Beyond 'Having a Domestic'? Regulatory Interpretation of European Data Protection Law and Individual Publication

Statutory Data Protection Authorities (DPAs) who act as the guardians of data protection across the European Economic Area (EEA) have faced unprecedented interpretative challenges as a result of the explosion of indeterminate publication by individuals in the form of blogs, social networking and other online forums. Through both a questionnaire and systematic review of EEA DPA websites, this article finds that these regulators have generally adopted a strict interpretation of the law here, although considerable internal variation is also present. Almost all see data protection as engaged, around half argue that publication in the general social networking context requires data subject consent and even when individual publication is targeted towards the collective public many DPAs demonstrate some reluctance to apply the special expressive purposes (aka the journalistic) derogation. This article argues for an alternative tripartite approach under the forthcoming Regulation which accommodates the competing free expression rights and also the limited capabilities reasonably to be expected of private individuals on a sounder and more consistent basis. The law's personal exemption should cover individual publication so long as this does not pose a serious prima facie *risk to privacy or other fundamental data protection rights. The special expressive purposes derogation should protect individuals who are disseminating a message to the collective public without discrimination. Finally, the Regulation's new freedom of expression clause should ensure that individual publication which principally instantiates self-expression is subject only to the core of data protection's substantive and supervisory provisions.*

Keywords: Blogging; Data Protection; Citizen journalism; Defamation; Freedom of expression; Online Abuse; Personal exemption; Privacy; Social Media.

1. Introduction

From its inception, European data protection has sought to create a common space for processing personal data within which "the fundamental rights and freedoms of natural persons and in particular their right to privacy"[1] are safeguarded. Since the coming into force of the EU Data Protection Directive 95/46, this regime has also led to the mandatory creation and empowerment of statutory Data Protection Authorities (DPAs) across the European Economic Area (EEA).[2] These regulators have become "the main actors protecting data protection rights",[3] playing a critical role in interpreting this legal framework. Unsurprisingly given their protective duties, both data protection law and the DPAs have established a relationship of some tension with the freedom to publish. This tension initially arose almost entirely in relation to the activities of organisations rather than private individuals. However, from the early 2000s, the emergence firstly of blogs and later social networking sites has resulted in a world where anyone can with relative ease "communicate his or her thoughts to the entire world"[4] with the consequence that "personal information is being posted online at a staggering rate".[5] These developments have presaged profound challenges for privacy, reputation and the structure of European data protection, resulting in an unprecedented interpretative dilemma for Europe's information regulators, the DPAs. Drawing on both an EEA DPA questionnaire and a website review, this article provides the first comprehensive empirical survey of how these critical actors have responded to this dilemma; building on this broad empirical base it then considers how legal interpretation could best evolve in the future under the forthcoming General Data Protection Regulation (GDPR).[6]

It is found that EEA DPAs have generally adopted a strict approach to the application of data protection law to individual publication, although considerable variation between the different regulators is also evident. The vast majority (although not all) DPAs hold that once personal information relating to somebody other than the publisher themselves is disseminated to an indefinite number, the personal exemption[7] cannot apply. There is also a consensus that the special expressive purposes derogation[8] covers far from all forms of indeterminate dissemination, with many holding instead that it only protects forms of expression undertaken by individuals which are patently akin to that of professional journalism. At the same time, there is a split between two groups of DPAs. The first clearly recognise that the regulation of individual publication may unduly impact on freedom of expression and, therefore, seek explicitly to interpret legal requirements with

---

[1] Directive 95/46, art. 1. See similarly article 1 of the Council of Europe *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (1981).

[2] The European Data Protection Directive (Directive 95/46) extends not only to the 28 EU Member States but also to three associated states – Iceland, Liechtenstein and Norway – which together with the EU make up the European Economic Area (EEA). See EEA Joint Committee, *Decision 84/1999 amending Protocol 37 and Annex XI (Telecommunication Services) to the EEA Agreement*. The precise relationship between the legal duties of these three associated states and related legal provisions such as the protection of data protection within the EU treaties remains a matter of great complexity, the consideration of which is beyond the scope of this article.

[3] European Union, Fundamental Rights Agency, *Access to Data Protection Remedies in EU Member States* (2013) (http://fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies_en.pdf), 9.

[4] Daniel J. Solove, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* (Yale University Press) (2007) 19.

[5] *Ibid,* 29.

[6] Regulation 2016/679 of the European Parliament and of the European 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 95/4/6/EC (General Data Protection Regulation).

[7] Directive 95/46, art. 3 (2).

[8] Directive 95/46, art. 9.

regard for this right, whilst the second instead presume that publication outside the special expressive area should be expected to comply with default data protection in full. Within the latter group, the great majority go further and hold that in general only consent can provide a proper legal basis for publication. As Van Alsenoy and others have argued, this has not only fuelled a strong "mismatch" with the "social practices of individuals" but, at least theoretically, seeks to burden individuals with duties which are "excessively burdensome and unrealistic",[9] especially when viewed from the perspective of the fundamental right to freedom of expression. In sum, the majority of DPAs have looked close to 'having a domestic'[10] with large swathes of individuals online, whilst a few others such as the UK and Ireland have developed equally extreme positions which appear to ignore the responsibility of individual publishers here entirely. Looking to the future, the forthcoming GPDR provides the opportunity to develop a new tripartite approach which balances data protection against both competing free speech rights and the limited capabilities which can reasonably be expected of private individuals on a more consistent and sounder basis. Firstly, interpretation of the personal exemption[11] should be widened to encompass those forms of individual publication which do not pose a serious *prima facie* risk of infringing privacy or other fundamental data protection rights. Second, a broad and non-discriminatory approach should be taken to the special expressive purposes derogation[12] so that it covers individuals disseminating a message to the collective public. Thirdly, individual publication which is both *prima facie* objectionable and predominantly aimed at self-expression and a general freedom to converse should, under the Regulation's new freedom of expression clause, (only) be made subject to data protection's core substantive and supervisory provisions. The practical challenges of implementing this vision should not be underestimated and will undoubtedly have to involve not only individuals themselves but also services such as social networking sites which facilitate (and often mould, structure and aggregate) their publication activities. However, only such a *via media* approach can ensure that Europe's twin commitments to upholding both data protection and freedom of expression in the digital age is effectively realised.

The rest of this article is structured into five parts. The next section outlines the key legislative, social, judicial and regulatory developments prior to the 2013 DPA survey. Section three, which forms the empirical heart of this piece, details the methodology and findings of this survey both as regards the questionnaire and the systematic review of DPA websites. The fourth section surveys judicial, regulatory and legislative initiatives subsequent to 2013 including, most importantly, the finalization of the GDPR. The fifth section analyses this data and develops a new approach to better balance rights and capabilities in this area under the new Regulation. Finally, the last section closes with some overall conclusions.

2. Developments Prior to the 2013 EEA Data Protection Authority Survey

2.1 – The Pan-European Data Protection Legislative Framework

Data protection emerged in the 1970s consequent to the rapid development of computers and computerized networking. From the beginning, Europe has been its legal champion. A Council

[9] Brendan V. Alsenoy,"The evolving role of the individual under EU data protection law" (2015) 15.

[10] The Urban Dictionary elucidates this British idiom as follows: "When people are arguing, this is commonly known as 'having a domestic', no matter the seriousness of the arguement [*sic*]" (Urban Dictionary, *Having a Domestic* (http://www.urbandictionary.com/define.php?term=Having%20A%20Domestic)). In this case, given that fundamental issues concerning freedom of expression, privacy and personal integrity are at stake, the matter under dispute must be considered quite serious.

[11] Regulation 2016/679, art. 2 (2) (c).

[12] Ibid, art. 85 (2).

of Europe Data Protection Convention was finalized in 1981[13] and in 1995 the EU adopted a framework Data Protection Directive 95/46 which was designed to "give substance to and amplify"[14] the Convention's provisions. From 2000 onwards, data protection has been recognised as a fundamental right within the new EU Charter,[15] and in 2009 the Treaty of Lisbon gave this instrument a legal status akin to that of the EU Treaties.[16] Uniquely, the right to data protection was also separately set out in the treaties themselves.[17]

The European data protection framework as specified in Directive 95/46 is far-reaching. Materially, its default scope encompasses "processing of personal data wholly or partly by automatic means" as well as in certain structured, manual filing systems.[18] The key terms here are defined very broadly. "Personal data" refers to "any information relating to an identified or identifiable natural person ('data subject')"[19] whilst "processing … by automatic means" includes "any operation" performed digitally including collection, consultation, dissemination and even erasure.[20] Meanwhile, the law's purpose is to establish a pan-European space for "protect[ing] the fundamental rights of natural persons, and in particular their right to privacy".[21] This ambitious aim leads in turn to the imposition of wide and often deep default duties on data "controllers" defined as anyone "who alone or jointly with others determines the purposes and means of the processing of personal data".[22] In sum, controllers must in general ensure that their data processing complies as necessary with a broad set of *data protection principles* including fairness, non-excessiveness and accuracy,[23] detailed *transparency rules* which set out requirements for ensuring the openness of processing vis-à-vis data subjects both on a proactive and retrospective basis,[24] strict *sensitive data rules* which generally ban the processing of criminal, health, political opinion, ethnic and other broad categories of information within the private sector at least unless this prohibition has been waived by the subject,[25] and a variety of *disciplining provisions* which seek to ensure that the core substantive elements of the law are not undermined by, for example, a failure to document processing, to maintain data security or to regulate the transfer of personal data overseas.[26] Turning to the *supervisory system*, although a right to a judicial remedy[27] and individual compensation[28] must also be made available, the establishment of one or more independent DPAs in each of the Member States constitutes the central and "essential component"[29] of this system. These regulators, which must be endowed with wide-ranging powers of investigation and

[13] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) (ETS 108).
[14] Directive 95/46, recital 11.
[15] EU Charter, art. 8.
[16] TEU, art. 6 (1).
[17] TFEU, art. 16.
[18] Directive 95/46, art. 3 (1).
[19] Thus, 'data' and 'information' are treated synonymously and their conceptualization appears wide enough to encompass even innocuous details about an individual, even if these are already in the public domain.
[20] Directive 95/46, art. 2 (b).
[21] Directive 95/46, art. 1.
[22] Directive 95/46, art. 2 (d).
[23] Directive 95/46, art. 6.
[24] Directive 95/46, arts. 10-12.
[25] Either through explicit consent or through a manifest making public of the data by the subject themselves. See Directive 95/46, art. 8.
[26] Ibid, arts. 17, 18-19, 21 and 25-26.
[27] Directive 95/46, art. 22.
[28] Directive 95/46, art. 23.
[29] Directive 95/46, recital 62.

intervention, have duties to monitor application of the law, hear claims by data subjects[30] and cooperate in the pan-European Article 29 DPA Working Party which is charged with promoting "uniform application" of the Directive across the EEA.[31]

Tempering this generally broad and stringent framework, the Directive also includes a number of exclusions and derogations which are designed to provide for a reconciliation with other rights and interests. Article 3.2 sets out an *exclusion* not only for processing "in the course of an activity which falls outside the scope of Community law" – a provision which simply mirrors the Directive's treaty base – but also processing "by a natural person in the course of a purely personal or household activity" (the *personal exemption*), with recital 12 clarifying that this is designed to shelter activities which are "exclusively personal or domestic, such as correspondence and the holding of records of addresses". Meanwhile, article 9 sets out a special regime for a particular sub-set of freedom of expression, namely "the processing of personal data carried out solely for journalistic, purposes or the purpose of artistic or literary expression", where it is stated that Member States should provide derogations if (but only if) "they are necessary to reconcile the right to freedom of expression with the rules governing freedom of expression" (the *special expressive purposes derogation*). Finally, other clauses permit (rather than require) Member States to adopt derogations from the data protection principles and transparency rules in a "legislative measure" where necessary *inter alia* for "protection of … the rights and freedoms of others",[32] from the sensitive data rules in the "substantial public interest" and subject to "suitable safeguards",[33] and from the requirement to notify automatic processing with the DPA[34] where processing is "unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipient or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored"[35] (*other limited derogations*). However, these latter clauses do not provide for the possibility of a derogation from key elements of the regime including the need for a legal basis for processing,[36] the general provisions for ensuring discipline in processing[37] and the system of both private and public supervision.[38]

2.2 – Transposition of European Data Protection Exemptions and Derogations in Member State law

All Member States have transposed the *personal exemption* into their laws, the wording of which varies little, if at all, from that found in Article 3 (2) of the Directive itself. However, five States (Austria, Italy, Latvia, Liechtenstein and Romania) do establish express and strict limitations

[30] Directive 95/46, art. 28.
[31] Directive 95/46, arts. 29-30.
[32] Directive 95/46, art. 13 (f).
[33] Directive 95/46, art. 8 (4). The requirements as regards lifting the default limits on processing data relating to offences, criminal convictions or security measures are slightly different and only require Member States to provide "suitable specific safeguards" (Directive 95/46, art. 8 (5)).
[34] Directive 95/46, art. 18 (1).
[35] Directive 95/46, art. 18 (2). Member States are in any case meant to ensure that any person can demand directly from the controller (or other designated body) the same information (other than that concerning data security) which would otherwise be notifiable to the DPA (Directive 95/46, art. 21 (3)).
[36] Directive 95/46, art. 7.
[37] Directive 95/46, arts. 16, 17, 21, 25 and 26.
[38] Directive 95/46, arts. 22, 23, 24, 28 and 29.

