2019, docket number 1 BvG 16/13.
18 GDPR, Arts 5–6.
19 Case 101/01, *Criminal proceedings against Bodil Lindqvist*, EU:C:2003:596, para. 47.
20 GDPR, Art. 18.
21 *Google Spain* (n 5), para. 34.
result of the GDPR. The article is structured into seven sections. Following this introduction, the next main section provides an overview of the formal development of pan-European data protection instruments up to the GDPR, looking especially at the derogations and exemptions relevant to freedom of expression. The other parts of the article then focus in more detail on particular types of freedom of expression as recognized by the GDPR. Section III looks at the scope and substantive norms applicable to journalism and similarly the special types of freedom of expression as detailed in Article 85(2). Following an analysis in Section IV of the potential role of the personal or household exemption set out in Article 2(2)(c), Sections V and VI likewise look at the scope and substantive norms applicable to broad expression as safeguarded in Article 85(1). The final section concludes by drawing the various strands of the argument together.

II. The formal nature and development of pan-European data protection law including the derogations and exemptions relating to freedom of expression

A. General nature and development

The General Data Protection Regulation (GDPR) 2016/679 is now the keystone pan-European legal instrument ensuring a harmonized system for safeguarding personal data and thereby enabling its free movement across the EU. Nevertheless, it has its roots in a process of pan-European legal coordination that spans over forty years. The first binding legal instrument, the Data Protection Convention, was drafted and agreed by the Council of Europe in 1981. In 1995 the EU adopted the Data Protection Directive (DPD) 95/46, which specified a common standard of data protection and required this to be implemented throughout the Union through legislation enacted in each Member State. In 2000 the EU recognized data protection as a fundamental right within the EU Charter22 and in 2009 this right acquired formal legal status under the EU Treaties.23 Finally, in 2016 the EU enacted the GDPR which, aside from certain special areas, applied directly without the need for further Member State action. This instrument has applied across the Union from 25 May 2018.24

Since the time of the Convention, European data protection has had a similar general scope, purpose, and shape. Absent a specific exception, it has encompassed any 'personal data' which are subject to 'processing' using automation (ie a computer) or, in some cases, even certain purely manual means. ‘Personal data’ has been defined to include any and all 'information about an identified or

---

22 Charter of Fundamental Rights of the European Union, Art. 8.
23 Treaty of European Union (TEU), Art. 6 (1) and Treaty on the Functioning of the European Union (TFEU), Art. 16.
24 GDPR Art. 99 (2).
identifiable’ natural person (or data subject)\textsuperscript{25} and ‘processing’ has been equally widely specified to include a full range of operations including \textit{inter alia} storage, retrieval, and dissemination.\textsuperscript{26} Meanwhile, the purpose of data protection has to been to protect a whole host of individual’s rights and freedoms which may be impacted by such processing including ‘in particular’ the ‘right to privacy’\textsuperscript{27} or, as the GDPR reframes it, the ‘right to the protection of personal data’\textsuperscript{28} itself. In order to achieve this, personal data processing has been made subject to:

- a broad range of \textit{data principles and legality provisions} centred on fairness, lawfulness, purpose limitation, data minimization, and data quality,\textsuperscript{29}
- detailed \textit{transparency and controls rules} which set out requirements for ensuring the openness of processing (both in general terms and, when subject to a data subject’s access request, in granular form), as well as an ability for the data subject to (at the least) prevent continued illegal processing of ‘their’ data,\textsuperscript{30}
- \textit{sensitive data rules} which heavily restrict the processing of data relating to criminality, health, sex life, and other categories which are deemed to pose a particular risk to the rights and freedoms of the data subject,\textsuperscript{31}
- \textit{integrity provisions} which seek to ensure that the rest of the scheme is not undermined by, for example, lax data security or the international transfer of the personal data to a jurisdiction where it will lack this kind of protection.\textsuperscript{32}

\section*{B. Derogations and exemptions relevant to freedom of expression}

European data protection has always sought to balance the broad default described above through a range of special derogations and exemptions, some of which are more or less relevant to freedom of expression. Looking first at the derogations, the Data Protection Convention did not contain any explicit provision related to this right. However, similarly to the qualified rights set out in the European Convention on Human Rights,\textsuperscript{33} this Convention did recognize that all but the integrity provisions mentioned above could be restricted insofar as this was ‘provided for by the law’ and constituted ‘a necessary measure in a democratic society in the interests of’ \textit{inter alia} ‘the rights and freedoms of others’.\textsuperscript{34} The

\begin{footnotesize}
\begin{itemize}
\item Data Protection Convention, Art. 2(a); DPD, Art. 2(a); GDPR, Art. 4(1).
\item Data Protection Convention, Art. 2(c); DPD, Art. 2(b); GDPR, Art. 4(2).
\item Data Protection Convention, Art. 1; DPD, Art. 1(1).
\item GDPR, Art. 1(2).
\item Data Protection Convention, Art. 5; DPD, Arts. 6–7; GDPR, Arts 5–6.
\item Data Protection Convention, Art. 8; DPD, Arts 10–12, 14–15, and 21; GDPR, Arts 12–22.
\item Data Protection Convention, Art. 6; DPD, Art. 8; GDPR, Arts 9–10.
\item Data Protection Convention, Arts 7 and 12; DPD, Arts 16–20 and 25–26; GDPR, Arts 24–49.
\item European Convention on Human Rights, Arts 8–11.
\item Data Protection Convention, Art. 9.
\end{itemize}
\end{footnotesize}
Convention’s Explanatory Report further elucidated that the latter phrase ‘concern[ed] major interests’ of ‘third parties’ including ‘for example freedom of the press’.\textsuperscript{35} Both the DPD and the GDPR contained a similar \textit{general derogation clause}, although each still mandated that a legal ground for processing be satisfied\textsuperscript{36} and the GDPR further specified that the data protection principles could only be limited ‘insofar as its provisions correspond[ed]’\textsuperscript{37} to the transparency and control rules. These two instruments also set out a standard derogation \textit{vires} related to the sensitive data rules using different wording that generally depended on the provision of additional safeguards and the satisfaction of a substantive public interest test.\textsuperscript{38}

Sitting alongside these standard derogations, both the DPD and the GDPR included articles explicitly dedicated to data protection’s interface with freedom of expression. The DPD confined itself to a derogatory provision focused solely on the pursuit of journalistic purposes, as well as artistic and literary expression. EU Member States were to accord such special expressive processing derogations from potentially any of the substantive provisions of data protection but ‘only if they [were] necessary to reconcile the right to privacy with the rules governing freedom of expression’.\textsuperscript{39} The GDPR formulated a modified version of this \textit{special expressive purposes derogation},\textsuperscript{40} notably expanding its reach to include academic expression and reserving to a recital the need for processing to be ‘solely’ for such purposes.\textsuperscript{41} Otherwise, this recital stressed the need to interpret the relevant concepts here ‘broadly’ and the article itself stressed that the derogations provided by Member States should be those ‘necessary to reconcile the right to the protection of data with the freedom of expression and information’. A linked provision required that these provisions and any update to them be notified to the European Commission. Alongside this, the GDPR also set out a \textit{broad freedom of expression} provision which required states ‘by law to reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information’\textsuperscript{42} even outside the area of special expression.

In contrast to the Data Protection Convention,\textsuperscript{43} both the DPD and the GDPR set out a full exemption from data protection for processing ‘by a natural

\textsuperscript{35} Data Protection Convention Explanatory Report, para. 58. For a full analysis of this provision as well as other transnational and national developments prior to when the DPD was proposed see D Erdos, \textit{European Data Protection Regulation, Journalism and Traditional Publishers: Balancing on a Tightrope} (Oxford: Oxford University Press, 2019) 57–69, 210–12.
\textsuperscript{36} DPD, Art. 13.
\textsuperscript{37} GDPR, Art. 23.
\textsuperscript{38} DPD, Art. 8(4); GDPR, Art. 9(1)(g). As regards criminal-related data, each instrument established a slightly different test, only requiring that ‘suitable specific safeguards’ (DPD, Art. 8(5)) or ‘appropriate safeguards’ (GDPR, Art. 10) be set down in law.
\textsuperscript{39} DPD, Art. 9.
\textsuperscript{40} GDPR, Art. 85(2).
\textsuperscript{41} Ibid, recital 153.
\textsuperscript{42} GDPR, Art. 85(1)).
\textsuperscript{43} Article 3(2)(a) of the Data Protection Convention did include a provision enabling State Parties to specify a list of any ‘categories of automated personal data files’ which it would not apply the
person in the course of a purely personal or household activity’. The wording of this provision was deliberately narrow and appeared focused on fully private activity. Indeed, a linked recital in the DPD emphasized this by giving as examples ‘correspondence and the holding of addresses’. Nevertheless, it has been increasingly debated whether this provision could play some role in reconciling data protection with certain types of public freedom of expression online. A new recital within the GDPR appears to create an opening to such possibilities. In sum, whilst stressing that protected activities should have ‘no connection to a professional or commercial activity’ and that the Regulation ‘applies to controllers or processors which provide the means for processing’, it also states that the exemption ‘could include’ not only the examples given in the DPD but also ‘social networking and online activity’ so long as these are undertaken within the context of purely personal or household activity.

III. Journalism and other special expression under the GDPR

A. Scope of special expression

As outlined above, the GDPR continued and developed the special expression framework established under the DPD by setting out a sui generis regime for processing ‘carried out for journalistic purposes or the purpose of academic artistic or literary expression’. Although none of these terms are explicitly defined, both a GDPR recital and CJEU case law under the DPD have clarified that they must be interpreted ‘broadly’. In particular, notwithstanding an earlier exclusive focus on institutional actors such as the Press, it is clear that this provision will apply ‘not only to media undertakings’ but rather to ‘every person’ pursuing the relevant purposes including, in principle, individuals using online Convention to. This provision has sometimes been used to notify an exemption for personal or household processing.

44 DPD, Art. 3(2); GDPR, Art. 2(2)(c).
45 DPD, recital 12.
46 See, for example, Article 29 Working Party, Proposals for Amendments regarding exemption for Personal or Household Activities (2013) <https://ec.europa.eu/justice/article-29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en.pdf> accessed 23 March 2021. Note, however, that the Working Party later stepped back from this perspective stating that it was ‘in favour of a limited and carefully balanced household [or personal] exemption applying to “purely” household activities as provided for in Directive 95/46/EC and interpreted by ECJ [European Court of Justice] case law’. See Article 29 Working Party, Appendix: Core topics in view of the trilogue (2015), 3 <https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf> accessed 23 March 2021.
47 GDPR, recital 18.
48 Ibid, recital 18; Case C-73/07 Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy, ECLI:EU:C:2008:727, para. 56.
49 Satamedia (n 49), para. 58; Case C-345/17 Proceedings brought by Sergejs Buivids, ECLI:EU:C:2019:122, para. 52.
platforms, such as for example YouTube, to ‘send, watch and share videos’ \(^{51}\) and other material. Confirming a definition originally put forward in the CJEU Grand Chamber case of Satamedia (2008), the Court in Buivids also held that journalistic activities were ‘those which have as their purpose the disclosure to the public of information, opinions or ideas’. \(^{52}\) To date, the Court of Justice has almost completely elided journalistic purposes with the special purposes in general \(^{53}\) and has, therefore, not explicitly addressed the meaning of the other special purposes which relate to art, literature, and now academia. However, at least in the context of activities orientated towards the dissemination of material to an indeterminate number, it seems likely that the core added value of these other concepts is to emphasize that material (‘information, opinions and ideas’) protected by this provision need not (even when initially published) be on a matter of immediate ‘public concern’. \(^{54}\) Rather, these communications may relate to broader artistic, literary, or academic matters which, to borrow from the European Court of Human Rights’ (ECtHR) European Convention on Human Rights jurisprudence, may legitimately be of interest to the public in a ‘democratic society’ committed to the values of ‘pluralism, tolerance and broadmindedness’. \(^{55}\) Thus, the ECtHR has stressed that ‘[t]hose who create, perform, distribute or exhibit works of art contribute to the exchange of ideas and opinions which [are] essential for a democratic society’. \(^{56}\) Meanwhile, the Court has also ‘underline[d] the importance of academic freedom’ including the freedom of academics to ‘distribute knowledge and truth without restriction’. \(^{57}\)

Notwithstanding its broad construction, there are critical limits to the scope of the special purposes derogation. For example, even though a search engine disseminates its indexing results to an indeterminate number of people, the CJEU Grand Chamber judgment of Google Spain (2014) was emphatic that ‘no es el caso’ (‘it is not the case’) that its activity could be conceived of as journalistic (or, by implication, any other type of special expression). \(^{58}\) Similarly, during its exploration of the individual upload of a video onto YouTube, the Court in Buivids (2019) stressed that ‘the view cannot be taken that all information published on the internet, involving personal data, comes under the concept of “journalistic activities” and thus benefits from the [special purposes] exemptions or derogations [in the DPD]’. \(^{59}\) Looking at both this jurisprudence and the purpose of the

---

51 Buivids (n 50), para. 55.
52 Ibid, para. 53.
53 See, for example, Google Spain (n 5), para. 85.
54 Janowski v Poland (2000) 29 EHRR, 705, para. 31.
55 Handside v United Kingdom (1979) 2 EHRR 245, paras 66–67.
56 Müller v Switzerland (1998) 13 EHRR 21, para. 31.
57 Sorguc v Turkey (2009) App no. 17098/03 (23 June 2009), para. 34. See also Sapan v Turkey App no 44102 (8 June 2010).
58 Case 131/12 Google Spain (2014), para. 85 (referencing authoritative Spanish version). For an unclear reason, the English translation was slightly more ambiguous, stating that it did not ‘appear to be’ the case that search engine indexing fell within this derogation.
59 Buivids (n 50), para. 58.
special expression regime, it is clear that the ‘the public’ in this context is not seen as equivalent to simply any indeterminate collection of people. Instead, it must be conceived of as a collective entity akin to at least a section of the body politic or society at large. The special expressive purposes derogation will, therefore, safeguard all legal and natural persons who genuinely seek to disseminate material to such a collective public, irrespective of whether this material is of a journalistic, academic, artistic, or literary nature. In contrast, notwithstanding that their number may be open and indeterminate, a controller who discloses information, opinions, or ideas to an essentially privatized group of individuals would fall outside of this derogation.

At least in principle, the special expressive purposes derogation depends on further legislative action by the Member States. Indeed, the GDPR text emphasizes this point by requiring this law to be notified to the European Commission. As previously explored, almost all Member States have enacted relevant provisions. Moreover, in some contrast to the situation under the DPD, the great majority have ensured that these provisions cover all types of special expression as set out within the GDPR. However, a small group of States have failed to legislate at all and a further limited group have adopted a narrower definition, generally by excluding explicit reference to academic expression. Nevertheless, as explored further below, the Court of Justice in Buivids (2019) indicated that, at least in the absence of appropriate local legislation, the special expressive purposes derogation must be treated as self-executing. It, therefore, seems clear that all those pursuing journalistic, artistic, academic, or literary expressive purposes should benefit from this derogatory scheme. The nature of the substantive norms which will be then be applicable is examined below in Section III.B.

B. Shape of the special expression regime

In contrast to the tighter pan-EU control of its scope, it is manifest that Member States retain very considerable discretion as regards the internal shape of the

---

60 For a full analysis of this point, completed prior to the finalization of the GDPR text, see D Erdos, ‘From the Scylla of restriction to the Charbybdis of licence? exploring the scope of the “special purposes” freedom of expression shield in European Data Protection’ (2015) 52 CML Rev, 119.

61 I bracket here whether, and if so in what limited circumstances, the creation and dissemination of material for academic, artistic, and/or literary purposes may be safeguarded even if it is not orientated towards some type of indeterminate publication. Any such activity would not be akin to the journalistic expression considered by the Court to date and its potential special safeguarding has not been significantly explored in other case law.

62 GDPR, Art. 85(3).

63 Under the DPD, nine EU States explicitly safeguarded only the pursuit of journalistic purposes (or, in a few cases, just the institutional media), whilst one further State also protected artistic but not literary expression. See Erdos (n 35), 213.

64 Ibid, 256–7.
special expression regime. Indeed, in *Satamedia* (2008) the CJEU Grand Chamber clearly articulated that the ‘obligation’ of ‘reconciliation’ between rights ‘lies on the Member States’.65 The German Constitutional Court strongly emphasized this point in its recent decision on online press archiving, stressing that the reconciliation between this activity and the right to be forgotten should presumptively be analysed through the prism of national constitutional human rights.66 Nevertheless, it remains clear that this task must also be carried in full conformity with the necessity standard set down in the DPD and now, taking specific inspiration from the EU Charter, also in the GDPR. Thus, even the German Constitutional Court recognized that a focus on national constitutional rights may be displaced where there were concrete and sufficient indications that the level of protection established by the EU Charter could be undermined by this.67 It also found it possible to strongly weight new data protection considerations, including the importance of taking into account the passage of time, ultimately holding that the ordinary courts should have considered what reasonable safeguards the Press could have itself implemented to shield the data subject from nominative searches on the open internet.68 In sum, therefore, it is misleading to refer to this regime, as has been quite common, as an ‘exemption’.69 Indeed, *Satamedia* (2008) emphasized this very point by ruling that ‘the derogations and limitations in relation to the protection of data must apply only in so far as is strictly necessary’.70 Drawing on an analysis originally developed by the ECtHR under the European Convention which is recognized as a ‘gemeinsames Fundament’ (‘common foundation’)71 of fundamental rights protection across Europe, the CJEU in *Buivids* (2019) further deepened this point. In sum, it stipulated that ‘in order to balance the right to privacy and the right to freedom of expression’ the following ‘relevant criteria’ had to be taken into account:

[the] contribution to a debate of public interest, the degree of notoriety of the person affected, the subject of the news report, the prior conduct of the person concerned, the content form and consequences of the public, and the manner and circumstances in which information was obtained and its veracity.