on when this may be relied upon if data is to be disclosed to others,[39] whereas two others (Ireland and the UK) arguably seek to broaden it by express reference to an individual's "recreational purposes".[40] Turning to the scope of the *special expressive purposes derogation*, much greater statutory diversity is apparent. Fifteen Member States do mirror the Directive's protection of journalism and literary and artistic expression in this regard.[41] Four States (Denmark, Iceland, Malta and Sweden) go further and include some kind of broader reference to freedom of expression here. In contrast, twelve construe this derogation more narrowly by excluding literary expression (Cyprus, Italy), artistic and literary expression (Greece), any actor other than the institutional media (Austria, Estonia, Germany, Hungary, Liechtenstein and Slovenia) or even fail to set out such a derogation at all (Croatia, Czech Republic and Spain).[42] Finally, very few States have sought to utilize the *other limited derogations* to set out protections of clear relevance to individual publication. The most important exception to this is Sweden which in 2007 granted a statutory exclusion from all substantive data protection for processing which "is not intended to be included in a collection of personal data which has been structured in order to facilitate search for or compilation of personal data" so long as this activity did not violate the privacy of the data subject.[43] Meanwhile, under Netherlands' law, controllers are absolved from compliance with both the transparency rules and the data protection principle prohibiting so-called 'incompatible' repurposing of data where *inter alia* this is necessary in the interests of protecting the rights and freedoms of other persons.[44] Moreover, following an analysis carried out in 2007,[45] the Netherlands granted a further "personal websites" exemption from notifying their processing with the DPA but only if data relating to any particular data subject is removed on request and in any case all data is deleted on termination of the website.[46]

2.3 – The Definition and Development of Individual Publication:

The purpose of this article is to explore how data protection regulators have and should respond at an interpretative level to the phenomenon of individual publication. 'Individual' here is understood to refer to a natural person acting within his or her private capacity rather than on behalf of a commercial, professional or organizational interest.[47] As regards 'publication', it is

[39] Austria, Federal Act Concerning the Protection of Personal Data (DSG), s. 45; Italy, Personal Data Protection Code, s. 5 (3); Latvia, Data Protection Act, s. 3 (3); Liechtenstein, Data Protection Act, art. 3 (a); Romania, Law No. 677/2001 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, art. 2 (8).

[40] Ireland, Data Protection Act, s. 1 (4) (d); UK, Data Protection Act, s. 16. It should also be noted that although one provision within Polish law expressly excludes processing of data by natural persons "for personal or domestic purposes exclusively", another states that the legislation applies *inter alia* to "natural and legal persons and organizational units not being legal persons, if they are involved in the processing of personal data as part of their business or professional activity or the implementation of statutory objectives", a phrasing which could imply that all non-business, professional or official activity by both natural and legal persons is outside the scope of this law. See Poland, Act on the Protection of Personal Data, art. 3 (a) (1) and art. 3 (2) (2).

[41] These are Belgium, Bulgaria, Finland, France, Ireland, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania, Slovakia and the UK (including its intra-EU overseas territory Gibraltar).

[42] For a full analysis including citation to all relevant legislation see Author (2015a).

[43] Sweden, Personal Data Act 1998, s. 5 (a).

[44] Netherlands, Personal Data Protection Act, art. 43.

[45] Netherlands DPA, *Publication of Personal Data on the Internet* (2007), 29 (http://www.dutchdpa.nl/downloads_overig/en_20071108_richtsnoeren_internet.pdf).

[46] Netherlands, Vrijstellingsbesluit Wbp, art. 38b.

[47] Clearly, it is quite possible for an individual to pursue even on his own account a professional, commercial and organizational publishing activity and, therefore, fall outside the definition of 'individual publication' set

recognized that this may be conceptualised very broadly.[48] However, for the purposes of this article, 'publication' will be defined as encompassing only those forms of dissemination which make information available to an indeterminate rather than a finite audience.[49] Such a discrete focus is justified on the basis that the phenomenon of general publication (hereinafter publication) will, other things being equal, have a particularly serious impact on the privacy and related rights which data protection is committed to upholding. The rise of this form of individual activity also raises particularly pressing issues as regards the need to ensure a coherence of legal and regulatory treatment with other actors' activities including professional journalists and new online information services. It is nevertheless recognised that more restricted forms of dissemination of personal data by individuals also raise significant privacy and related concerns and that, in very serious circumstances, the application of data protection even in more limited contexts cannot be ruled out.[50] Further consideration of this issue, however, lies beyond the scope of this article.

Individual publication in the sense defined above is essentially an online phenomena. Given that its origins can be traced back to the rise of bulletin boards and other forums in the late 1970s and 1980s[51] it clearly predates the genesis of Directive 95/46 (although perhaps not data protection itself[52]). Nevertheless, until the early 2000s, such publication generally remained a niche activity. Since then, the rapid development of firstly personal blogging and then online social networking has resulted in a radical qualitative shift. As regards the development of personal web sites in the form of web logs (or blogs), Solove provides the following startling figures: "There were about 50 blogs in 1999, a few thousand in 2000, more than 10 million in 2004, and more than 30 million in 2005. By the end of July 2006 there were approximately 50 million blogs".[53] The later growth of social

---

out here. Examples include acting as a professional freelance journalist or running an online forum or social networking site (even on a non-profit basis). The application of default data protection provisions may breach other fundamental human rights such as freedom of expression in these contexts also. Further consideration of these issues, however, lies outside the scope of this article.

[48] For example, in UK defamation law, publication includes the dissemination of information even to one person who is not the person identified in the information or their spouse. See *Wennhak v Morgan* (1888) 20 Q. B. D. 635 (HC).

[49] As per the e-Privacy Directive, dissemination only to a finite audience can be considered to constitute only a 'communication' rather than a 'publication' of data. See Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, art. 2 (d).

[50] In fact, it is clear that several DPAs have sought to develop guidance especially in the social networking context which would apply data protection norms irrespective of whether information is disseminated to a determinate or indeterminate number of persons. Such a move, however, ought to be resisted since it runs the serious risk of intruding unduly on an individual's private life and shackling them with clearly disproportionate burdens. On the other hand, it may be argued that at least when manifestly inappropriate data is disseminated to a large body of determinate contacts, then a constrained interpretation of the personal exemption may be necessary to protect data subject rights. An obvious example here would be revenge pornography. If so, then a modified version of the legal structure forwarded in this article could be adopted such that the in cases of large-scale but determinate individual publication the personal exemption shields all but manifestly and seriously objectionable information (rather than the much lower threshold of simply *prima facie* objectionable information which would apply in indeterminate contexts).

[51] As early as 1983, the Fifth International Conference of Data Protection Commissioners noted with concern that "the application of new media disseminated by cable networks may involve a considerable hazard to the personal right of privacy" because *inter alia* "[v]ideotex experience shows that suppliers and subscribers are publishing sensitive data on the new media" ("Preserving Data Protection in the New Media" (1984) 8 *Transnational Data Report,* 416).

[52] The first genuinely comprehensive data protection statute was adopted in Sweden in 1973. For a translation see Paul Sieghart, *Privacy and Computers* (Latimer New Dimensions) (1976) 165-171.

[53] Daniel J. Solove, Daniel, *The Future of Reputation: Gossip, Rumor and Privacy on the Internet* (Yale University Press 2007) 21.

networking has been even more striking with Van Dijck noting that "[i]n December 2011, 1.2 billion users worldwide – 82 percent of the world's Internet population over the age of 15 logged on to social media sites, up from 6 percent in 2007. Within less than a decade a new infrastructure has emerged, penetrating every fiber of culture today".[54]

Both of these developments raise very serious new challenges as regards the protection of privacy and personal information more generally. Thus, Solove again notes

> Many blogs are more akin to diaries than news articles, op-ed columns or scholarship. According to one survey, bloggers most commonly write about their personal experiences (37 percent), whilst only 11 percent blog about politics … In lieu of diaries, people are blogging. And bloggers are getting younger and younger. One news article reports that even seven-year-old children have blogs. As people chronicle the minutia of their daily lives from childhood onwards in blog entries, online conversations, photographs, and videos, they are forever altering their futures – and those of their friends, relatives, and others.[55]

Meanwhile Mann, perhaps with some hyperbole, argues that the development of online social networking has "conspired to invite impersonation, denigration, sexual or aggressive solicitation, cyber-bullying, and happy slapping to the members of social networking websites (SNWs). The situation is serious – serious because the user-generated content (UGC) that is displayed on-screen is destroying users' lives; serious too, because of the volume of users at risk from posting their content".[56] The 2016 annual survey of English teachers carried out by the NASUWT trade union drew specific attention to some of these problems, with those reporting having suffered insulting online comments or information from pupils and parents numbering 60% and 43% respectively.[57] Highlighting the sense of helplessness which can accompany such experiences, 63% failed to report perceived instances of online abuse involving pupils "because they felt no action would be taken", whilst in 56% of cases no action was taken against parents for their postings.[58] General Secretary Chris Keates commented at the launch of these results: "Over the three years the NASUWT has been running this survey the situation has deteriorated … Online abuse is traumatic and potentially life changing. Victims need strong support through a zero tolerance approach".[59]

2.4 – Court of Justice and Article 29 Working Party responses prior to 2013:

---

[54] Jose Van Dijck, *The Culture of Connectivity: A Critical History of Social Media* (Oxford University Press 2013) 4.

[55] Daniel J. Solove, *The Future of Reputation*, 24.

[56] Bruce L. Mann, "Social Networking Websites – A Concatenation of Impersonation, Denigration, Sexual Aggressive Solicitation, Cyber-Bullying or Happy Slapping Videos", (2009) 17(3) *International Journal of Law and Information Technology* 252-267.

[57] Although not reported at such a level of granularity, the NASUWT press release on the UK-wide results not only indicated a similar pattern but also noted with concern that "[o]ver the three years the NASUWT has been running the survey the situation has deteriorated" (NASUWT, *Social media abuse endemic in schools*, http://www.nasuwt.org.uk/Whatsnew/NASUWTNews/PressReleases/NASUWT_015430).

[58] NASUWT, *Abuse of Technology* [England edition 2016] 6-7, http://www.nasuwt.org.uk/consum/groups/public/@journalist/documents/nas_download/nasuwt_014375.pdf. It is clear that the vast majority of these comments (83% and 84% respectively) had been posted on the social networking site Facebook.

[59] NASUWT, *Social media abuse endemic in schools* [UK-wide press release] (2016), http://www.nasuwt.org.uk/Whatsnew/NASUWTNews/PressReleases/NASUWT_015430.

The relationship between Directive 95/46 and individual publication was first considered in *Lindqvist* (2003),[60] an early and seminal case in the Court of Justice of the European Union (CJEU)'s data protection jurisprudence. The case concerned the relationship between the Directive and Mrs Lindqvist's publication on her personal website of "personal data on a number of people working with her on a voluntary basis in a parish of the Swedish Protestant Church"[61] and attracted the intervention of the European Commission as well as that of three Member States. Lindqvist argued that her activity was exempted by article 3(2) of Directive 95/46 and that in any case the Directive's provisions were disproportionate and unpredictable and therefore "contrary to the general principle of freedom of expression enshrined in Community law".[62] The Commission rejected this and instead argued that, "given the purpose of the internet page at issue", it constituted "an artistic and literary creation [sic] within the meaning of Article 9 of that Directive".[63] Whilst not endorsing that proposition, both the Netherlands and Swedish Governments argued that, since freedom of expression was clearly engaged, "the national court must endeavour to balance the various fundamental rights at issue by taking account of the circumstances of the individual case".[64] Finally, although essentially confining itself to technical aspects of the case, the UK Government implied that the general provisions of European data protection could legitimately apply in full here.[65]

The CJEU judgment clearly held that Lindqvist fell within the Directive's provisions. Article 3(2)'s shielding of "purely personal or household activity" was confined "only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people",[66] whilst its reference to "activit[ies] which falls outside of Community law" only covered the "activities of the State or of State authorities".[67] The Court also declined to agree with the Commission that article 9 was engaged. However, in the process of rejecting Lindqvist's argument that the Directive itself violated freedom of expression, it acknowledged that:

> Mrs Lindqvist's freedom of expression … and her freedom to carry out activities contributing to religious life have to weighed against the protection of the private life of the individuals about whom Mrs Lindqvist has placed data on her internet site. Consequently, it is for authorities and courts of the Member States … to make sure they do not rely on an interpretation of [the Directive] which would be in conflict with the fundamental rights protected by the Community legal order or with the other general principles of Community law, such as inter alia the principle of proportionality.[68]

No subsequent CJEU case has directly considered individual publication online. However, the Grand Chamber decision of *Satamedia* (2008),[69] which centred on the commercial activity of making public domain tax income data on 1.2 million Finnish residents available via a hard-copy catalogue and mobile messaging service, did give extensive consideration to the scope of Article 9 of the Directive (the *special expressive purposes derogation*). In sum, it found that "[i]n order to take