In a novel development, the CJEU also mandated that account should also be taken of ‘the possibility of the controller to adopt measures to mitigate the extent of the interference with the right to privacy’.72 Notwithstanding the primary role of national fundamental rights, it is important and indeed likely that the CJEU

65 *Satamedia* (n 49), para 54.
66 BVerfG, 6 November 2019 docket number 1 BvG 16/13 (n 17).
67 Ibid, para. 71.
68 Ibid, para. 153.
69 See, for example, H Hijmans, ‘Right to have links removed: evidence of effective data protection’ (2014) 21 Maastricht Journal of European and Comparative Law, 555.
70 Case 73/07 *Satamedia* (2008), para. 56.
71 BVerfG, 6 November 2019 docket number 1 BvG 16/13 (n 17), para. 57.
72 *Buivids* (n 50), para. 66.
will continue to play a significant role in systematizing standards within this area under the GDPR. First, the status of the GDPR as a directly applicable Regulation should intrinsically place more weight on the need to ensure that ‘the level of protection’ is ‘equivalent in all Member States’ including, at least in broad terms, even in highly sensitive areas such as journalism. Secondly, the GDPR now explicitly requires that the exercise of journalism and other forms of special expression be reconciled with the right to the protection of personal data rather than (only) the right to privacy as is recognized in the European Convention. As Kokott and Sobotta (2013) have emphasized, data protection encompasses ‘all information on identified or identifiable persons’ and therefore has a ‘wider scope’ than the right to privacy.73 In addition, the ‘specific requirements [of default data protection] help to focus the debate on areas that are particularly susceptible to interference with [an individual’s] fundamental rights’.74 Although Kokott and Sobotta focus specifically on data protection’s fairness and purpose specification requirements, the same could be said for other default duties including, for example, as regards accuracy and data limitation. These requirements do not only protect the right to privacy (at least as narrowly conceived) but also other individual rights such as reputation, rehabilitation, and human dignity. All these rights are under unprecedented threat as a result of the digital publication and spread of content including of a journalistic (or other special expressive) nature. Therefore, whilst the pursuit of journalism and other special expression will often require a departure from the strictures of even core data protection norms, pan-EU law should oblige judicial (and, at first instance, also regulatory Data Protection Authority) processes to play a key role in articulating and further specifying the threshold of strict necessity which is applicable to derogations here.

As previously stated, the great majority of state legislatures have enacted local statutes which seek to reconcile special expression with data protection. Not least since the GDPR primarily allocates the local legislature this task and they patently have strong democratic credentials, it is clear that these bodies are granted a wide margin of appreciation here and so any resulting law must be deserving of very high respect. Nevertheless, it has been manifest since Satamedia that these local provisions must be interpreted as far as possible in line with the CJEU’s strict necessity standards. A particular problem, however, is that certain of these laws palpably and explicitly fail to adhere to these or other human rights standards. For example, four States effectively disapply substantive data protection entirely within some or all of the special expression area, thereby effectively treating the special expression provision as a full carve-out rather than a strictly limited (albeit far-reaching) derogatory regime.75 However, in Buivids (2019) the CJEU

73 J Kokott and C Sobotta, ‘The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR’ (2013) 3 International Data Privacy Law, 222, 225.
74 Ibid, 228.
75 Notably, Sweden, Germany (with minimal inclusion excluded for the institutional press where subject to self-regulation through a press council), Denmark (outside of institutional journalism
found that, even under the DPD text, the courts (and therefore presumably also Data Protection Authorities (DPAs) in the first instance) were required to ensure that the derogations in principle allowed within the special expressive clause were only applied to the extent that they satisfied a strict necessity threshold:

If it should transpire that the sole objective of the recording and publication of the video in question was the disclosure to the public of information, opinions or ideas, it is for the referring court to determine whether the exemptions or derogations provided for in Article 9 of Directive 95/46 are necessary in order to reconcile the right to privacy with the rules governing freedom of expression, and whether those exemptions and derogations are applied only in so far as is strictly necessary.  

At the other end of the spectrum, at least three States fail to provide special expression with any significant statutory safeguarding from very far-reaching and sometimes very onerous default data protection stipulations. Following the mirror logic of Buivids, the courts (and DPAs) must still ultimately grant special expression the benefit of any derogation which they consider strictly necessary to vindicate freedom of expression. A wide national margin of appreciation nevertheless remains critical here. Therefore, so long as national fundamental rights are able to ensure such a balance, the German Constitutional Court is right to hold that they may remain the principal lodestar in this special area. Nevertheless, not least given that only around half of the EU Member States explicitly recognize data protection itself as a constitutional right, the potential need for a residual application of pan-EU standards should not be lightly discarded. The case for such a residual application of the tests laid down in the GDPR is strengthened both by this instrument’s status as a directly applicable regulation and its recognition of data protection as a fundamental right. Moreover, not just the GDPR but also the EU Treaties themselves encapsulate the fundamental right to data protection and both this right and also freedom of expression are also safeguarded within the EU Charter. Under the Charter, neither of these core rights should be subject to limitation unless this is provided for by law, respects the essence of the right, is necessary and proportionate, and genuinely meets either the objectives of general interest or the need to protect the

76 Buivids (n 50), para. 68.
77 Namely, Croatia, Hungary, and Spain. See Erdos (n 35), 163.
78 J Cannataci and J Mifsud-Bonnici, ‘Data protection comes of age: The data protection clauses in the European Constitutional Treaty’ (2005) 14 Information and Communications Technology Law, 5, 8.
79 GDPR, Art. 1(2).
80 TFEU, Art. 16(2). The relevance of this provision (and the concomitant Charter right) has already been stressed by the CJEU in the Grand Chamber case of Case C-362/14 Maximillian Schrems v Data Protection Commission, ECLI:EU:C:2015:650, para. 40.
81 Charter of Fundamental Rights of the European Union, OJ 2010 C 83/389, Arts 8 and 11.
rights and freedoms of others. These broadly mirror those specified in CJEU case law to date and should remain relevant at a local level wherever there are clear indications that national legislative and constitutional provisions would themselves prove insufficient.

In conclusion, therefore, local legislative and constitutional provisions within this special area must be accorded full respect insofar as they represent a reasonable reconciliation or balance. Nevertheless, these provisions should still be interpreted in line with the strict necessity standards as specified in Satamedia and Buivids. Moreover, in cases where local provisions do not provide for reasonable reconciliation on their face, then the courts (and, subject to judicial oversight, also the DPAs) should invoke pan-EU standards to ensure that those protections (for personal data) and/or derogations (for the exercise of special expression) are nevertheless applied where strictly necessary.

IV. Personal exemption and personal expression

A great deal of the personal data circulating online originates not from institutional actors such as the professional media but has instead been initiated by natural persons operating within a purely amateur context. This personal expression includes data which does not relate only to these individuals but often also to third parties at various degrees of proximity to them. Indeed, Buivids provides a concrete example in the form of a ‘video recording in the station of the Latvian national police’ which was uploaded onto YouTube and inter alia showed ‘police officers going about their duties’. The CJEU in this confirmed that, although subject to a clearly delineated purposive test, amateur individuals were not in principle excluded from benefiting from the special expression derogation discussed immediately above. However, a prior issue arose as to whether any or even all online publication by amateur individuals would be excluded from the scope of statutory data protection entirely due to the operation of the personal or household exemption. In Buivids itself the CJEU confirmed a line of cases (stretching back to Lindqvist in 2003) which, at least if the data were thereby disseminated to an indeterminate number of persons, peremptorily ruled out such a possibility:

[S]ince Mr Buivids published the video in question on a video website on which users can send, watch and share videos, without restricting access to that video, thereby permitting access to personal data to an indefinite number of people, the processing of personal data at issue in the main proceedings does not come within the context of purely personal or household activities.

82 Ibid, Art. 52.
83 Buivids (n 50), paras 15–16.
84 Ibid, para. 43.
Related case law has also construed the personal or household exemption very narrowly. Thus, in *Ryneš* the CJEU found that an individual’s use of CCTV technology to protect his or her own home would still fall outside this exemption to the extent that such video surveillance ‘covers, even partially, a public space and is accordingly directed outwards from the private setting of the person processing the data in that manner’.\(^{85}\) Finally, a CJEU Grand Chamber ruled in *Jehovan todistajat* (2018) that data collected in the context of ‘door-to-door preaching’ by individuals within a Jehovah’s Witness congregation was similarly outside the exemption since this activity ‘was directed outwards from the private setting’\(^{86}\) and details of persons who no longer wished to be contacted were sent on to the congregation itself which was held to constitute ‘a potentially unlimited number of persons’.\(^ {87}\)

The logic of the above case law would result in this exemption being inapplicable to all but strictly private communication to a pre-defined (and presumably quite limited) number of persons for reasons which were clearly related to the personal life of that individual and/or their household. This would rule out use of the exemption not only where dissemination was to the world at large but even where it was limited to ‘friends-of-friends’ on a social networking site or a small community forum of variable membership. Given that data protection in principle imposes numerous requirements on the processing of personal data, such a rigid approach may be considered ‘excessively burdensome’.\(^ {88}\) On the other hand, a categorical exemption for amateur individuals would radically conflict with this framework’s aim of ensuring the ‘effective and complete protection of data subjects’.\(^ {89}\) Indeed, Xanthoulis correctly argues that:

> [T]he granting of a full exemption from data protection requirements to any user who uploads materials on the internet as a private individual would lead to easy circumvention of the rules and, in an age of UGC [User Generated Content], would fundamentally undermine data protection and privacy itself.\(^ {90}\)

It may, therefore, be generally preferable to tackle the resulting difficulties through the partial derogations explored elsewhere in this piece rather than through a categorical and complete exemption. In any case, the GDPR text largely maintains the previous peremptory and narrow approach by maintaining the

---

\(^{85}\) Case 212/13 *František Ryneš v Úřad pro ochranu osobních údajů*, ECLI:EU:C:2014:2428, para. 33.

\(^{86}\) Case 25/17 *Proceedings brought by Tietosuojavaltuutettu (Johovan todistajat intervening)*, ECLI:EU:C:2018:551, para. 44.

\(^{87}\) Ibid, para. 45.

\(^{88}\) B Van Alsenoy, ‘The Evolving Role of the Individual under EU Data Protection Law’ (2015) CiTiP Working Paper 23/2015, 15 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2641680>, accessed 23 March 2021.

\(^{89}\) Napoleon Xanthoulis, ‘Negotiating the EU Data protection reform: reflections on the household exemption’ in A. B. Sideridis et al. (eds), *E-Democracy, Security, Privacy and Trust in a Digital World* (Berlin: Springer, 2013), 141.
Nevertheless, the GDPR’s accompanying recital does now state that this ‘could’ include ‘social networking and online activity undertaken within the context of [purely personal or household] activities’.92 This opens up the possibility for a partial adoption of a less restrictive approach. In this regard, it is important to recognize that the CJEU has generally only stressed the need to adopt a broad construction of data protection’s scope when the relevant processing is ‘liable to infringe fundamental rights, in particular the right to privacy’.93 Given this, the GDPR’s personal exemption should be construed so as to exclude activity carried out under the direct authority and control of an amateur individual natural person so long as this does not pose a serious prima facie risk of infringing the core privacy, reputation, rehabilitation, dignity, and other rights which data protection exists to support. Since special expression generally looks to secure a high impact and visibility, the pursuit of this kind of activity would still generally not fall within the scope of the exemption even if only an amateur individual were involved. This would be particularly true of journalistic activity which, perhaps especially in its ‘citizen journalism’ guise, often seeks to act as a social ‘bloodhound’94 and can thereby inflict grave and sometimes unwarranted ‘damage on an individual’.95 In contrast, the exemption should safeguard activities linked to a general freedom of self-expression, so long as this is not itself intrusive and does not pose a significant risk to a third party data subject’s rights. At least unless explicitly objected to, such processing could cover the publication of both running text and photographic images which contained the personal data of others but could reasonably be considered to be innocuous.96 In contrast, other types of individual expression which included third-party personal data would still fall to be assessed under either the special expression regime (if it constituted a bona fide message of information, opinions, or ideas directed at the collective public) or (alongside many other expressive activities) the regime for broad expression which is explored in Section V.

91 GDPR, art. 2(2)(c) (emphasis added).
92 Ibid, recital 18.
93 Rynesi (n 85), para. 29.
94 Reynolds v Times Newspapers [2001] 2 AC 127, 205 (Lord Nicholls).
95 UK, House of Lords, European Communities Committee, Protection of Personal Data HL 75 (1993), 39.
96 Following reasonable notice of an objection, it would be necessary to redetermine in light of all the evidence that the dissemination was indeed reasonably innocuous or was otherwise justified under either the special expression derogation or the broad expression regime.
V. Broad expression: Scope and (ideal and actual) legislative regime

A. Scope of broad expression

Many forms of third-party personal data publication by amateur individuals are manifestly of a kind which may pose a significant risk to another individual’s rights. Examples include the posting of a clearly negative evaluation concerning another natural person (whether acting in their public or, still more so, private capacity), the disclosure of clearly private and personal details of other non-public figures in, say, an online blog and the incessant and focused observation even of public activity which may well be experienced as a potentially unwarranted form of surveillance. Moreover, notwithstanding that they may be disseminated to the world at large, all this activity will generally be conducted for significantly more privatized purposes than those safeguarded within the special expression regime. Thus, Daphne Kellner correctly notes that:

A tweet about a dishonest car mechanic, a Yelp review of a botched medical procedure, or a post criticizing an individual Etsy or Amazon vendor . . . appears to be a far cry from the privileged—and often professionalized and even licensed—categories of expression listed in Article 85(2).97

Moreover, these types of broad expressive activity have become very common. Indeed, writing back in 2007, Solove stated:

Increasingly, people are exposing personal information about themselves and others online. We can now readily capture information and images wherever we go, and we can then share them with the world at the click of a mouse. Somebody you’ve never met can snap your photo and post it on the Internet. Or somebody that you know very well can share your cherished secrets with the entire planet.98

Subsequent socio-technological developments including ever more powerful mobile ‘phones’ and the rise of micro-blogging platforms such as Twitter have significantly accelerated these trends. However, although Solove’s described examples are generally invidious, more reasonable kinds of self-expression online can legitimately further important human values including the ‘right to identity and personal development’.99 Furthermore, rating websites concerning public-facing individuals including, for example, car mechanics and doctors not only enable an individual to express an opinion about matters of importance to them but have also become a crucial way in which potentially very valuable

97 D Keller, ‘The right tools: Europe’s intermediary liability laws and the EU 2016 General Data Protection Regulation’ (2017) 33 Berkeley Technology Law Journal, 287, 342.
98 D Solove, The Future of Reputation: Gossip, Rumor, and Privacy on the Internet (New Haven, CT: Yale University Press, 2007), 2.
99 F.G. and J. H. v United Kingdom 45 EHRR 51 (2001). To date, European jurisprudence has engaged with these values in the context of protecting private life. However, especially in a digital age, they also seem relevant in a freedom of expression setting.
information is distributed to other natural persons who are seeking out commercial, educational, social, and many other sorts of service and experience. This kind of processing thereby touches on distinctly valuable aspects of freedom of expression, which includes the ‘right to receive and impart information and ideas without interference’, and thereby raise issues which go beyond the ubiquitous and endemic tension between data protection control and the unbridled distribution and manipulation of information. It is precisely this kind of activity which should be governed under the broader safeguarding of freedom of expression set out in Article 85(1) of the GDPR. The same is clearly true of the activities of search engines and other online services such as Facebook and Twitter which promote, aggregate, organize, and enable the ready retrieval of a very wide range of material including personal data for a broad range of purposes. As explored above, the CJEU in Google Spain was very clear that such activity could not be assimilated within the special expression regime. However, through facilitating a whole range of expressive activity including self-expression and special expression, these activities also engage distinctly important aspects of the right to freedom of expression. Indeed, in the subsequent case of GC et al. v CNIL, the CJEU has clarified that at least search engine indexing can be ‘necessary for exercising the right of freedom of information of internet users’ and that this is ‘a right protected by Article 11 of the Charter’. Article 85(1) of the GDPR is clearly inspired by Article 11 of the Charter and, like the latter instrument, explicitly emphasizes not only freedom of expression in general but also its specific sub-right, the freedom of information. It is, therefore, clear that all these kinds of activities fall within these broad freedom of expression protections. The following sub-sections explore the complex legislative questions which thereby arise concerning how such activities are and should be substantively governed under the GDPR.

B. Ideal (legislative) shape of broad expression regime

Article 85(1) baldly states that ‘Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information’. Individual States, rather than the Union itself, are clearly the direct recipients of this instruction. It is, therefore, somewhat inaccurate to state, as the German Constitutional Court did at least as regards search engines in its recent Right to be Forgotten II ruling, that this area is ‘vollständig vereinheitlichten’ (‘fully harmonized’). Indeed, this point was in fact recognized during the course of the CJEU recent Grand Chamber judgment of Google v CNIL (2019):

100 Charter of Fundamental Rights of the European Union, Art. 11.
101 GC et al. v CNIL (n 15), para. 66.
102 The CJEU has confirmed this point in Google v CNIL (n 16), para. 67.
103 BVerfG, 6 November 2019 docket number 1 BvG 276/17, para. 77.
[T]he interest of the public in accessing information may, even within the Union, vary from one Member State to another, meaning that the result of weighing up that interest, on the one hand, and a data subject's rights to privacy and the protection of personal data, on the other, is not necessarily the same for all the Member States, especially since, under ... Article 85 of Regulation 2016/679, it is for the Member States ... to provide for the exemptions and derogations necessary to reconcile those rights with, inter alia, the freedom of information. 104

Nevertheless, in contrast to the special purposes regime set out in Article 85(2) and Article 85(3), the clause does not set out any specific *vires* to enable this instruction to be discharged and there is likewise no obligation to notify the European Commission of any action taken. The broad pursuit of freedom of expression and information is only explicitly referred to in one other GDPR provision, namely, Article 17(3)(a) which disapplies the right to erasure and to be forgotten 'to the extent the processing is necessary for exercising the right of freedom of expression and information'. The exercise of other data subject rights including rectification, restriction and objection are not directly affected by this. 105 Compared with special expression, this less permissive treatment of broad freedom of expression (including its sub-right, the freedom of information) reflects the fact that these activities do not directly further the same high social purposes as special expression but are still capable of triggering comparable risks for data protection rights. The distinction made between special expression and these other types of freedom of expression is also a manifest and deliberate legislative choice. 106 Likewise, the final wording of Article 85(1) is clear that such expression remains within the scope of the GDPR and that it is, therefore, the responsibility of the Member States to legislate any derogations from this as are necessary. 107

Putting these various deductions together, the GDPR appears to require Member States to deploy the GDPR’s standard derogation clauses in order to