[60] C-101/01 *Lindqvist, Criminal Proceedings Against Bodil*, EU:C:2003:596.
[61] *Ibid* at [2].
[62] *Ibid* at [73].
[63] *Ibid* at [33].
[64] *Ibid* at [76].
[65] *Ibid* at [55].
[66] *Ibid* at [47].
[67] *Ibid* at [42].
[68] *Ibid* at [87].
[69] C-73/07 *Tietosuojavaltuutettu v. SatakunnanMarkkinapörssi Oy and Satamedia Oy*, EU:C:2008:727.

account of the importance of the right to freedom of expression in every democratic society, it is necessary … to interpret notions relating to that freedom, such as journalism, broadly"; as a result, activities involving personal data processing must be considered as carried out "solely for journalistic purposes" if "the sole object of those activities is the disclosure to the public of information, opinions or ideas".[70] The Court also reiterated *Lindqvist*'s very limited construction of exceptions to the Directive set out in article 3(2), emphasising further that "the directive does not lay down any further limitation of its scope of application."[71]

The Article 29 DPA Working Party (hereinafter Working Party) made an initial, albeit rather limited, intervention in its 1997 Recommendation on *Data Protection and the Media* which argued that "[a]rticle 9 of the directive respects the right of individuals to freedom of expression. Derogations and exemptions under article 9 cannot be granted to the media or to journalists as such, but only to anybody processing data for journalistic purposes".[72] However, it was not until 2009 in its opinion on online social networking that the Working Party gave any sustained attention to individual publication. Echoing *Lindqvist*, this opinion stated that, whilst "[i]n most cases, users are considered to be data subjects",[73] "[i]f a user takes an informed decision to extend access beyond self-selected 'friends' data controller responsibilities come into force".[74] Whilst noting tangentially that users might benefit from "other exemptions such as the exemption for journalistic purposes, artistic or literary expression"[75] and additionally that "[u]sers should, in general, be allowed to adopt a pseudonym",[76] the opinion argued that European data protection generally imposed very serious restrictions on publication activity in the social networking context. Thus, it held that social networking site users should be "reminded that uploading information about other individuals may impinge on their privacy and data protection rights",[77] that (absent a Member State exemption) "[s]ensitive personal data may only be published on the Internet with the explicit consent from the data subject or if the data subject has made the data manifestly public himself"[78] and even that users should be advised that "pictures or information about other individuals, should only be uploaded with the individual's consent".[79] In February 2013, and as part of its input on the

[70] *Satamedia* at [61]. The precise definition provided by the Court here was, in theory at least, confined to processing "relating to documents which are in the public domain under national legislation".
[71] *Ibid* at [46].
[72] European Union, Article 29 Working Party, Recommendation 1/1997 *Data protection law and the media* (WP 1) (1997) 8.
[73] European Union, Article 29 Working Party, *Opinion 5/2009 on online social networking* (WP 163) (2009), 6.
[74] *Ibid*, 6.
[75] In such a situation, it argued, "a balance needs to be struck between freedom of expression and the right to privacy" (*Ibid*, 6).
[76] *Ibid*, 13.
[77] *Ibid*, 7.
[78] *Ibid*, 8. The Working Party did footnote that Member State exemptions were possible here. It also deployed a purposive rather than literal meaning of the concept of sensitive personal data stating that "[t]he Working Party in general does not consider images on the Internet to be sensitive data, unless the images are clearly used to reveal sensitive data about individuals" (*Ibid*). This would suggest that photographs which incidentally reveal a person's ethnic or racial origins (as, in fact, all colour photography would appear to do) or information concerning their health or religious beliefs would not on that account only be considered sensitive data. Unfortunately (although understandably given the wide wording found in article 8 of the Directive) a number of courts have opted for a stricter approach. See *Murray v. Big Pictures*, [2007] EWHC 1908 (Ch); [2007] EMLR 22 (overruled but not on this point); Hoge Raad (Netherlands Supreme Court), (23 March 2010) LJN BK6331. The need for a purposive approach is recognised in Recital 34 of Directive 95/46 which spoke of the sensitive data as "data which are capable by their nature of infringing fundamental freedoms or privacy".
[79] *Ibid*, 12.

now-adopted GDPR,[80] the Working Party issued a statement on the personal exemption which was drafted by the UK DPA[81] but endorsed by the Working Party as a whole. In considerable contrast to its 2009 opinion, this statement argued that "the fact that an individual makes his blog or her social networking profile available to the world" should not be "determinative" of whether such activity lies outside the household exemption but should rather constitute "an important consideration" amongst many.[82] It therefore developed a new multi-factorial test to determine the applicability of the personal exemption which it argued should be laid out in a Recital to the new GPDR as follows:

> This Regulation should not apply to processing of personal data by a natural person which is exclusively personal or domestic, such as correspondence, the holding of addresses of personal contacts or the use of social network sites that is outside the pursuit of a commercial or professional objective. In determining whether the processing falls within the exception, consideration should be given to whether the personal data is disseminated to an indefinite number of persons, rather than to a limited community of friends, family members or acquaintances; whether the personal data is about individuals who have no personal or household relationship within the person posting it; whether the scale and frequency of the processing of personal data suggests professional or full-time activity; and whether there is evidence of a number of individuals acting together in a collective and organised manner. The application of the exemption is constrained by the need to guarantee the rights of third parties, particularly with regard to sensitive personal data. In this connection, account should be taken of the extent to which a natural person might be liable according to the provisions of other, relevant national civil or criminal laws, e.g. defamation.[83]

3. The 2013 EEA Data Protection Authority Survey

3.1 – Survey Methodology

In recognition of the critical role Data Protection Authorities (DPAs) perform not only as an "essential component"[84] of European data protection law but as its "guardians",[85] the empirical survey presented here sought to explore in detail the interpretative approaches adopted by these statutory regulators in each of the EEA Member States. It was divided into two parts. In the first place, in March 2013 a questionnaire was sent to both national and regional EEA DPAs[86] with replies being accepted until the end of July 2013. The questionnaire's purpose was to capture the broad interpretative *stance* of these agencies as regards individual publication. It therefore presented

[80] The contours of the Regulation will be dealt with in sub-section 4.2 below.
[81] David Smith, "EU General Data Protection Draft Regulation" (2013) (https://www.youtube.com/watch?v=Rgt_5h3Qemk) at 00:32-00:38.
[82] European Union, Article 29 Working Party, Statement of the Working Party on current discussions regarding the data protection reform package Annex 2 Proposals for Amendments regarding exemption for personal or household activities (2013), 9.
[83] *Ibid*, 10.
[84] Directive 95/46, recital 62.
[85] C-518/07 *Commission v Germany* (2010), EU:C:2010:125 at [23].
[86] Regional DPAs have been established in the intra-EU British overseas territory of Gibraltar, the Spanish regions of the Basque Country and Catalonia and in each of the sixteen German Länder. In the German Land of Bavaria alone, regulation remains divided between the public and private sectors. In light of the focus of the questionnaire on essentially private sector matters and given the complication which a response from both of these regulators would cause, no attempt was made to contact the public sector regulator. In the event, the Bavarian DPA responsible for the private sector also did not participate in the questionnaire.

them with the following two scenarios corresponding respectively to hypothetical activity by an individual blogger and a social networker respectively:

- Individual blogger: "In his spare time, an individual publishes a blog that discusses and disseminates gossip about various celebrities. It is freely available on the Internet and visited by several hundred people a week."
- Social networker: "A member of a Social Networking Site (SNS), the membership of which is generally open to individuals worldwide, 'tags' a photo of an identified individual and makes an informed decision to make this freely available to all members of the site."

Although free-text responses were also permitted, DPAs were invited to indicate in relation to these scenarios, which of the following statements was considered correct:

A. Data protection does not apply.
B. Data protection applies, but the activity in question must benefit from all the special derogations and exemptions for journalism, art and literature envisaged in Article 9 of Directive 95/46/EC.
C. The general provisions of data protection law apply, but must be interpreted with regard for other fundamental rights including freedom of expression.
D. The general provisions of data protection law apply in full.

These statements sought to crystallize the four broad approaches put before the Court of Justice in *Lindqvist*. In essence, they represent ordered options ranging from no application (A) through to full application (D) of the default data protection provisions.

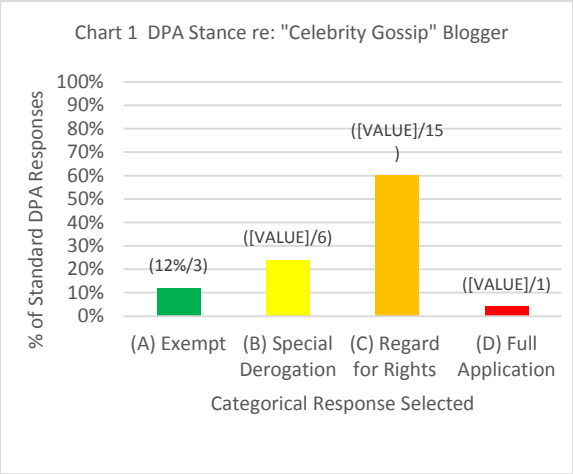
Although useful for revealing the lay of the land, it was recognised that the questionnaire data would inevitably be broad-brush. Therefore, to complement this, DPA websites were systematically reviewed for more detailed interpretative *guidance* related specifically to the individual publication. Between March 2013 and the end of that year, the websites of thirty-seven DPAs were examined including those operating at the national level in all 31 EEA Member States and additionally those of the six sub-national regulators which responded to the questionnaire. Ultimately, as further elucidated in sub-section 3.2 below, it proved possible to categorize almost all the guidance collected into three broad groups, namely, (1) the potentially permissive, (2) the mid-range and (3) the stringent.

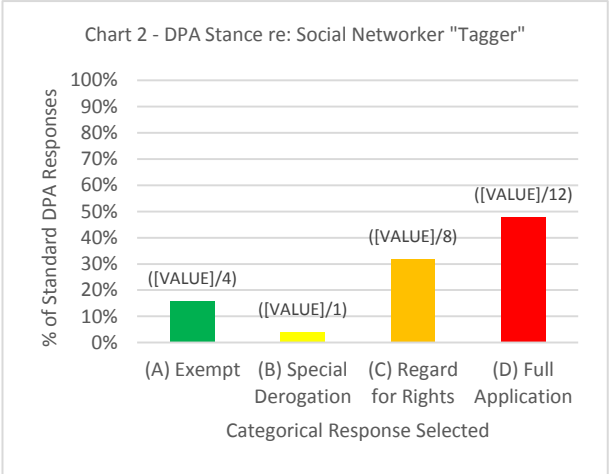
Given that the DPA questionnaire data itself has already been written up,[87] this section will focus on presenting the DPA website data and linking it back to that of the questionnaire. However, before turning to this, the questionnaire data itself will be briefly summarized.

3.2 – The EEA DPA Questionnaire

Responses to the two DPA questionnaire scenarios concerning individual publication online were obtained from twenty-nine regulators comprising twenty-three out of the thirty-one national DPAs (74% of the total) together with six regional bodies. As regards both scenarios, twenty-five standardized responses were received (in two cases each with additional text specification) together with four free-text answers. These results for each responding DPA are specified in the article's appendix, whilst chart one and two below present the standard responses received as regards the blogger and the social networker scenarios respectively.

[87] David Erdos, "Data Protection Confronts Freedom of Expression on the 'New Media' Internet: The Stance of European Regulatory Authorities" (2015) 40(4) European Law Review 531-562.





Turning first to consider the blogger scenario, it is striking that despite the subject matter ("celebrity gossip") overlapping with a certain type of (admittedly often salacious) professional journalism, only approximately a quarter of DPAs saw the special expressive purposes derogation (B) as being engaged.[88] Instead, a clear majority (60%) saw this rather as an instance where general provisions data protection apply but must be interpreted with regard for freedom of expression (C). Only a small minority of DPAs selected either of the other options.[89] The four free-text responses displayed considerable uncertainty as to how such blogging should be regulated, with two closest to the special derogation category (B),[90] one to the regard for rights category (C)[91] and one midway along the spectrum as a whole.[92]

[88] Moreover, although indicating that the special purposes derogation was applicable, the Estonian DPA indicated that the "practice" of the authority additionally took into account the criteria of interpreting general data protection with regard for freedom of expression (C).

[89] Moreover, whilst indicating that data protection was fully applicable (D), the Cypriot DPA included two texts which appeared to qualify this considerably: "As a rule, the exemption of journalistic purposes (freedom of expression) should also be applied to persons who are not journalists by profession but publish data in relation to cases for which there is an increased journalistic public interest at the time of publication" and "Discussing gossips does not necessarily imply the processing of personal data. Re-publishing personal data made publicly available by other media would not be in breach of the Law unless the Commissioner ascertains a contravention of the Law in line with section 4(2) of the DP [Data Protection] Law [of Cyprus]."

[90] Thus, the Swedish DPA stated that the blog "would fall under the Data Protection Act, but only under a simplified provision – not the provisions in full" (which was interpreted as akin to (C)) or "could possibly be exempted" if done for "journalistic purposes" (which was interpreted as akin to (A)). Similarly, the German Land of Rhineland-Palatinate DPA held that "[i]f it was only a private activity without journalistic importance" option (c) would apply but that if it could be classified as journalistic then data protection law would only be applicable to administrative processing rather than this activity itself (which was interpreted as akin to A). In each case, the combined elements of the response averaged most closely to (B).

[91] The Austrian DPA indicated that whilst a special section of the law regulated the relationship between data protection and the media (which was interpreted as akin to B), "[t]he regular Data Protection Act may apply to blogs and similar less regulated 'media'" and if so data protection law would apply in full (D). In this case, the combined elements of this response averaged most closely to (C).

[92] The Slovenian DPA stated that data protection would apply in full (A) "if the published data is such that would be protected under data protection law, e.g. if it has been acquired from a data controller and published without legal grounds". However, "[i]f it is merely gossips, not originating from a certain data controller, the general law on defamation and breach of privacy applies [and data protection would not be applicable at all]" (which is akin to option (D)).

Moving on to look at the social networker scenario, almost a majority (48%) of the standard responses held that default data protection must simply apply in full here (D). Nevertheless, a sizable number (32%) saw this rather as a situation where general data protection had to be interpreted with regard for freedom of expression (C). Moreover, although almost none saw the special derogation as applicable (B), a significant number (16%) held that data protection was not applicable at all (A), albeit with caveats in two cases.[93] Meanwhile, although one free-text response related most to the regard for rights category (C),[94] the other three displayed an (albeit ambiguous) reluctance to apply data protection law here and so were closest to option A.[95]

3.3 – The EEA DPA Website Review

Interpretative guidance related to individual publication was located on twenty-four out of the thirty-seven websites examined (65%), which included twenty-two (71%) of the 31 national DPA websites but only two (33%) of the six regional DPA sites explored. Although both the extent and comprehensiveness of this guidance differed, in only two cases (namely, the Austrian[96] and Lithuanian[97] DPA websites) did the guidance prove impossible to categorize as a result. In the other twenty cases, the guidance fell within the following three groupings arrayed according to the strictness of approach taken.

Firstly, six DPAs (27% of the grouped total) fell within a *potentially permissive group (1)* in that their guidance suggested that most forms of individual publication online should not be subject to data protection law at all (Irish, Slovenian and UK DPAs) or should be treated as essentially akin to journalistic/special expression (Finnish and Icelandic DPAs) or at least should not attract regulatory attention (Czech DPA). Turning to more detailed consideration of this guidance:

[93] Thus, in additional text the Maltese DPA stated that "[a]pplicability depends on the type of profile and whether this is intended for personal use or for other purposes such as business, or to disseminate special news or information of a journalistic nature" whilst the Slovenia DPA noted that "[i]f the member is a data controller, data protection law might apply".

[94] Thus, the Swedish DPA response stated that "such publication would fall under the Data Protection Act, but only under a simplified provision – not the provisions in full".

[95] Thus, the Finnish DPA responded that "[a]pplication of the Data Protection law (Personal Data Act) depends on the purpose of the tagging", the Polish DPA stated "[i]n general we consider that the SNS [Social Networking Site] itself is a data controller, and not the individual", whilst the Slovakian DPA held that "Data Protection applies only in the case when a purpose and means of data processing are determined and such activity is performed systematically. If these three conditions are not fulfilled the case of privacy infringement fall within the scope of the Civil Code".

[96] The Austrian DPA website included very limited information in a publication targeted at teenagers which simply stated that, similarly to the Press, individuals are responsible for anything they upload such as falsehoods, racist statements and pictures including in social networks and blogs and this can lead to serious consequences including fines or imprisonment. See Austrian DPA, *Du bestimmst …* (2010) (https://www.dsb.gv.at/DocView.axd?CobId=38031). This DPA was a questionnaire participant holding that as regards the social networking user example general data protection law applied in full ((D)) and that as regards the blogger example the law might either likewise apply in full or the provision in the law concerning journalistic purposes might be applicable (a free-text answer).

[97] Relevant information found on the website of the Lithuanian DPA was confined to a press release on cyberbulling on Facebook in which the authority *inter alia* advised users to respect other individuals' right to the protection of personal data in their use of the network. See Lithuania, Valstybinę duomenų apsaugos inspekciją, *Facebook reakcija į internetinėje žiniasklaidoje skelbtą straipsnį* (2012) (https://ada.lt/go.php/lit/Facebook-reakcija-i-internetineje-ziniasklaidoje-skelbta-straipsni/28). This DPA was also a questionnaire participant and held that as regards both the social networker and blogger examples the general data protection provisions would apply but must be interpreted with regard for fundamental rights such as freedom of expression ((C)).

- The *Czech DPA* held that individual pieces of information published in the context of *inter alia* blogs and social networks would in most cases lie outside the scope of statutory data protection intervention by the DPA since, it argued, the purpose of this law was to regulate systematic or targeted use of personal data[98] and under the principle of *ultima ratio* not just criminal but even administrative penalties could only be deployed if private action was inappropriate or ineffective.[99]
- The *Finnish DPA* held, in the context of a complaint against a private person's personal website, that as a rule data protection law should not be applied to articles and similar writings on account of this constituting an editorial or literary expression. The law on mass media including its limitations would be applicable. The DPA also stressed that freedom of speech protected publication regardless of the method used. However, no specific guidance was found regarding publication in the rather different general social networking context.[100]
- The *Icelandic DPA* argued that, as regards publication on the internet generally and Facebook specifically, it might be necessary to take into account provisions in Icelandic data protection allowing derogations "in the interest of" journalism, art or literature[101] and that in any event a case-by-case balance between privacy and freedom of expression (as protected in the Icelandic Constitution and the European Convention) was required which it stated it was not competent to make binding decisions on.[102]
- The *Irish DPA* held, in the context of its 2011 audit of Facebook Ireland, that (apparently irrespective of whether publication was indefinite in nature) "[u]nder Irish law where an individual uses Facebook for purely social and personal purposes to interact with friends etc they are considered to be doing so in a private capacity with no consequent individual data controller responsibility. This so-called domestic exemption means for instance that there are no fair processing obligations that arise for an individual user when posting information about other individuals on their Facebook page."[103]
- The *Slovenian DPA* recommended in a 2009 leaflet concerning Facebook that users respect others and avoid publishing either data or photos without consent. However, whilst noting that individuals have a constitutional right to privacy and other laws (harassment, defamation, undue image recording) might apply, it nevertheless held it had no direct responsibility here.[104] Further guidance on data protection and the media highlighted this DPA's peculiar understanding that data protection law solely applied to "personal data which is intended for its inclusion in a filing system"[105] and would therefore only be triggered either as regards such "personal data collections"[106] or where the data "had been illegally supplied from [such] collections of personal data".[107]
- The *UK DPA* in guidance on "online forums such as social networking sites, message boards, or blogs" [108] stated that the household exemption would apply "whenever someone uses an online forum purely in a personal capacity for their own domestic or recreational purposes"[109] and that it therefore "will not consider complaints made against individuals who have posted personal data whilst acting in a personal capacity, no matter how unfair, derogatory or distressing the posts may be".[110]

---

[98] Czech, Úřad pro ochranu osobních údajůp, *Zveřejňování osobních údajů na internet* (2012), 1, https://www.uoou.cz/files/stanovisko_2012_13.pdf.

[99] *Ibid*, 2. The final paragraph of the guidance nevertheless stated that individuals nevertheless retained an ability to assert their rights through civil court proceedings (*Ibid*, 3).

[100] Finland, DPA, *Henkilötiedot yksityisen henkilön kotsilvuilla* (2004) (https://web.archive.org/web/20111224022923/http://tietosuoja.fi/48518.htm).

[101] See Iceland, Data Protection Act, art. 5.

[102] Iceland, Persónvernd, *Fyrirspurn um friðhelgi einkalífs og tjáningarfrelsi á Netinu* (2010) (http://www.personuvernd.is/efst-a-baugi/nr/991).

[103] The report even went on to argue that "[t]he Article 29 Working Party Opinion 5/2009 on online social networking also recognized this distinction". See Ireland, Data Protection Commissioner, *Facebook Ireland Ltd Report of Audit 21 December 2011*, 24 (https://dataprotection.ie/documents/facebook%20report/final%20report/report.pdf).

[104] Slovenia, Informacijski pooblaščenec, *Kako uporabljati facebook ... in preživeti* (https://www.ip-rs.si/fileadmin/user_upload/Pdf/brosure/Kako_uporabljati_FB_in_preziveti_tisk__v2_-net.pdf).

[105] Slovenia, Informacijski pooblaščenec, *Media and the protection of personal data*, p. 8 (https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Media_and_the_Protection_of_Personal_Data.pdf)

[106] *Ibid*, 7.

[107] *Ibid*, 28.

[108] UK, Information Commissioner's Office, *Social networking and online forums – when does the DPA apply?*, p. 2 (https://ico.org.uk/media/for-organisations/documents/1600/social-networking-and-online-forums-dpa-guidance.pdf).

[109] *Ibid*, 3.

[110] *Ibid*, 15.

The rather amorphous understandings of law and regulation within this group is confirmed by linking this guidance back to rather divergent responses given by the relevant DPA in the questionnaire which rather often appeared in some tension with the published guidance. (This linkage was not possible in the case of the UK and Icelandic DPAs since they were not questionnaire participants). The Czech DPA held that data protection was fully applicable (D) in the social networker scenario and that as regards the blogger it also applied but had to be interpreted with regard for freedom of expression (C). Meanwhile, the Irish DPA selected this general balancing option (C) in both scenarios. The Slovenian DPA held that data protection would be inapplicable (A) in the social networker scenario, but its free-text answer as regards the blogger essentially sat midway along the entire spectrum.[111] Finally, the Finnish DPA held that the special expressive purposes derogation (B) would apply in the case of the blogger and in relation to social networker gave a somewhat ambiguous free-text answer which nevertheless came closest to the inapplicability of data protection (A).[112]

Secondly, another five DPAs (23% of the grouped total) were categorized within the *mid-range group (2)* since their guidance suggested that, even within an ordinary social networking context, individuals could make personal information public without consent so long as this was judged to be harmless (Denmark, Spanish Catalan), not annoying (Greece), necessary and not overridden by the interests of data subjects (Netherlands) or not offensive (Sweden). Information specifically flagged up for strict scrutiny comprised photographic images (Denmark, Greece), sensitive data (Netherlands, Denmark) and structured data (Sweden). Additional protection for special expressive purpose processing was also sometimes highlighted, although in one instance (Netherlands) the test proposed appeared weighted in favour of professional as opposed to amateur activity. Turning to a more detailed elucidation:

- The *Danish DPA*, which confined itself to the social networking context, held that users should publish information with consent (or parental consent for minors) unless the data was "harmless" meaning "something so innocent that one would not normally feel that their privacy was infringed upon". Even such data had to be removed on request unless "you have a legal basis for not doing so" such as expression of "opinion in a way that is permissible in relation to freedom of expression" which is not "unlimited".[113] Portrait photos – any photo whose purpose "is to depict one or more specific people" – in any case required consent and the publication of private and sensitive information would generally require clear and distinct consent.[114] Another part of the guidance did however state that data protection could "not be used to prohibit you from expressing your opinion" although it was stressed that "[y]ou must still refrain from disclosing the most private and sensitive data about other persons".[115]
- The *Greek DPA* published "tips" («ευμβουλές») on publishing information on social networks or forums which stated that users should not publish content that might "annoy" («ενοχλήσουν»). The guidance for photos and videos was more cryptic (and potentially more severe) since one part stated that approval should be sought here whilst another stated only that potentially "annoying" («ενοχλητικά») publication should be avoided.[116]

[111] See *supra* note 92.
[112] In sum, it stated that "application of the Data Protection law (Personal Data Act) depends on the purpose of the tagging". This might suggest if the purpose of tagging was not in any way professional or commercial then data protection would not apply at all.
[113] Denmark, Datatilsynet, *What you may disclose* (https://www.datatilsynet.dk/english/social-networks/what-you-may-disclose/).
[114] Denmark, Datatilsynet, *What you may not disclose* (https://www.datatilsynet.dk/english/social-networks/what-you-may-not-disclose/).
[115] Denmark, Datatilsynet, *When you disclose data* (https://www.datatilsynet.dk/english/social-networks/when-you-disclose-data/).
[116] Greece, Greece, Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Συμβουλές για τη δημοσίευση προσωπικών δεδομένων σε υπηρεσίες κοινωνικής δικτύωσης ή φόρουμ (http://www.dpa.gr/portal/page?_pageid=33,147396&_dad=portal&_schema=PORTAL).