104 Google v CNIL (n 16), para. 67.
105 See GDPR, Arts 16, 18, and 21.
106 The European Parliament’s version of the GDPR would have made no such distinction, although its understanding of freedom of expression (as set out in an accompanying recital) may have been essentially confined to special expression in any case. See Art. 80(1) and recital 121 of the European Parliament text in General Data Protection Regulation Four Column Table (n.d.) <http://www.europarl.europa.eu/cmsdata/99508/3_4column_table_EN.docx>, accessed 23 March 2021.
107 The European Council’s version of the GDPR would have rendered both these points less clear by stating that ‘[t]he national law of the Member State shall reconcile protection of personal data pursuant to this Regulation with the right to freedom of expression and information’ (Art. 80(1) of the European Council text in ibid). Related to this, at least four national delegations had argued that the balance between data protection and freedom of expression (potentially even within the area of special expression) should be struck by the courts rather than the legislature. However, with the exception of Spain, these delegations did not clarify whether such judicial empowerment would at least require legislative authorization. See EU Council Document 14098/1/14 REV 1 (20 October 2014) (reporting stance of the Spanish and Slovak delegations) and 14270/1/14 REV 1 (24 October 2014) (reporting viewpoint of Belgium and UK delegations).
effect a reconciliation here. As outlined in Section II.B above, these clauses provide a comprehensive blueprint for derogations from the data protection principles, transparency and control rules, and the legality conditions especially as regards sensitive data. In sum, the general test for a derogation is laid down in the Article 23 ‘restrictions’ clause, although slightly different sensitive data tests are set out for criminal-related data and special data (eg concerning health) in Articles 10 and Article 9(1)(g) respectively. It follows that with reference to such core substantive aspects, the relevant derogatory clauses should be invoked and applied. Unfortunately, however, these provisions leave completely unaddressed the potential need for derogations from the myriad of GDPR integrity provisions including as this concerns the documentation and formalized assessment of processing, joint controller and/or processor agreements, and provisions on the international transfer of data outside Europe. The vast majority of these highly complex provisions are rule-based and so can lack the flexibility required for contextual application, as may be necessary when ensuring a balance with broad expression even as overseen by companies or other legal persons. Moreover, at least when it concerns individual activity, the need for further derogations was voiced (though not resolved) during the GDPR negotiations. For example, the Belgium delegation expressed concern that the ‘the rules of the GDPR are too complicated for the individual persons’, whilst the German delegation stated that ‘to what extent data protection rules should apply to private persons, the German delegation thinks that in these cases the obligations for private persons as controllers should be strictly limited’. More concretely, the Austrian delegation proposed a recital stating that ‘[g]iven the limited or inexistent influence of users on the design of social networking services or other forms of cloud based services[, ] personal and household activities potentially adversely affecting legitimate interests of data subjects shall only be subject to obligations resulting from’ the data protection principles, data subject consent (insofar as relevant), the special data rules, the right to rectification, the right to erasure and to be forgotten, and the right to object. The subsidiary nature of the integrity rules within the GDPR framework as a whole must also be taken into account. In sum, rules related to documentation, assessment, and even international data transfer have no intrinsic value but rather are designed to be proportionate measures which undergird and support core substantive duties. Given that a significant restriction

---

108 GDPR, Art. 30 and Art. 35 (noting especially the peremptory lists of processing subject to mandatory assessment drawn up under Art. 35(4)).
109 Ibid, Arts 26 and 28.
110 Ibid, Arts 44–49.
111 An exception may be the international data transfer provisions which do enable (albeit essentially as a last resort) for transfers to take place where necessary inter alia for ‘important reasons of public interest’ (GDPR, Art. 49(1)(d)).
112 EU Council Document 8372/15 (30 April 2015).
113 EU Council Document 12267/2/14 REV 2 (2 September 2014).
114 EU Council Document 14784/14 (28 October 2014).
of the latter has been explicitly recognized to be potentially necessary, then it is highly likely that some limitation on the rigours of the related integrity provisions may also be similarly justified. Finally, and most importantly, there is an overriding need to vindicate fundamental rights within primary law, even if this comes into conflict with secondary legislation. Article 11 of the EU Charter (as well as the European Convention and, often through somewhat different phraseology, most national constitutions) protects freedom of expression including the ‘freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers’. Although the codification of law in the GDPR must be accorded high jurisprudential respect, it has ultimately to give way to these higher imperatives. Taking into account all of these factors, derogations from the integrity rules should be permitted under the same conditions as set out Article 23, the GDPR’s general restrictions clause. Moreover, as a result of the instruction set down in Article 85(1), the enactment of such necessary derogations must also be considered mandatory in the area of broad expression.

It follows that, whilst ensuring respect for ‘the essence of the fundamental rights and freedoms’, Member States should legislate ‘necessary and proportionate’ derogations to safeguard these broad types of freedom of expression (which are encompassed within ‘the rights and freedoms of others’). However, there should be no limitation on the need for an ordinary legal ground for processing and the data protection principles must likewise only be restricted insofar as their ‘provisions correspond to the rights and obligations’ set out in the detailed rules on data subject transparency and control.119 Under the derogatory tests set out in Article 23, there also remains a general expectation that the Member State derogations which are adopted will be as specific as possible including as to ‘the safeguards to prevent abuse’ and ‘the risks to the rights and freedoms of data subjects’. Turning finally to the sensitive data rules, Member States must instead ensure that any derogations are, as regards criminal-related data, subject to ‘appropriate safeguards’ and, vis-à-vis the other so-called special categories, ‘necessary for reasons of substantial public interest’, ‘proportionate to the aim pursued’, ‘respect[ful] [of] the essence of the right to data protection’ and that they ‘provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject’.

These conditions must be interpreted with full respect for both the fundamental right to freedom of expression and the limited competence of the European

115 GDPR, Art. 23(1)(i).
116 Ibid, Art. 7.
117 Ibid, Art. 6.
118 Ibid, Art. 23.
119 Ibid, Arts 12-22.
120 Ibid Art. 23 (2).
121 Ibid, Art. 10.
122 Ibid, Art. 9(1)(g).
Union in this context. Ultimately, therefore, Member States retain a substantial margin for manoeuvre even in this broad expressive area. A number of different options are, therefore, possible. For example, subject to providing clear and effective redress mechanisms for data subjects if things go wrong, they could decide to set down these broad conditions in statute and leave it to the judiciary to apply them on a case-by-case basis. Alternatively, they could consider that certain provisions such as the right to erasure and to be forgotten require no further restriction and so no derogation is necessary. Finally, they could instead explicitly subject different types of broad expressive actor to divergent treatment. For example, subject again to the provision of effective redress, amateur individuals and other small-scale publishers might be awarded the benefit of all possible derogations here. On the other hand, commercial-scale operations such as an evaluation or rating website might be made subject to considerably wider duties including, for example, a duty to assess likely high-risk processing through structured impact assessments and to formally document processing activity. Indeed, German DPAs have mandated that controllers engaged in the ‘[o]peration of rating portals’ must—so long as their processing is ‘[l]arge-scale’—always undertake a data protection impact assessment (DPIA) under article 35, albeit using powers of regulatory rule-making under article 35(4) of the GDPR rather than invoking statutory provisions adopted through the legislature. Other European DPAs have not explicitly set out a similar mandatory requirement.

Whichever national schemes are adopted, it is important to recognize that (in contrast to special expression) the ‘core’ substance found in the legal grounds for processing and the data protection principles must always continue to play a role within broad expression. At least in outline, these aspects have indeed been ‘fully harmonized’ as a result of the GDPR. Thus, absent data subject consent, the legal grounds requirement requires controllers to ensure that their processing is ‘necessary for the purposes of the legitimate interests’ being pursued and that these are not ‘overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data’. Alongside this balancing test, the data protection principles set out applicable standards as regards

---

123 Ibid, Art. 17.
124 Ibid, Art. 21.
125 Ibid, Art. 35.
126 Ibid, Art. 30.
127 Datenschutzkonferenz, List of Processing Activities for which a DPIA is to be carried out, Europa.eu (n.d.), <https://edpb.europa.eu/sites/edpb/files/decisions/20181017_ah_dpia_list_1_1_germany_en.pdf> accessed 21 March 2021.
128 These other lists may be consulted at European Data Protection Board, Register for Decisions taken by Supervisory Authorities and Courts on Issues Handled in the Consistency Mechanism, Europa.eu (n.d.), <https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions_en> accessed 21 March 2021.
129 GDPR, Art. 6(1)(a).
130 Ibid, Art. 6(1)(f).
fairness, lawfulness, transparency, purpose limitation, data and storage limitation, accuracy, and integrity including confidentiality. Nevertheless, these latter provisions do need to be interpreted contextually and with full regard for freedom of expression. Partially confirming the approach of the German Constitutional Court in Right to be Forgotten II, it is correct that any such interpretation specifically related to these standards must be ultimately guided by freedom of expression, privacy, and data protection rights specified in the EU Charter and perhaps not those set out in national constitutions. Certainly, and as discussed further in relation to GC et al. v CNIL (2019) in sub-section VI.A below, the CJEU has drawn extensively on EU Charter rights when interpreting European data protection provisions in the area of broad expression. To be more specific regarding what sort of interpretation would ultimately be appropriate:

- The requirement for fair and balanced processing should control or prohibit expressive processing which impacts upon the data subject in a disproportionate or unreasonable manner but should not further restrict an individual publisher’s right to present their own viewpoint.
- The transparency principle should not always require a proactive disclosure of processing similar to the GDPR’s related transparency rules but must exclude truly deceptive or covert data collection and/or a lack of general openness following a data subject’s positive request for this.
- The purpose limitation principle certainly should not mandate that an expressive purpose actually be written down but the expressive nature of the purpose must nevertheless be clear and processing must remain consistent with this.