- The *Netherlands DPA* published an extensive guide to the publication of personal information on the internet which argued that such activity was legitimate if necessary *inter alia* for furtheringlegitimate interests not overridden by the rights and interests of the data subject.[117] Otherwise unequivocal and rescindable consent had to be present which would in any case be required when publishing sensitive data not manifestly made public by the data subjects themselves. The guidance emphasised that a wide range of duties would anyway be applicable including the data protection principles, proactive and retrospective transparency rules and overseas data transfer rules.[118] Whilst acknowledging that a special laxer regime applied for exclusively journalistic, literary and artistic publication, the guide only set out an indicative, multi-factorial test for journalismwhich, with its emphasis especially on "regular activity", appeared somewhat tilted in favour of professional as opposed to amateur activity.[119]
- The *Spanish Catalan DPA* published guidance originally produced by an NGO (the Comisión de Libertades e Informátion) and aimed at 15-17 year olds which held that those engaging in blogs, forums and chats should always be respectful and tolerant of the views of others and should not insult, threaten or do anything that could harm others.[120]
- The *Swedish DPA* held that, whilst information in a structured format such as a database (or derived from the same) generally must comply with data protection in full, publishing or otherwise processing information in the form of running text or photos was permissible so long as this was not "offensive" ("kränkande").[121] Offensive data could anyway be published by individuals who want to inform, exercise criticism and stimulate debate on social issues of importance to the public as this would be covered by exemptions for journalistic purpose.[122]

The focus on the need for a strict balance in this area was mirrored strongly in the linked DPA questionnaire responses (which were not received from either Danish or the Netherlands DPAs). The standard responses from the Greek and Catalan DPA held, both as regards the blogger and the social networker scenarios, that general data protection interpreted with regard for freedom of expression was applicable (C). The free-text response from the Swedish DPA was similar as regards the social networker but more permissive as regards the blogger.[123]

Thirdly, a majority of some eleven DPAs came within the *stringent group (3)* since they suggested that, at least in the general social networking context which constituted the principal focus of the guidance, publication of personal information should be based on data subject consent. (In two instances (Norway, Italy) this categorization was only marginally made as there was also clear overlap with some themes in the mid-range group above). In most instances a particular

[117] Netherlands DPA, *Publication of Personal Data on the Internet* (2007), 23-25 (https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/en_20071108_richtsnoeren_internet.pdf).

[118] *Ibid*, 5. The guidance also expressly noted that "[c]ontrollers who do not comply … can be subject to legal action by data subjects … [and] [i]n addition may be subject to the supervisory powers of the Dutch DPA, varying from mediation to the institution of an official inquiry or the imposition of incremental penalties" (*Ibid*, p. 57).

[119] The guide suggested the following four questions (where assent to all would definitely constitute journalism but only the last of which was deemed in and of itself essential): (a) Is the activity orientated towards the (objective) collection and distribution of information?, (b) Is it a regular activity?, (c) Is the aim of the publication to raise a topic of social significance? and (d) Does the publication grant data subjects the right to reply or obtain rectification after publication? (*Ibid*, 43-45).

[120] Comisión de Libertades e Informátion, *Proyecto CLI – PROMETEO 2008/09 Manual Práctico de 15 a 17 año* (http://www.apd.cat/media/1856.pdf)**,** 4. The guide featured participation also from the Spanish national and Spanish Basque DPAs. It stressed that benefits of online activity for expression, interactivity and sociality (3) as well as the dangers of harassment and bullying (15).

[121] Sweden, Datainspektionen, "Publicering på Internet" (http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/publicering-pa-internet/).

[122] *Ibid*. The guidance clarified that this would not normally cover the publication of data of a purely private nature. However, it was further noted that publications which had obtained authorization from the Authority for Radio and Television would be absolutely exempt from data protection although constitutional offenses such as defamation would continue to be applicable.

[123] See *supra* note 94 and 90.

(Belgium, Estonia, France, German Schlewsig-Holstein, Norway) or even exclusive (Cyprus, Italy, Malta) emphasis was given to the publication of images, but in the other three cases the emphasis remained more general (Latvia, Luxembourg, Spanish Federal). In at least five instances (Belgium, Estonia, France, Luxembourg, Italy) other protective aspects of data protection were also explicitly stressed, whilst in at least three (France, Italy, Norway) the special protections for sensitive data were noted. Whilst stressing the default of consent, in approximately half of these cases (Belgium, Cyprus, Estonia, Italy, Spanish Federal) the guidance did explicitly acknowledge that individuals could benefit from a more permissive regime for special expressive processing such as journalism. Turning to more detail on this guidance:

- The *Belgium DPA* held that social networkers would need to secure the consent of third parties when publishing pictures or information about them and would additionally acquire general data controller responsibilities.[124] A much longer and formal Recommendation on images provided detail on the same principle, arguing that for pictures targeted on particular individuals consent should be in writing and mention both proactive and retrospective transparency rules as well as rights to rectification and opposition. Tacit consent would only be acceptable for photos incidentally including individuals and not affecting honour and good reputation. A more permissive regime, however, was applicable to anyone performing a journalistic role including individuals.[125]
- The *Cyprus DPA* held that publishing a picture or video of a third party required consent.[126] However, when adjudicating on the YouTube publication of a video showing a conflict between journalists at a press conference, the DPA determined that even when not performed by a professional, activity such as this could fall within the journalistic derogation.[127]
- The *Estonian DPA* stated that social networkers should not publish "other people's information" ("teiste inimeste andmeid") without consent, should not denigrate others and should not treat others as they would not wish to be treated.[128] Much more formal and extensive instructions were issued on the use of cameras stressing the same principle but with a special gloss for photography in public places[129] and also with acknowledgment that individuals promoting a debate on a topic of public interest could claim the journalistic derogation.[130]
- The *French DPA's* guidance on both blogs[131] and the publication of images in social networks[132] stressed the need for consent and the right to oppose publication at any time. The former also stressed the need to give

[124] Belgium, Commission de la protection de la vie privée, *Réseaux sociaux* (https://www.privacycommission.be/fr/themes-des-faq/internet/reseaux-sociaux).

[125] Belgium, Commission de la protection de la vie privée, *Recommadation no 2/2007 due 28 novembre 2007 Object: Recommandation d'initiative concernant la diffusion d'images (A/2007/033)* (https://www.privacycommission.be/sites/privacycommission/files/documents/recommandation_02_2007_0.pdf).

[126] Cyprus, ραφείου Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Χρηση του Διαδ1κτύου καi των κίνητών τηλεφώνων, 2-3 (http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/15F0006C47D1F7CDC2257562002E57F3/$file/Internet&MobilePhoneUse.pdf?OpenElement).

[127] The analysis also concluded that (at first glance) there had been no violation of the law in the instant case. See Cyprus, ραφείου Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, ΕΡΩΤΗΜΑ: Δημοσίευση εικόνων στο YOUTUBE (2010) (http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/1AD7691E1A6C7A40C225791700307E2B?OpenDocument).

[128] Estonia, Andmekaitse Inspektsioon, *Meelespea suhtlusportaali kasutajale* (2012), 5 (http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Suhtlusportaali%20kasutaja%20meelespea.pdf).

[129] Estonia, Andmekaitse Inspektsioon, *Juhend Kaamarate Kasutamise Kohta* (2013) (accessed via http://www.aki.ee/et/uudised/uudiste-arhiiv/uut-kodulehel-kaamerate-kasutamise-juhis), 8. In sum, the gloss stated that at public events tacit consent would suffice but that in other public places individuals should be informed and given the opportunity to avoid the photographed area.

[130] *Ibid*, 14.

[131] French DPA, *Blogs: la loi informatique et libertés s'applique mais ils sont dispensés de déclaration à la CNIL* (2006) (https://web.archive.org/web/20140307090640/http://www.cnil.fr/linstitution/actualite/article/article/blogs-la-loi-informatique-et-libertes-sapplique-mais-ils-sont-dispenses-de-declaration-a-la-c).

information on rights such as access and rectification, that sensitive data should not be published on websites and that retention should be proportionate to the site's purpose.[133]

- The *German Schleswig-Holstein DPA's* internet guidance stated a general rule that any private individuals ("privatperson") had the right to determine what information was published about them and by whom. Rights in relation to clearly identifiable images were particularly stressed, but with exceptions such as incidental inclusion and images related to contemporary history.[134] Targeted social networking guidance repeated the same principle in relation to images.[135]
- The *Italian DPA's* guidance was confined to two decisions (from 2003 and 2005 respectively) concerning mobile phones with still photo[136] and video[137] capability respectively. Both stipulated that general safeguards within data protection law apply, that those recorded must be informed, give written consent if the data was sensitive and by default provide consent in all cases (although the photo decision did state that certain (unspecified) statutory exceptions to this existed). Both decisions also expressly noted derogations for "journalistic activities and non-systematic publication of papers, essays and other intellectual works".
- The *Latvian DPA's* recommendation on social networking stated that publication of information about a person should only take place with their consent, defined as at least their implied understanding that they are aware of and don't oppose this.[138]
- The *Luxembourg DPA* stated that social networkers should ensure that information about others was only published with consent and that it be adequate and not slanderous, discriminatory or published out of context.[139] Other guidance stressed that data protection rights applied across the internet.[140]
- The *Maltese DPA* guidance which focused on 'street photography' not only argued that image publication (as opposed to an image kept for a purely personal activity) would fall within data protection but strongly recommended that even for photojournalism "no processing shall be allowed without the informed consent of the data subject". Where this was not realistic, facial blurring to render the individual unidentifiable was recommended. Failure to adhere to this could result in regulatory and/or civil court action. The guidance did however note the need for a balance with freedom of expression and the relevance of factors such as the public or private nature of both the photo's location and individual whose image was captured and whether publication

---

[132] French DPA, *Les conseils de la CNIL pour mieux maîtriser la publication de photos* (2012) (https://web.archive.org/web/20130125231255/http://www.cnil.fr/dossiers/internet-telephonie/actualite/article/les-conseils-de-la-cnil-pour-mieux-maitriser-la-publication-de-photos/).

[133] This guidance on blogs is not currently available on the French DPA website. However, generally more limited guidance still available stresses that publication of photos requires written consent, spreading of artistic work also requires permission and that inclusion of defamatory, libellous, offensive or racist material against a person could result in criminal prosecution (French DPA, *Les obligations du blogueur* (2009) (https://www.cnil.fr/fr/les-obligations-du-blogueur).

[134] German Schleswig-Holstein DPA, *Persönlichkeitsverletzungen im Internet, Kurzhinweise zum Vorgehen* (https://www.datenschutzzentrum.de/faq/persoenlichkeitsrechte.htm). Whilst this is an archive part of the site, substantively the same information appears on the live version at https://www.datenschutzzentrum.de/artikel/1033-FAQ-Persoenlichkeitsverletzungen-im-Internet,-Kurzhinweise-zum-Vorgehen.html#extended.

[135] German Schleswig-Holstein DPA, *Soziale Netzwerke: Wo hört der Spaß auf?*, 14 (https://www.datenschutzzentrum.de/uploads/blauereihe/blauereihe-soziale-netzwerke.pdf). Some additional guidance was given as regards fake profiles and offensive content.

[136] Italy DPA, *MMS and Data Protection* (2003) (http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1672134).

[137] Italy DPA, *Videofonini: cautele per un uso legittimo* (2005) (http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1089812).

[138] It was also specifically stated that violation could result in an administrative liability. See Latvia, Datu valsts inspekcija, *Datu valsts inspekcijas rekomendācija, Personas datu apstrāde tiešsaistes sociālajos tīklos* (2010), p. 17 (http://www.dvi.gov.lv/lv/wp-content/uploads/jaunumi/publikacijas/rekomendacija_soc.pdf).

[139] Luxembourg, Commission Nationale pour la Protection des Donnés, *Responsabilités des utilisateurs* (http://www.cnpd.public.lu/fr/dossiers-thematiques/nouvelles-tech-communication/reseaux-sociaux/responsabilite/index.html).

[140] Luxembourg, Commission Nationale pour la Protection des Donnés, *Protection des données existante sur la toile?* (http://www.cnpd.public.lu/fr/dossiers-thematiques/nouvelles-tech-communication/reseaux-sociaux/protection-toile/index.html).

was in the public interest. These comments implied some restriction of the consent (or blurring) requirement at least in a journalistic context.[141]

- The *Norwegian DPA* advised social networkers not to share photos or information about others without consent and to be careful about publishing political opinion, belief and sexual orientation information which is considered sensitive.[142] Detailed guidance on photography stressed that 'portrait' photos required explicit and informed consent, that non-offensive 'situation' photos could in principle be published without this but that as it was sometimes difficult to differentiate between these categories or determine what might be offensive, consent should be followed as a rule.[143]
- The *Spanish Federal DPA*'s internet guidance stated the general rule that individuals should not publish images, videos or any other record without the prior consent of those involved, but added that where individuals published as a journalist, the same duties and responsibilities would apply as for the professional media.[144]

Relating this back to the DPA questionnaire returns (received from all bar the Spanish Federal and Norwegian DPAs), as regards the social networker scenario all held that data protection must apply in full (D) other than the Italian DPA which stated rather that an interpretation with regard for freedom of expression was required here (C) and the Maltese DPA which stated,albeit with caveats,[145] that data protection would not apply here at all (A). The blogger scenario responses were much more varied with five (Belgium, Estonian,[146] German Schleswig-Holstein, Italian and Maltese DPAs) holding that the special expressive purposes derogation would apply (B), three (French, Latvia and Luxembourg DPA) that data protection interpreted with regard for freedom of expression was apposite (C) and one (Cyprus DPA[147]) that data protection would apply in full (D).