131 Ibid, Art. 5(1).
132 BVerfG, Nov. 6 2019, docket number 1 BvG 276/17 (n 103).
133 See also Google Spain (n 5) and Google v CNIL (n 15). This focus on the EU Charter also makes sense of the CJEU’s understanding that in cross-border broad expressions cases with significant impacts on data subjects beyond a single Member State it must be possible in a regulatory context for the GDPR’s consistency mechanism to be used to ensure a joint pan-European DPA enforcement decision. Any such decision would necessarily have to draw primarily on the EU Charter in a fundamental rights context. See Google v CNIL (n 15), paras 68–69.
134 Ibid, Art. 5(1)(a).
135 Ibid, Art. 6(1)(f).
136 Ibid, Art. 5(1)(a).
137 Ibid, arts 13–14.
138 Ibid, Art. 5(1)(b).
139 In requiring that any purpose be ‘explicit’, the English version of the principle might suggest otherwise. However, as the Article 29 Working Party has pointed out, other language versions of this principle (which are identical in both the GDPR and the former DPD) use wording (eg ‘eindeutig’ in German and ‘egyértelmű’ in Hungarian) that only require any purpose to be clear or unambiguous rather than necessarily written down. See Article 29 Working Party ‘Opinion 03/2013 on Purpose Limitation’ (Europa.eu, 2 April 2013) 17 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> accessed 23 March 2021.
140 Thus, once such data is clearly repurposed—for example, through the results of a rating website evaluation being entered into an employment record—then it would need to be subject to the general data protection provisions rather than those applicable to broad expression.
Data limitation/minimization (both in general\textsuperscript{141} and over time\textsuperscript{142}) should grant individual actors a considerable margin of discretion as to which information they consider relevant to their expressive purpose but must prohibit the publication of clearly excessive amounts of third party personal data, especially after objection from the data subject.

The accuracy principle\textsuperscript{143} should fix controllers with a duty of care to ensure that the overall effect of any publication of data is not significantly false or misleading,\textsuperscript{144} whilst still respecting the right of any individual expressive actor to express their own viewpoint and the general right of access to the historical record.

Although the integrity and confidentiality principle\textsuperscript{145} should not mirror the detailed integrity rules set down in relation to such matters as impact assessments\textsuperscript{146} and international data transfer,\textsuperscript{147} it should require the controller to take all reasonable steps to secure any confidential data, to comply with relevant substantive standards and to refrain any action aimed at their deliberate circumvention (as may arise \textit{inter alia} through an international transfer of data).

C. Current legislative shape of the broad expression regime

In significant contrast to special expression, the current governance of broad expression is complicated by the general absence of specific derogatory schemes at Member State level. Indeed, an analysis of local legislation indicates that twenty-one States (or almost 80 per cent of the EU) have not adopted any derogation expressly related to broad expression.\textsuperscript{148} Moreover, judged by reference to the construction of Article 85(1) presented above, the provisions adopted in the six States which have legislated are (at least somewhat) problematic. In sum, as outlined in Table 1, one state (Sweden\textsuperscript{149}) has sought to ensure that all activity

\textsuperscript{141} GDPR, Art. 5(1)(c).
\textsuperscript{142} Ibid, Art. 5(1)(e).
\textsuperscript{143} Ibid, Art. 5(1)(d).
\textsuperscript{144} Thus, in a search engine context, significant inaccuracy which significantly impacts an individual’s enjoyment of data protection and whose ready circulation cannot be clearly linked to a specific freedom of information interest should probably be delisted. In other cases, however, accuracy problems might be resolved by ensuring that the most prominent results are accurate and the overall listing does not present a misleading picture of the individual as a whole. See \textit{mutatis mutandis} GC \textit{et al v CNIL} (n 15), para. 78 (coming to a cognate solution as regards the timeliness of information).
\textsuperscript{145} Ibid, Art. 5(1)(f).
\textsuperscript{146} Ibid, Art. 35.
\textsuperscript{147} Ibid, Arts 44–49.
\textsuperscript{148} Relevant legislation (in authoritative English translation where available) is set out at Centre for Intellectual Property and Information Law, \textit{European Data Protection—National Laws: Current and Historic}, (n.d.), <https://www.cipil.law.cam.ac.uk/resources/european-data-protection-national-laws-current-and-historic> accessed 23 March 2021.
\textsuperscript{149} Sweden, Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, § 7.
covered by its Law on Freedom of Expression is granted an absolute exemption from data protection. This rule of precedence is even in conflict with the standard of strict and necessary rights balancing required in the area of special expression. Although this law’s registration and other formality requirements may make it of little general use to amateur individuals, its substantive protection of all forms of public ‘database’ render it potential applicability to most forms of broad expression carried out in a corporate context and even some activities which would fail to meet the broad expression threshold. Meanwhile, four

| State      | Details of broad expression substantive derogations |
|------------|---------------------------------------------------|
| Denmark    | Expressly states that the GDPR does not apply where it would be contrary to Article 10 of the ECHR or Article 11 of the EU Charter. |
| Greece     | Fused with special expression, provides substantive exemption as necessary to reconcile data protection with freedom of expression and information from all but purpose limitation principle, general security duties, and requirements to bind processors and others acting on a controller’s behalf. |
| Ireland    | Fused with special expression, provides substantive exemption from all but integrity and confidentiality principle where, having regard to the importance of freedom of expression and information in a democratic society, compliance would be incompatible with exercise/purposes. Specifically stated that these rights shall be interpreted in a broad manner. DPA may refer questions of law to the courts. |
| Malta      | Fused with special expression, provides substantive exemption from all but sensitive data rules (other than criminal data) and international data transfer provisions where, having regard to the importance of freedom of expression and information in a democratic society, compliance would be incompatible with the exercise of freedom of expression and information and the controller ensures processing is proportionate, necessary, and justified for reasons of substantial public interest. |
| Portugal   | Fused with special expression, states that GDPR does not prejudice the exercise of freedom of expression and information but that, especially as regards sensitive (including criminal-related) data, freedom of information must respect human dignity and personality rights protected in the Portuguese law and that this provision does not legitimize disclosure of personal data such as address and contact information unless widely known already. |
| Sweden     | States that GDPR does not apply to the extent that it would be contrary to the Swedish Freedom of Expression Act. |

150 Broadly defined as ‘collection[s] of information stored for automatic data processing’ (Sweden, Freedom of Expression Act, Art. 1).

151 Indeed, this law has been successfully invoked to justify the publication of information such as detailed credit reports. The Swedish DPA recently successfully fined one such website for various forms of publication which fell outside of the publishing certificate granted to it under this law. See European Data Protection Board, ‘Administrative Fine of 35 000 EUR Imposed on the Swedish
States (Greece, Ireland, Malta, and Portugal) incorrectly fuse the safeguarding of broad expression with that of special expression, thereby leading inter alia to the clear risk that the continued application of core aspects of data protection within the former area may be overlooked. Nevertheless, with the partial exception of the Portuguese derogation, all these laws do include an open-textured test which can be contextually interpreted depending on whether special or broad expression is at issue. Finally, Danish law confines itself to stating that the freedom of expression as set down in the EU Charter and European Convention must take precedence over the GDPR. Although helpful to state formally, this principle merely restates the accepted legal hierarchy between European primary and secondary law and so cannot provide the sort of specificity that is required in this area.

VI. Broad expression: Case law and future treatment

A. CJEU approach in GC et al. v CNIL (2019)

In the general absence of relevant statutory provisions at Member State level, the CJEU has been required to directly construct derogations from the substantive law through its own case law. By far the most important judgment in this context is GC et al. v CNIL (2019). Following on from the seminal judgment of Google Spain (2014), this reference was sent from the French Conseil d’État and also concerned search engine indexing, a quintessential broad expression activity. The case focused on whether and, if so, what derogation a search engine could benefit from in relation to the sensitive data rules and also how it should handle the indexing of data which had become out of date and, therefore, potentially in violation of inter alia the relevance, adequacy, and necessity aspects of data minimization. Since the latter specifically concerned the continued circulation of information related to past criminal proceedings which ‘no longer correspond[ed] to the [data subject’s] current situation’, a partial link was established between these twin dilemmas. Although the Conseil d’État had originally lodged its questions at a time when the Data Protection Directive 95/46 was still in force, the CJEU Grand Chamber recognized that ‘in order to ensure that its answers will in any event be of use to the referring court’ it would need also to

152 Greece, Law 4624/2019, s. 28.
153 Ireland, Data Protection Act 2018, s. 43.
154 Malta, Data Protection Act 2018, s. 9.
155 Portugal, Lei no 58/2019—Lei de execução do RGPD, Art. 24.
156 Denmark, Data Protection Act 502/2018, s. 3(1).
157 GC et al. v CNIL (n 15), para. 71.
158 Ibid, para. 33.
consider these questions from the perspective of the GDPR. In light of the focus of this article, it will be that aspect of the Court’s analysis which will be explored.