4. Developments Subsequent to the 2013 EEA Data Protection Authority Survey

In the process of finalising this article in February 2017, the guidance outlined above was rechecked and in all but three cases[148] found to remain on the DPA's current website. This data therefore represents an essential empirical starting-point for analysis in this area. Nevertheless, there are also some important recent CJEU judgments, further Working Party pronouncements and, most critically, the provisions of the now finalized GDPR to consider. It should also be noted that on

[141] Malta, Office of the Information and Data Protection Commissioner, *Data Protection and Street Photography* (https://idpc.gov.mt/en/Documents/Data%20Protection%20and%20Street%20Photography.pdf)
[142] Norway DPA, "Personvern i sosiale medier" (https://www.datatilsynet.no/teknologi/internett/Personvern-i-sosiale-nettsamfunn/).
[143] Norway DPA, "Publisering av bilder på nett" (https://web.archive.org/web/20130831160226/http://www.datatilsynet.no/Teknologi/Internett/Bilder-av-barn-pa-nett/). The same information is now available at under a slightly amended title at https://www.datatilsynet.no/Teknologi/Internett/Bilder-pa-nett/.
[144] Spanish DPA, *Recomendaciones a usuarios de Internet*, 44 (http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_recomendaciones_internet_052009.pdf) (currently broken link).
[145] The caveats were that "[a]pplicability depends on the type of profile and whether this is intended for personal use or for other purposes such as business, or to disseminate specific news or information of a journalistic nature."
[146] With a gloss towards category (C). See *supra* note 88.
[147] With a liberalizing gloss. See *supra* note 89.
[148] Namely, the Finnish DPA's guidance on personal webpages (*supra* note 100), the Spanish DPA's internet guidance (*supra* note 144) and a single page of guidance from French DPA concerning blogging (*supra* note 133).

24 June 2016, the UK voted by referendum to leave the EU, thereby casting into grave doubt the UK's (and also Gibraltar's) membership of not only EU itself but also wider EEA community.[149]

4.1 – Recent Court of Justice and Working Party Developments:

CJEU data protection jurisprudence has developed in an increasingly severe direction from 2014 onwards. In *Ryneš* (2014)[150] the Court held that the personal exception had to be "narrowly construed"[151] and therefore couldn't extend to household CCTV which "covers, even partially, a public space"[152] irrespective of whether the only onward disclosure was to the police. In coming to this conclusion, the Court especially stressed that "in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy", the data protection framework had to be interpreted in light of the fundamental rights now entrenched in the legally binding EU Charter.[153] In *Google Spain* (2014), a CJEU Grand Chamber found a search engine indexing published content to be "controller"[154] outside the special derogation safeguarding processing "solely for journalistic purposes".[155] It nevertheless suggested that search engines would only acquire data protection obligations where their processing "significantly and additionally" affects data subjects and even then only needed to act "within the framework of its responsibilities, powers and capabilities".[156] The *Google Spain* judgment was also strongly influenced by the need to interpret data protection in light of the *Charter*'s provisions.[157]

Guided by these developments, in 2015 the Working Party published a statement on the finalization of the GPDR which, in contrast to the reformist perspective in its 2013 statement, argued that "[t]he Working Party is 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".[158] Its opinion on drones, published at the same time, similarly backed a strict understanding of the personal exemption.[159] The previous year, the Working Party also published guidelines on *Google Spain* which accepted that search engines were non-journalistic data controllers but held that certain limitations arose from the right to freedom of expression (specifically, in this context, of internet users wanting to obtain information from the service).[160]

---

[149] The UK has championed a more permissive approach to individual publication not only internally also in pan-European forums (see *supra* note 81). Therefore, it cannot be ruled out that a UK departure from the EU (and probably also the EEA) may have a wider impact on European law and policy in this area.
[150] C-212/13 *František Ryneš* v. *Úřad pro ochranu osobních údajů* (2014), EU:C:2014:2428.
[151] at [19].
[152] *Ibid* at [33].
[153] *Ibid* at [28].
[154] C-131/12 *Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* at [32].
[155] *Ibid* at [85].
[156] *Ibid* at [38].
[157] *Ibid* at [68].
[158] European Union, Article 29 Working Party, *Appendix: Core topics in view of the trilogue* (2015), 3.
[159] See European Union, Article 29 Working Party, *Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones* (WP 231) (2015), 9.
[160] European Union, *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "*Google Spain and Inc V. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*" C-131* (WP 225) (2015), 6.

4.2 – The General Data Protection Regulation (GDPR)

Initially proposed by the Commission in 2012,[161] the GDPR was finally agreed in April 2016 and will replace Directive 95/46 on 25 May 2018.[162] This instrument reflected a belief that "[r]apid technological developments and globalisation"[163] "require a strong and more coherent data protection framework … backed up by strong enforcement".[164] The Regulation therefore expands the Directive's already stringent default substantive standards through, in particular, moreextensive provisions for ensuring transparency for data subjects[165] and more discipline provisions especially as regards specifying arrangements between joint controllers[166] and between controllers and processors.[167] The data protection principles are augmented to include references to transparency,[168] data security[169] and controller accountability;[170] the private and, more especially, public supervisory systems are also significantly enhanced (notably through empowering DPAs to initiate fines of up to €10M or €20M for most breaches of the law).[171] Optional limited derogations for Member States continue but are generally subject to tighter specification[172] and will no longer cover the data protection principles in and of themselves. They also can't limit either the discipline provisions or the supervisory system, both of which are subject to the expansions noted above. Turning to the personal exemption, the existing wording excluding only processing "by a natural person in the course of a purely personal or household activity" is retained verbatim,[173] but with a new Recital worded as follows:

> This Regulation should not apply to processing of personal data by a natural person in the course of a purely personal or household activity and thus without a connection with a professional or commercial activity. Personal and household activities could include correspondence and the holding of addresses or social networking and on-line activity undertaken within the context of such personal or household activities. However, this Regulation should apply to controllers or processors which provide the means for such personal and household activities.[174]

Turning finally to provisions dealing with freedom of expression, article 85(2) sets out a slightly expanded version of the special expressive purposes derogation,[175] with article 85(3) requiring that national laws adopted in this area be notified to the Commission. At the same time, a new provision included in article 85(1) states more broadly (and cryptically) 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".

---

[161] See *supra* note 80.
[162] Regulation 2016/679, art. 99 (2).
[163] *Ibid*, recital 6.
[164] *Ibid*, recital 7.
[165] *Ibid*, art. 12 to 15.
[166] *Ibid*, art. 26.
[167] *Ibid*, art. 27.
[168] *Ibid*, art. 5(1)(a).
[169] *Ibid*, art. 5 (1) (f).
[170] *Ibid*, art. 5 (2).
[171] Or, in the case of an undertaking, either 2% of 4% of annual global turnover if this is higher. See *ibid*, art. 79.
[172] Article 23 (2) in particular lays down eight types of specific provisions which legislative measures made under this article may have to include to be valid.
[173] Regulation 2016/679, art. 2 (c).
[174] *Ibid*, recital 18.
[175] *Ibid*, art. 85 (2).

5. Analysis and Future of Data Protection and Individual Publication

The European data protection framework has from its inception been predicated on providing a "high level of protection"[176] for individuals in relation to their privacy and related rights. Since 2009 this stance has been augmented by the inclusion of data protection itself as a fundamental right within the EU Treaties.[177] It is in this context that EEA DPAs have generally adopted a theoretically strict interpretative approach to regulation here, even as regards the mushrooming phenomenon that is individual publication online. At the same time, however, there is also a good deal of confusion and disparity even between the DPAs themselves, as well as a clear gap between most DPA guidance and social realities online. On the one hand, an unduly stringent and bureaucratic approach risks attempting both to indirectly chill and even directly curtail legitimate rights to freedom of expression, as well as setting up legal standards which are impossible to practicably achieve. On the other hand, and equally problematically, a failure to provide effective and appropriate safeguards may leave individuals without adequate redress in relation to very real, serious and growing threats to their rights, albeit emanating from other natural persons and even if now entrenched as purportedly acceptable social practices in parts of the online world. From the point of view of data protection law, this tension potentially relates to at least three areas – (i) the special expressive purposes derogation, (ii) the personal exemption and (iii) other limited derogations which may be available for safeguarding freedom of expression. It is also apparent that the impending coming into force of the GDPR provides an important opportunity to secure a more consistent and balanced approach to these important and challenging issues. This section will therefore analyse all of the data presented above and seek to develop a more coherent interpretation as regards each of these three discrete legal aspects.

5.1 – The Special Expressive Purposes Derogation

Given that the special expressive purposes derogation constitutes the only clause in the current Directive and still the principal one in the new Regulation which is explicitly designed to reconcile data protection with free speech, it makes sense to commence analysis here. This provision currently shields processing "solely for journalistic purposes or the purpose of artistic or literary expression"[178] and in the future will shield processing "for journalistic purposes or the purpose of *academic* artistic or literary expression".[179] As an (albeit particularly permissive) derogation rather than a full exception, it mandates the establishment by Member States of a special regime which (within a certain margin of manoeuvre) ensures a balance between two competing rights.[180] In referring to special purposes rather than special actors, it is not restricted to professional journalists, artists and academic or non-academic writers but rather is in principle open to everyone (a reality given emphasis by the CJEU in *Satamedia*) including private individuals. Although only approximately half of those DPAs which provided some guidance on individual publication addressed this issue, the great majority that did gave voice to this crucial liberal

[176] Directive 95/46, recital 8; Regulation 2016/679, recital 10.
[177] *TFEU*, art. 16; *EU Charter*, art. 8.
[178] Directive 95/46, art. 9.
[179] Regulation 2016/679, art. 85(2) (emphasis added).
[180] Directive 95/46, recital 37; Regulation 2016/679, recital 153.

democratic point. In contrast, in the DPA questionnaire only a minority[181] accepted that the individual in the blogger scenario fell within this, notwithstanding that they were disseminating material ("celebrity gossip") which is widely recognised as journalistic when carried out by the professional media.[182] The GDPR's apparent removal of the requirement that processing be conceptualized as "solely"[183] for the special expressive purposes as well its general emphasis on construing this clause "broadly"[184] provides an opportunity to decisively reject such prioritization of expression by actors with a particular professional status. Nevertheless, whilst wider than just journalism (let alone professional as opposed to 'citizen' journalism), the clause rightly remains tied to the pursuit of expressive purposes which, in principle, have a particularly strong social value. Publication which aims at the dissemination of a message ("information, opinions or ideas"[185]) to the collective public, including not only those which are narrowly journalistic but also those which instantiate an artistic, literary and now also an academic purpose, should be safeguarded under this derogation. Nevertheless, many forms of individual publication online fail to instantiate such purposes.[186] Thus, not only are a good number of blogs "more akin to diaries than news articles, op-ed columns or scholarship"[187] but most forms of social networking are either exclusively or very predominantly concerned only with self-expression and a linked general freedom to converse. Like search engine indexing in *Google Spain*, these forms of processing cannot fall within a reasonable interpretation of the special expressive purposes derogation even if generously construed.

5.2 – The Personal Exemption

The strong focus on self-expression in many cases of individual publication may suggest that data protection's personal exemption should apply here. In general, however, current DPA interpretation firmly rejects this. Thus, only a small minority of DPAs (12% and 16% respectively) who provided standard responses to the blogger and social networker questionnaire scenarios held that such activity would be exempt (see Charts 1 and 2 above). Similarly, as regards the published guidance, not only did only around half of those falling within potentially permissive group (itself

[181] A few of the DPAs (German Federal, German Mecklenberg-Vorpommern, German Schleswig-Holstein, Hungary, Lichtenstein) which opted to stricter forms of regulation here may have felt constrained by their national data protection laws attempting, unlike EU law itself, to confine the special purposes to the institutional media alone. See *supra* section 2.2 above.

[182] Celebrity gossip journalism is sometimes controversial as the harms such dissemination causes can be both serious and out of balance with the objective value of this to the public. Nevertheless, this highlights not that this such activity cannot be journalistic but rather that in specific instances it might fail to respect the need for a proper balance between competing rights which is (or should be) an integral part of the special expressive purposes derogatory regime at Member State level.

[183] Strangely, whilst this restriction was removed from article 85(2) itself, it was retained in recital 153. In any case, it seems clear that it will remain necessary that that any activity protected by this clause can be conceived as falling "entirely" although not "exclusively" within the special expressive purposes. For an analysis of this distinction see David Erdos, "Freedom of Expression Turned On Its Head? Academic Social Research and Journalism in the European Privacy Framework" [2013] *Public Law* 52-73.

[184] Regulation 2016/679, recital 153.

[185] *Satamedia* at [61].

[186] See the similar analysis in the 2013 Working Party statement: "It would be wrong to say that all of an individual's personal online activity is being done for the purposes of journalism or artistic or literary expression" (European Union, Article 29 Working Party, *Statement of the Working Party on Current Discussions*, 1-2).

[187] Daniel J. Solove, *The Future of Reputation*, 24.

only 27% of the DPA total) clearly suggest that self-expression might be fully exempt,[188] but the guidance falling within the other groupings was grounded on the notion articulated in *Lindqvist* that all indeterminate publication of personal information (at least if related to third parties) necessarily fell within data protection's scope. Such an understanding similarly underpinned the Working Party's opinion on social networking from 2009 and strongly influenced its 2015 statement on the GPDR and its opinion on drones. On the other hand, the Working Party's 2013 statement clearly supported some deployment of the personal exemption in this area. Moreover, at least three arguments do support a wide role for the personal exemption here. Firstly, the numerous substantive and also procedural duties which default data protection would impose on controllers are challenging even in relation to large organizations; in the context of individuals they therefore pose an acute risk of being highly disproportionate or even impossible to discharge.[189] Secondly, self-expression and the linked freedom to converse further vitally important human values, notably the "right to identity and personal development".[190] It is therefore vital to take fully into account the impact which legal restrictions may have on such values,[191] even if existing freedom of expression jurisprudence does not fully do so yet.[192] Thirdly, given the explosion of the individual publication online, the application of data protection framework in this area poses a serious and growing "logistical challenge"[193] especially for DPAs and in particular if they are expected to respond in full to each and every complaint made.

At the same time, however, there are also strong arguments against expanding the scope of the personal exemption to cover individual publication in general. First and foremost, as explored in section 2.2 above, in an age of ubiquitous networked computing such activity can seriously undermine an individual's right to the protection of personal information. It is true that, as the Working Party's 2013 statement pointed out, a variety of other national laws do play a role within this space.[194] However, these laws remain entirely unharmonized and, when analysed from the perspective of data protection, may suffer from fairly obvious deficiencies. To take one example, English defamation law includes a 'single publication rule' which generally prohibits a claimant pursuing a remedy for the ongoing publication of defamatory information if that information was

[188] Such a categorical approach was clearly present in the case of the UK and arguably also present in the case of Finland, Ireland and Slovenia. In contrast, the Czech and Icelandic guidance clearly still sought to apply data protection to some extent even within this context.

[189] See Brendan Van Alsenoy, "The evolving role of the individual under EU data protection law", 15.

[190] *P. G. and J. H. v United Kingdom* (44787/98) (2001) at [56]. It is striking that judicial recognition of these values has been forthcoming so far not in a freedom of expression context but rather in cases involving the protection of private life.

[191] In this context, the Article 29 Working Party's 2013 statement rightly "notes the positive impact of much online data processing done by natural persons – in terms for example of cultural exchange, the development of new forms of discourse and democratisation" and rightly argued that "[d]ata protection law must be applied in a way that these positive aspects of individual's personal use of the online world are allowed to flourish" (European Union, Article 29 Working Party, *Statement of the Working Party on Current Discussions*, 2).

[192] This current deficiency may be explained both by the narrow institutional nature of most freedom of expression jurisprudence (see e.g. "almost all free expression jurisprudence is, today, media jurisprudence" (Helen Fenwick & Gavin Phillipson, *Media Freedom Under the Human Rights Act* (Oxford University Press 2006), 2) and by the fact that high impact individual publication has only become a widespread phenomenon relatively recently and so litigation in this area is in many respects embryonic.

[193] European Union, Article 29 Working Party, *Statement of the Working Party on Current Discussions*, 7.

[194] The Working Party noted laws relating to libel, harassment, malicious communications, threatening behaviour, incitement, persecution and discrimination (European Commission, Article 29 Working Party, Statement of the Working Party on Current Discussions, 6). However, other legal provisions which appear clearly relevant are general protections in tort law relating to the protection of private life and, in many jurisdictions, also one's image.

initially published more than one year previously.[195] This conflicts markedly not only with data protection's understanding that electronic publication is an ongoing 'processing' activity but also that the passage of time may be an aggravating rather than mitigating factor when assessing the legality of continuing to publish stigmatic material relating to an individual.[196] Procedurally, these laws also fail to provide a cognate to the DPAs which, at least in serious cases, should provide assistance to data subjects in their quest for a vindication of rights - redress which in many jurisdictions otherwise entails the risk of very considerable legal expense.[197] Secondly, and relatedly, European data protection law's broad safeguarding purpose – encapsulated in *Google Spain* as ensuring the "effective and complete protection of data subjects, in particular of their right to privacy"[198] - could simply not be achieved if a general and absolute exemption was provided for the individual publication of personal data. To the contrary, as Xanthoulis argues:

> [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.[199]

It must be an imperative to avoid an interpretation of the law which would lead to such a result.[200] Thirdly, the GDPR's continued exclusion only of processing "by a natural person in the course of a purely personal or household activity" places strong limits on a broad construction of the personal exemption. It is true that any reasonable interpretation of this provision in today's reality requires the adoption of a purposive rather than strictly black-letter approach. Thus, a rigid interpretation of

---

[195] UK, Defamation Act 2013, s. 8 and Limitation Act 1980, s. 4A. It is true that under the Limitation Act courts do retain discretion to waive such limitation periods on grounds of equity (Limitation Act 1980, s. 32A). However, not only does this remain an individual rather than a structural solution, but in practice it is rare for such statutory periods to be set aside.

[196] Thus, the Court of Justice in *Google Spain* argued that "even initially lawful processing of accurate data may, in the course of time, become incompatible with the directive where those data are no longer necessary in light of the purposes for 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 those purposes and in the light of the time that has elapsed." (at [93]).

[197] A striking example is legal action taken (which ultimately involved Facebook, YouTube, Google and others) by Irish student Eoin McHugh to remove material relating to an internet video clip falsely portraying him as a taxi fare evader. As reported last year, this led to him facing potential costs of €1.9m. See "Student who took legal case over taxi video faces €1.9m costs", *Irish Times*, 12th June 2015.

[198] C-131/12 *Google Spain* (2014) at [38].

[199] 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* (Springer, 2013), 141.

[200] In certain cases involving UGC it may be possible to adopt a broader conceptualization of the personal exemption so long as the UGC service provider is itself subject to EEA law and can be considered to be determining all of the core means and purposes for processing (and therefore acting as 'sole' controller). This, for example, might be the case when a user uploads a review to a rating website which falls within the purposes and published terms and conditions of such a site. The user in this case could simply be considered an individual from who personal information was being obtained by this controller indirectly (see Directive 95/46, art. 11 and Regulation 2016/679, art. 14). In many other cases, however, it must be recognised that the user is acting so autonomously in determining the purposes and means of processing (at least jointly with the service provider) such that this would not be appropriate. This would be the case with many forms of social networking and perhaps all blogging activity. In any case, it is recognised that where a user situated within Europe is interacting with a website not established in Europe or otherwise subject to European law, it would still be necessary to adopt a stricter interpretation of the personal exemption in order to ensure the effective protection of data subjects.

the phrase "by a natural person" (rather than the broader one of "by or on behalf of a natural person") may suggest that the individual themselves must directly carry out the processing operations using his or her own equipment (e.g. a personal computer or mobile phone) rather than delegating this to a processor acting under their instruction (e.g. an online platform contractually limited to providing access only to a restricted number of persons predetermined by the individual).[201] Similarly, the CJEU's *Lindqvist* holding that the personal exemption cannot cover any processing "accessible to an indefinite number of people"[202] would if strictly interpreted lead to the conclusion that even if an individual was publishing only information exclusively about themselves they may have a legal requirement, for example, to ensure the accuracy of the data,[203] register the processing with the DPA authority[204] and even in some circumstances obtain the DPA's authorization for processing.[205] However, even the most stringent DPAs implicitly accept that the personal exemption covers all processing of information exclusively about the individual him or herself and that it can in principle shield an individual in relation to processing carried out not only by them directly but also on their behalf. Many, including the Working Party itself,[206] go much further and advocate the general right to pseudonymous profiles on social networking sites despite the fact that, in circumstances when data protection law applies in full, this would almost inevitably conflict with the requirement for every controller to disclose their real identity to data subjects at least when collecting information directly from them.[207] The broader range of activity referred to in recital 18 of the GDPR compared to recital 12 of the current Directive – notably the addition of "social networking and online activity" – must also be recognized. However, not only does this recital pointedly only state that "personal and household activities could [not must] include … social networking and on-line activity undertaken within the context of [personal or household] activities"

[201] As Helberger and van Hoboken note if, as would be the case under a rigid interpretation, "the factual circle of the processing of the personal data involved always has to be confined to the personal or household sphere" then "the household [or personal] exemption becomes almost meaningless" since "with the rise of cloud competing … hardly any processing of information is confined to the factual personal sphere" (Natali Helberger and Joris van Hoken, "Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers" [2010] *Computer Law International* 101-109 at 103).

[202] *Lindqvist* at [47].

[203] Directive 95/46, art. 6 (d).

[204] *Ibid*, art. 18.

[205] *Ibid*, art. 20. Cunha, Marin and Sartor similarly note that even individuals freely publishing data about themselves exclusively "appears to be incompatible with some paternalistic data protection rules, literally understood. Consider for example the provision contained in various EU member states' data protection regulations according to which sensitive data can be published only with the authorization of the data protection authority. Assume that a gay person decides to 'come out of the closet', and declare his sexual identity on his blog or public Facebook profile. It would appear that he has published sensitive private data with the consent of the data subject (himself), but without the authorization of the data protection authority, committing therefore a punishable offence … The same would apply to a person affected by breast cancer, who tells on her online blog how she is bravely fighting against her illness, without losing hope and interest in life, to encourage others to do the same. She would be engaging in an illicit activity, for publishing health information without the required authorization" (Mario Viola de Azevedo Cunha, Luisa Marin and Giovanni Sartor, "Peer-to-peer privacy violations and ISP liability: data protection in the user-generated web" (2012) 2(2) *International Data Privacy Law* 50 at 52.

[206] See *supra* note 76.

[207] Directive 95/46, art. 10. Van Alsenoy et. al. comment similarly that article 10 of the Directive "may impose a significant limitation on the pseudonymous use of SNS, whereas several Data Protection Commissioners have only recently advocated that SNS providers should enable and encourage the creation and use of pseudonymous profiles" (Brendan Van Alsenoy, Joris Ballet, Aleksandra Kuczerawy and Jos Dumortier, "Social networks and web 2.0: are users also bound by data protection regulations?" (2009) 2(1) *Identity in the Information Society* (65) 76.

but a decision was made to maintain the reference only to "purely" personal or household activity in the normative part of the Regulation, in full recognition that this term has been consistently narrowly construed by the CJEU from *Lindqvist* to *Ryneš*.[208]

Ultimately, the need to avoid outcomes which are clearly disproportionate and unfairly chilling of self-expression points to a strong case to effect an expansion of the personal exemption even into the area of individual publication of third party information. At the same time, it must be recognised that recent *Charter*-influenced CJEU jurisprudence outlined above emphasizes that data protection's core purposes require that a strict construction of the personal exemption be maintained as regards the processing of personal data which is clearly "liable to infringe fundamental rights, in particular the right to privacy".[209] Given this, the personal exemption should be reinterpreted to exclude individual publication from data protection law but only so long as the publication in question does not pose a serious *prima facie* risk of infringing the core privacy, reputation and related rights which data protection is dedicated to safeguard.[210] At the least, such a construction would completely exclude individual liability in relation to the sort of "harmless", not "annoying" or not "offensive" publications mentioned within the 'mid-range' guidance of the Danish, Greek and Swedish DPAs explored above.[211] On the other hand, publication which is *prima facie* 'offensive' due, for example, to its pejorative nature (e.g. a clearly negative review of a teacher, sole trader or even personal acquaintance), its disclosure of private details concerning personal life (especially if related to sensitive categories of data such as criminality, sex or health life) and/or because of an incessant and focused observation which amounts to a potentially unwarranted form of surveillance would rightly continue to fall outside this absolute exemption.

5.3 – Limited Derogations Safeguarding Freedom of Expression

[208] Both outcomes are at variance with the Council of the EU's text which had proposed a deletion of "purely" from the substantive provision and a statement in the Recital that "[p]ersonal and household activities include social networking activities and on-line activity undertaken within the context of such personal household activities". See Council of the EU, General Data Protection Regulation – Preparation for a General Approach (9565/15) Annex (2015), recital 15 [later renumbered to rectal 18] and art. 2 (2) (d) [later renumbered to art. 2 (2) (c)].

[209] *Ryneš* at [29].

[210] In requiring that beyond indeterminate publication an additional factor ("serious *prima facie* risk of infringing … privacy, reputation and related rights") must be present before genuinely individual publication is subject to data protection, this construction bears some resemblance to the Article 29 Working Party's 2013 proposal (which it implicitly withdrew in 2015). However, the essential difference is that this additional factor, unlike many of the ones mentioned in the Working Party's proposed Recital, explicitly synergises with and therefore safeguards the core purposes of data protection. Moreover, opting for a bi-factorial rather than multi-factorial test dramatically reduces the legal uncertainty (and consequent practical reality of inappropriately wide DPA discretion) which would have likely bedevilled the Working Party's 2013 proposals.

[211] Moreover, in contrast to the suggestion made by the Danish DPA in some of its guidance explored above, the test would ultimately be objective not subjective. Certainly, any case made by the data subject not to publish (or to cease publishing) information related to them should be taken into account and will clearly sometimes be compelling (e.g. if an individual fleeing a violent former partner requests that an apparently innocuous yet identifiable picture of them which nevertheless links them to a specific time and place not be published or be removed). However, information which is objectively inoffensive should not lose its exemption simply on account of an idiosyncratic opposition by an identified data subject. Otherwise, the exemption would only protect information published with at least the implied consent of the data subject, a stipulation which would be too restrictive of valuable forms of self-expression.