Turning to consider the direct substantive interface with the sensitive data rules, the Court’s starting point was to stress that these applied both ‘to every kind of processing’ of such data and ‘to all controllers carrying out such processing’. An ‘enhanced protection’ of this data was necessary as its processing was liable to constitute ‘a particularly serious interference with the fundamental rights to privacy and the protection of personal data guaranteed by Article 7 [respect for private and family life] and Article 8 [protection of personal data].’ For much the same reason, a narrow interpretation of ‘data relating to “offences” and “criminal convictions”’ (criminal-related data) was rejected, such that criminal-related data encompassed ‘information relating to legal proceedings brought against an individual, such as information relating to the judicial investigation and the trial . . . regardless of whether or not, in the course of those legal proceedings, the offence for which the individual was prosecuted was shown to have been committed.’ Looking first at the other so-called special data categories, the Court explored whether certain default liftings of the general prohibition on processing might have applicability to search engine indexing. Although the relevance of the lifting based on data subject ‘consent’ was rejected, the Court accepted that a search engine could itself make use of a default provision which authorizes processing where ‘the data in question are manifestly made public by the data subject’. Nevertheless, it implicitly acknowledged that a wide range of processing operations would, in principle, still remain within the general peremptory prohibition and that no legislation at the Member State level had sought to displace this. In that context, it argued that a search engine receiving a deindexing request should directly rely on a provision which enables Member

159 Ibid, para. 42.
160 Ibid, para. 44.
161 Ibid, para. 72.
162 GDPR, art 9(2)(a).
163 See GC et al. v CNIL (n 15), para. 62.
164 GDPR, Art. 9(2)(e).
165 Exactly which processing remains in principle prohibited is somewhat opaque. Clearly any special data which were not published by the data subject through a manifest and purposive act would still be fully protected. In addition, the use of the present tense in the phrase ‘are manifestly made public’ appears to purposively exclude situations where a data subject published data (eg through an injudicious public social networking post) but has then taken active steps to reassert their privacy (eg by, for example, deleting this post), at least where a sufficient time has elapsed such that the initial publication can reasonably be considered to be in the past.
166 It is beyond the scope of this article to examine why the controller duties of a search engines has essentially been limited to taking action to bring name-based (and perhaps certain other) searches into conformity with data protection following a specific request from the data subject. The justifiability or otherwise of these limitations relates not to the substantive nature of the data protections standards but rather to the allocation of responsibility to and between various online operators.
States\textsuperscript{167} (rather than controllers) to establish specific derogations on the grounds of ‘substantial public interest’:

\[ \text{T} \text{he [search engine] operator must, on the basis of all the relevant factors of the particular case and taking into account the seriousness of the interference with the fundamental rights to privacy and protection of personal data laid down in Articles 7 and 8 of the Charter, ascertain, having regard to the reasons of substantial public interest referred to in . . . Article 9(2)(g) of Regulation 2016/679 and, in compliance with the conditions laid down in those provisions, whether the inclusion of the link in the list of results displayed following a search on the basis of the data subject’s name is strictly necessary for protecting the freedom of information of internet users potentially interested in accessing that web page by means of such a search, protected by Article 11 of the Charter.}\textsuperscript{168}

Looking next at criminal-related data rules, the CJEU was required to construe a provision which prohibited processing not ‘under the control of official authority’ except ‘when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects’.\textsuperscript{169} Despite being unable to point to any specific law authorizing search engine processing, the Court held that indexing may, by virtue of those provisions and subject to compliance with the other conditions of lawfulness laid down by that directive [sic], be lawful in particular if appropriate and specific guarantees are provided for by national law, which may be the case where the information in question has been disclosed to the public by the public authorities in compliance with the applicable national law.\textsuperscript{170}

The Court indicated that, in any case, the substantial public interest derogatory provision set out in relation to the other sensitive data categories above could similarly be directly applied to legitimize the ongoing processing of criminal-related data.\textsuperscript{171}

Turning finally to the ongoing dissemination by a search engine of criminal-related data which ‘no longer corresponds to [the data subject’s] current situation’,\textsuperscript{172} the Court recognized that a serious tension with the data protections principles arose since

\textsuperscript{167} According to Article 9(2)(g) of the GDPR itself, such a specific law may also be adopted by the Union itself. However, in light of the specification in Art. 85(1) that it is for Member States to reconcile data protection with freedom of expression (and information), the adoption of such a law at Union level would clearly raise complex questions concerning legal competence.

\textsuperscript{168} GC et al. v CNIL (n 15), para. 68.

\textsuperscript{169} GDPR, Art. 10.

\textsuperscript{170} GC et al. v CNIL (n 15), para. 73. Notwithstanding the reference only to the former directive, the context of this statement suggests it was intended also to extend to the GDPR. Nevertheless, the referencing only of the directive may be telling since it included rather more open language here, permitting processing if suitable safeguards are provided under national law, subject to derogations which may be granted by the Member States under national provisions providing suitable specific safeguards (DPD, Art. 8(5)).

\textsuperscript{171} GC et al. v CNIL (n 15), para. 75.

\textsuperscript{172} Ibid, para. 71.
it follows from the requirements laid down ... in Article 5(1)(c) to (e) of Regulation 2016/679, that even initially lawful processing of accurate data may over time become incompatible with the ... regulation where those data are no longer necessary in light of the purposes of which they were collected or processed. That is so in particular where they appear to be inadequate, irrelevant or no longer relevant or excessive in relation to the purposes and in light of the time that has elapsed.\textsuperscript{173}

Nevertheless, the Court indicated that, insofar as processing remained ‘strictly necessary for reconciling the data subject’s right to privacy and protection of personal data with the freedom of information of potentially interested internet users’,\textsuperscript{174} the same substantial public interest derogatory provision could also be directly invoked here.\textsuperscript{175} However, the use of this derogation could not entail the data protection principles ceasing to have any relevance. On the contrary, the Court stated that even where full de-referencing of such out-of-date information was not justified, the search engine operator was

in any event required, at the latest on occasion of the request for de-referencing, to adjust the list of results in such a way that the overall picture it gives the internet user reflects the current legal position, which means in particular that links to web pages containing information on that point must appear in first place on the list.\textsuperscript{176}

B. Future shape of the broad expression regime

It has been argued in Section V.B above that a full and proper implementation of the broad expression regime would require each Member State to adopt its own legislative reconciliation, whilst adhering to both core substantive elements and common derogatory tests which the GDPR clearly and explicitly seeks to maintain. \textit{GC et al. v CNIL} should not be read as prohibiting such a possibility. On the contrary, the CJEU’s repeated reference to a search engine acting ‘in compliance with the conditions laid down in [the derogatory] provisions’\textsuperscript{177} is quite compatible with Member States further delineating and specifying these in local law. However, it must be recognized that the widespread adoption of such local law is, at least in the short term, not realistic. As established in Section V.C, twenty-one, or almost 80 per cent, of the Member States have failed to explicitly legislate on this topic at all. Moreover, given that all but one state\textsuperscript{178} has now enacted local provisions designed to implement the GDPR, further immediate legislative intervention generally appears unlikely. Nevertheless, thought must still be given to the impact of the (albeit somewhat unclear) legislative provisions

\textsuperscript{173} Ibid, para. 75.
\textsuperscript{174} Ibid, para. 78.
\textsuperscript{175} Ibid, para. 75.
\textsuperscript{176} Ibid, para. 79.
\textsuperscript{177} Ibid, paras 66, 68, and 75.
\textsuperscript{178} Three years on from the GDPR applying, Slovenia has yet to enact any legislation designed to implement those aspects which require national action.
which have been adopted in the six States specified in Table 1. Looking first at the Danish provision, the wording here is so general that it can probably do little beyond provide extra reassurance that some reconciliation between data protection and broad expression must be found. The potential role of the provisions in Greece, Ireland, Malta, and Portugal are more complex. In light of the hierarchy of norms embedded in EU membership itself, these provisions should not be construed in a way which would disapply the mandatory structure of the broad expression regime as set down in EU law itself and elucidated in conformity with pan-European rights standards discussed in Section IV.B above. In particular, the data protection principles and the legal grounds for processing must continue to play a strong role here. That said, as regards those derogations which are potentially applicable, the controller should be able rely on a presumption of legality so long as they adhere to the derogatory standards set down in national law. Nevertheless, in line with the EU principle of indirect effect, those standards should be interpreted in a way which is as consistent as possible with pan-EU standards. Thus, to take a relevant example, a Greek broad expression controller departing from the special data rules should only be required to demonstrate that any departure from the special data rules was ‘[t]o the extent necessary to reconcile data protection with the right to freedom of expression and information’.\textsuperscript{179} However, as far as possible, the notion of necessity here should be read as compatibility not only with the \textit{EU Charter} but also with the proportionality and safeguarding measures set down in Article 9(2)(g) of the GDPR itself. The legislation adopted in Sweden poses even greater difficulties. This purports to grant vast swathes of broad expression (and potentially even processing which would fail to satisfy the broad expression threshold) a complete exemption from all data protection standards. This is clearly inconsistent with pan-EU norms to which Sweden is bound to grant a priority as a result of EU membership. To the extent of the manifest inconsistency, it must therefore be disapplied. However, Swedish controllers should not only still be able to benefit from all the derogations permitted by EU law, but any interpretation of the relevant standards should take into account the strong priority granted to freedom of expression by the Swedish legislature. Turning finally to look at the great majority of States where no \textit{sui generis} and express legislative derogation has been enacted, the CJEU was correct in \textit{GC et al. v CNIL} to recognize that a balance between data protection and freedom of expression must still be found. However, in order to respect the apparent legislative choice as reflected in the formal law, the need for a reconciliation with freedom of expression should be construed strictly and only the minimum necessary derogations be provided for.

The pan-EU nature of the broad expression regime must ultimately be expounded through CJEU (and other) case law. In this regard, \textit{GC et al. v CNIL}\textsuperscript{179}
is clearly an important starting point. Nevertheless, certain elements of it lack conceptual clarity and there is also a need for considerably more elucidation of relevant standards. Looking first at the initial issue, the emphasis placed on the GDPR’s substantial public interest derogatory clause throughout the judgment appears particularly problematic. It might be tempting to read this as an endorsement of an understanding that the sensitive data rules are *lex specialis* and so may replace other legal provisions when sensitive data is being processed. However, although the substantial public interest derogation is of relevance to the lifting of the prohibition of processing so-called special data, it has no application whatsoever in relation to the other sensitive category, namely, criminal-related data. This is governed by its own rules which state that the prohibition here—which is limited to private sector processing—may be lifted when ‘authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects’. Contrary to the Court’s suggestion, it does not appear very logical to claim that the mere release of criminal-related data by public authorities necessarily authorizes its processing by, for example, a search engine. Nevertheless, given that this service furthers freedom of expression (and, in particular, its sub-right freedom of information) as protected by Article 11 of the EU Charter (and also national constitutional instruments), it is reasonable to argue that (in the absence of specific legislation) these instruments can themselves authorize a search engine engaging in an appropriately balanced and safeguarded processing of such data. Indeed, such a claim would appear no more strained than the CJEU’s own finding that the substantial public interest derogatory clause could and should be construed to be self-executing and, thereby, capable in and of itself of lifting the prohibition on processing special category data.

Looking beyond the sensitive data rules themselves, it is vital to recognize that a *lex specialis* understanding of the sensitive data regime is conclusively and expressly rejected in the GDPR. In sum, recital 51 states:

> Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection. ... In addition to the specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Therefore, any limitation of these other principles and rules must find their own separate grounding. In this regard, the relevant GDPR provision is in fact Article 23(1) which authorizes restrictions through a ‘legislative measure’ which ‘respects the essence of the fundamental rights and freedoms and is a necessary and

---

180 GDPR, Art. 9(1)(g).
181 For a sympathetic but nuanced analysis of this claim see Article 29 Working Party, ‘Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC’ (Europa.eu 2014), 14–15 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf>, accessed 23 March 2021.
182 GDPR, Art. 10.
183 *GC et al. v CNIL* (n 15), para. 73.
proportionate measure in a democratic society’ to safeguard *inter alia* ‘the rights and freedoms of others’. Through a pathway which takes in Article 13 of the Data Protection Directive 95/46 and Article 8 of the Data Protection Convention, this clause is modelled on the limitations to the qualified rights found in the European Convention on Human Rights\(^{184}\) and Article 52(1) of the *EU Charter*. It is, therefore, the most overarching embodiment of an understanding that ‘[t]he right to the protection of data is not an absolute right’ but ‘must be considered in relation to its function in society and be balanced with other fundamental rights, in accordance with the principle of proportionality’.\(^{185}\) Given this, it is also the most appropriate clause to draw on in relation to the various integrity provisions, such as data processing record-keeping,\(^{186}\) which are not expressly within the scope of either this or any other GDPR derogatory clause. Even more manifestly, it is clearly directly applicable to core substantive provisions such as the data protection principles. In this regard, and in the absence of any specific statute, the reference to ‘legislative measure’ must be expansively interpreted so as to take account of Article 11 of the *EU Charter* and cognate freedom of expression protections within national constitutional law. In sum, these instruments should themselves authorize otherwise permissible derogations so long as these are strictly necessary to effect a reconciliation between data protection and freedom of expression. At the same time, it is vital to recognize that Article 23(1) itself only envisages a derogation from the principles in so far as ‘its provisions correspond to the rights and obligations provided for’ in the GDPR’s detailed transparency rules and control rights.\(^{187}\) In other words, the Regulation establishes a very strong presumption that these fundamental principles will not be entirely disappplied but only limited through interpretation in accordance with the *EU Charter*. Notwithstanding its failure to reference Article 23(1), this limitation helps make sense of the CJEU’s important finding that a search engine refusing to deindex out-of-date data under the principles of adequacy and/or relevance must still ensure that the ‘overall picture it gives the internet user reflects [the data subject’s] current legal position’.\(^{188}\)

\(^{184}\) See *European Convention for the Protection of Human Rights and Fundamental Freedoms 1953*, ETS 5, 213 UNTS 22, Arts 8–11.

\(^{185}\) GDPR, recital 4.

\(^{186}\) Ibid, Art. 30.

\(^{187}\) Namely, GDPR, Arts 12–22 and 34. Interestingly, the cognate provision in the former Directive (DPD, Art. 13) set out no such caveat.

\(^{188}\) *GC et al. v CNIL* (n 15) , para .78.
expression contexts. Amongst the most pressing issues to be taken forward are a contextual interpretation of many of the other data protection principles including transparency,$^{189}$ accuracy$^{190}$ and integrity and confidentiality.$^{191}$ The discussion at the end of Section V.B should hopefully provide certain initial pointers in this regard and European DPAs can and should also play a key role in developing further guidance. Nevertheless, this is ultimately a very substantial judicial task and so needs to be prioritized by both the CJEU and national courts.

### VII. Conclusions

The interface between EU data protection and freedom of expression has sometimes been conceptualized as granting journalism an essentially absolute exemption from this law, whilst subjecting all other forms of activity involving the dissemination of personal data to the full force of the general rules. This understanding has always been incorrect and has become increasingly so with the GDPR. At the same time, as highlighted not just by CJEU judgments but also the German Constitutional Court’s recent *Right to be Forgotten* rulings, the steady development of ubiquitous online expression has seen the interface between data protection and freedom of expression emerge out of its somewhat esoteric origins into a mainstream topic of legal concern. The GDPR seeks to regulate this increasingly critical interface according to what is best understood as a tripartite substantive schema based on the personal exemption, special expression derogation, and broad expression regimes. These three frameworks all have different scopes and different relationships with substantive data protection. The *personal exemption*$^{192}$ in principle can provide certain individual activity with an absolute exclusion from data protection but, in light of the need to ensure ‘effective and complete protection of data subjects’,$^{193}$ can only cover relatively innocuous processing which is not ‘liable to infringe [another data subject’s] fundamental rights, in particular the right to privacy’.$^{194}$ *Special expression* encompasses not only journalism but also academic, artistic, and literary activities$^{195}$ which serve similarly critical and sensitive public interests. The central commonality here is that any indefinite dissemination of personal data is orientated towards a collective public or society at large. Although, given their different constitutional traditions, the EU Member States retain wide discretion here, these activities are not exempt from the GDPR but must benefit from any and all derogations as ‘strictly

---

$^{189}$ GDPR, Art. 5(1)(a).

$^{190}$ Ibid, Art. 5(1)(d).

$^{191}$ Ibid, Art. 5(1)(f).

$^{192}$ GDPR, Art. 2(2)(c).

$^{193}$ *Google Spain* (n 5), para. 34.

$^{194}$ *Rynei* (n 85), para. 29.

$^{195}$ GDPR, Art. 85(2).
necessary\textsuperscript{196} to effect a balance between the fundamental rights of data protection and freedom of expression. Meanwhile, whilst not directly instantiating such high public interests, distinctly valuable aspects of freedom of expression can also be furthered by, for example, self-expression on social networking sites and the facilitation of a wide range of expressive purposes by search engines and other online platforms and services. These activities fall within the GDPR’s \textit{broad expression} regime\textsuperscript{197} which requires Member States and ultimately DPAs and courts to reconcile rights according to more detailed derogatory standards and in a way which retains a direct role for the core substantive aspects of data protection, namely, the legitimating grounds for processing and the data protection principles. Whilst it would not be completely accurate to state as the German Constitutional Court suggested recently that this area is completely harmonized within the EU,\textsuperscript{198} the GDPR certainly mandates both stricter limitations and common standards here which should be interpreted by reference to the \textit{EU Charter}.

This article has sought to provide a comprehensive elucidation of the basic rationale, scope, nature of these three regimes, and how they jointly govern the relationship between data protection and freedom of expression. Clearly, however, this can only be a starting point. Further scholarly and ultimately both judicial and legislative specification remains imperative. The applicable substantive norms must also be robustly and effectively enforced. That can often appear to be a Sisyphean undertaking in today’s tangled and ubiquitously globalized online environment. Luckily, therefore, an analysis of those wider issues is a task for another day.

\textsuperscript{196} Buivids (n 50), para. 68.

\textsuperscript{197} GDPR, Art. 85(1).

\textsuperscript{198} BVerfG, 6 November 6 2019, docket number 1 BvG 276/17 (n 103), para. 77.