Notwithstanding both a broadened approach to the personal exemption and a generous interpretation of the special expressive purposes derogation, a good deal of individual publication would continue to fall outside both provisions. Whilst some instances of this kind of publication are manifestly unwarranted,[212] many others instantiate forms of self-expression and the freedom to converse which are in principle of legitimate value. Thus, Daphne Kellner 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 may not be covered [by the special expressive purposes derogation] … This kind of material is a far cry from the privileged – and often professionalized and even licensed – categories of expression listed in Article 85.2. But it is precisely this democratic cacophony that makes the Internet so different from prior speech platforms. Without clear free expression protections … this speech is at risk.[213]

Notwithstanding contrary suggestions in much of the DPA guidance considered above, communications such as these would clearly be unduly censored if only permitted with the identified individual's consent. Moreover, even if such a stringent interpretation of the law was rejected, these forms of publication would still be inappropriately chilled if required to adhere in full to data protection's general rules and disciplining provisions, not least since stipulations such as detailed requirements for transparency notices, for the registration or documentation data processing and for ensuring specific contractual arrangements with data processors imply "expertise and resources which are typically only available to organisations"[214] and, therefore, go beyond the *capacity* which can reasonably be expected in the context of personal activity (even if connected to the indeterminate dissemination of information). On the other hand, given that the identified individual's rights may be very significantly engaged by such content and in the absence of the strong public interest rationale which undergirds lawful special expressive purposes activity, data protection law rightly gives emphasis to ensuring that this individual is properly safeguarded. In sum, therefore, what appears necessary is for the law to encapsulate a new type of balancing of rights and interests which (in contrast to that required by the special expressive purposes derogation) also guarantees the subject's core substantive and supervisory data protection rights.

In principle, Directive 95/46 includes general derogatory clauses which recognize that the protection of freedom of expression as well as other "rights and freedoms"[215] may require such a crafting of such a middle area between the deployment of the special expressive purposes derogation[216] and the full application of data protection's default provisions. However, these clauses, which were outlined in sub-sections 2.1 and 2.2 above, have two serious drawbacks. In the first place, they are officially styled as optional[217] and, as a result, have rarely been deployed by Member States in the free speech area. Secondly, they fail to include within their scope a number of

---

[212] Such content ranges widely from the phenomenon of 'revenge porn' to vicious public shaming campaigns targeted towards ordinary members of the public for trivial, or even wholly innocuous, activity.

[213] Daphne Kellner, "The GDPR's express free expression provisions" (2016) (manuscript on file with author).

[214] Brendan Van Alsenoy, B., "The evolving role of the individual under EU data protection" (2015).

[215] Directive 95/46, art. 13 (f). For the cognate provision applicable to the sensitive personal data rules, which is grounded on a test of substantial public interest and/or the provision of suitable safeguards, see arts. 8 (4) – 8 (5).

[216] Directive 95/46, art. 9.

[217] Of course, given that EU Member States are mandated to act consistently with European human rights standards when implementing EU law, it could be argued that they must invoke these clauses to the extent required to protect freedom of expression. Notwithstanding such legal theories, the fact remains that this has not happened.

the law's problematic provisions including detailed rules on overseas data transfer,[218] contractual relationships between controllers and processors[219] and the requirement to register and/or document data processing activities.[220] Nevertheless, notwithstanding the general failure to deploy these clauses in formal law, the CJEU signalled early on in the *Lindqvist* case that both "authorities and courts" had a duty in certain cases outside of special expression to explicitly interpret data protection with regard for freedom of expression.[221] Turning to the DPA questionnaire, the need for such an explicit weighing or balancing through interpretation was recognized by 60% of authorities in the case of the amateur 'celebrity gossip' blogger and almost one third in the case of the social networker photo 'tagger' scenarios (see Charts 1 and 2). However, as argued in sub-section 5.1 above, in light of the its subject matter, the blog would appear to fit better within the more forgiving special expressive purposes derogation. Moreover, the logic presented in sub-section 5.2 above would suggest that the social networker scenario might actually fit within the personal exemption, although clearly this would depend at least on the nature of the photo at issue.[222] Turning to the DPA website review, almost no regulator's published guidance set out a non-special purposes interpretative balance outside of the kind of essentially 'inoffensive' publication which, as argued above, should fall within the personal exemption.[223] Thus, although the *Lindqvist* dicta is clearly helpful as far as it goes, these facts highlight one of its key difficulties, namely, that it remains uncertain when DPAs (or indeed courts) will accept that it does indeed apply. It is also unclear whether the *Lindqvist* instruction should lead (in appropriate circumstances) to whole sections of the law, such as the rules as regards transparency or sensitive data, being disapplied or whether, to the contrary, it can only result in already open-textured or clearly non-fundamental elements of the law being given a particular gloss. In any case, even if *Lindqvist* does mandate radical interpretative surgery, the fact that the statutory law itself fails to provides for the necessary balance sits in strong tension with the need for limitations on freedom of expression (and indeed other fundamental rights) to be "provided for by law" (as per the *EU Charter*)[224] or "prescribed by law" (as per the *European Convention)*.[225]

---

[218] Directive 95/46, arts. 25-26.

[219] Directive 95/46, art. 17 (2)-(4).

[220] It is true that art. 18 (2) does allow member states to provide for exemptions where processing is "unlikely … to adversely affect the rights and freedoms of data subjects". However, in the area we are now discussing some risk of data subject's rights and freedoms must be present. In any case, under art. 21 (3), Member States must still ensure that any person can still demand the same information (other than concerning data security) which would otherwise be notifiable to the DPA directly from the controller (or other designated body). A documentation of data processing may, therefore, still be necessary.

[221] C-101/01 *Lindqvist* at [87].

[222] Clearly, if the photo clearly intruded on a private and intimate activity or was designed to inflict shame on an individual, then it would not be exempt. It is also recognised that the 'tagging' of the photo may be used by the social network in order to market their services to the identified individual or for other purposes going well beyond public expression. However, generally speaking, it would be the social network rather than the uploading user who would be responsible for such additional processing activities. Matters would likely be different if the user was clearly informed and explicit of the additional processing and took a decision to bring it about.

[223] Potential exceptions to this include the Danish DPA guidance as regards the expression of opinions and the Icelandic DPA more generally. Interestingly, both fall within the small number of jurisdictions have adopted a broad reference to freedom of expression within their data protection law. See David Erdos, "Data Protection Confronts Freedom of Expression on the 'New Media' Internet" at 551.

[224] EU Charter, art. 52.

[225] European Convention, art. 10. A further difficulty with the *Lindqvist* dicta is that it was only explicitly directed to the interpretation of the Directive itself rather than that of the transposition national law. However, in *Promusicae* the Court of Justice, albeit in the context of an analysis of the more specialized e-

As noted in section 4.2 above, similarly to the existing Directive, the GDPR also contains general clauses explicitly allowing for (but not mandating) derogations to be made outside of the special expressive purposes but in the interests of freedom of expression. In sum, under article 23, derogations may be made from the transparency rules and certain data subject rights, together with the data protection principles in so far as these correspond to these detailed rules and rights, so long as any restrictions are made by way of a legislative measure, respect the "essence of the fundamental rights and freedoms" and are a "necessary and proportionate measure in democratic society to safeguard" *inter alia* "the rights and freedoms of others". Rather more restrictively, derogations may also generally be made from the sensitive data regime on the basis of a law which respects the essence to the right to data protection, provides for "suitable and specific measures to safeguard the rights and the interests of the data subject" and applies to processing which is "necessary for reasons of substantial public interest".[226] (As regards data relating to criminal convictions and offences only, the GDPR states that it is simply necessary for the law to set down "appropriate safeguards".)[227] However, no derogatory provision covers the data protection principles in and of themselves,[228] the need for a legal basis for processing[229] and the discipline provisions including the overseas transfer rules,[230] the requirement to document data processing,[231] to establish arrangements where a joint controller situation arises[232] and to comply with detailed requirements as regards the engagement of a data processor.[233] It is therefore clear that, from the point of view of facilitating the kind of balance under discussion here, these provisions suffer from similar drawbacks to the cognate provisions in the existing Directive and, once the generally more stringent default nature of the GDPR is taken into account, one of a more serious nature.

On the other hand, as likewise outlined in sub-section 4.2, the GDPR also contains a clause additional to the special expressive purposes derogation stating 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".[234] Whilst unfortunately lacking any further specification, this clause does clearly require Member States to use the derogations available elsewhere in the GDPR in order to pass discrete legislation giving effect to this need for balance. However, in two further respects this clause is at least extremely opaque and potentially very restrictive. Firstly, given that, in contrast to the special expressive purposes derogation which immediately follows,[235] it

---

Privacy Directive 2002/58, indicated that this interpretative obligation should in fact be read to encompass also national transposing law (C-276/06, Productores de Música de España (Promusicae) v Telefońica de España SAU, EU:C:2008:54 at [68]). In any case, this distinction will become much less important in the era of the Regulation since most of provisions which are clearly problematic will be in principle directly effective under the Regulation itself.

[226] Regulation 2016/679, art. 9 (2) (g).

[227] *Ibid*, art. 10.

[228] I*bid*, art. 5.

[229] *Ibid*, art. 6.

[230] *Ibid*, chapter V.

[231] *Ibid*, art. 30. Assuming that an amateur individual may be treated as an organisation comprised of just one person, art. 30 (5) does establish that documentation is not required unless processing is likely to result in a risk to the rights and freedoms of data subjects and/or the processing is not occasional and/or the processing includes any sensitive data. It is clear that the processing under examination here will fail at least the first and very possibly the other two elements of this test.

[232] Ibid, art. 26. The reality of joint control as regards the determination of purposes and means would appear to be perfectly possible as regards, say, an individual social networker and a corporate social networking site.

[233] *Ibid*, art. 28.

[234] *Ibid*, art. 85 (1).

[235] *Ibid*, art. 85 (2).

does not set out any special vires,[236] it is unclear whether it grants Member States an ability to grant necessary derogations here even if they are not otherwise permitted under the GDPR. Secondly, it is not clear whether this clause mandates (or even allows for) DPAs (and courts) to grant derogations here in the absence of a specific Member State law setting these out.

Taking these two issues in turn, it is clear that the use by Member States only of derogation vires otherwise available in the GDPR will as explored above still lead to a disproportionate burden being placed on individuals. On the other hand, the deliberate absence of express additional vires must be acknowledged. In light of this dilemma, it seems appropriate to recognise the existence of implied vires here but to interpret these narrowly and strictly.[237] In sum, derogations made under this clause should not undermine either the substantive or supervisory essence of European data protection's general derogatory scheme. Thus, at a substantive level, no derogation should be possible from the need for a legal basis for processing[238] or from the data protection principles in and of themselves.[239] Turning to sensitive data, so long as a purposive rather than literal interpretation of this concept is adopted,[240] it may be thought that a rule mandating consent here is not inappropriate.[241] However, this would overlook particular circumstances when publication absent consent may be warranted. For example, an accurate and not manifestly unfair (albeit clearly negative) report on a sole trader such as a builder could very easily at least imply criminal activity such as fraud or health difficulties which rendered that person incapable of performing their task effectively. In any case, it seems unlikely that the GDPR's definition of consent[242] including in particular its mandatory and categorical rescinability[243] is generally appropriate in a self-expressive context. Given this, broadly paralleling the 'public interest' derogations from the sensitive data rules set down elsewhere in GDPR,[244] exceptions here should in each particular case require strong justification and a heightened responsibility from the controller to safeguard the remaining rights of the data subject. As regards the discipline provisions such as documentation and arrangements for joint controllers and/or processors, both the instrumental, as opposed to intrinsic purposes of these provisions, and the near certainty of a disproportionate outcome if these were fully applied in this context must be recognised. Given this, individuals should only be subject to the general security

[236] Or indeed and again unlike the special expressive purposes derogation (*ibid*, art. 85 (3)) to require Member States to notify the Commission of law adopted under the clause.
[237] Such an approach would mirror the construction and interpretation of implied terms and licenses within private contractual law.
[238] Absent the data subject's consent (Regulation 2016/679, art. 6 (1) (a)), the only possible basis would be that "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subjects which require protection of personal data, in particular where the data subject is a child" (Regulation 2016/679, art. 6 (1) (f)). In other words, a balancing of interests (and indeed rights) would be required.
[239] *Ibid*, art. 5.
[240] Such an approach has been promoted both the Working Party and by Recital 34 of Directive 95/46 (see *supra* note 78). It receives similar backing from Recital 51 of the Regulation which seeks to define such data as that which is "[p]articularly sensitive in relation to fundamental rights and freedoms".
[241] Even if this were the case, it must be recognised that allowing for data relating to criminal convictions and offences to be processed in this context even with consent would require a derogation from the categorical ban on processing such data in the private sector as set out in art. 10 of the Regulation.
[242] *Ibid*, art. 7.
[243] *Ibid*, art. 7 (3).
[244] See Regulation 2016/679, art. 10 (for data relating to criminal convictions and offences) and art. 9 (2) (g) (for other categories of sensitive data). It should be noted that at least art. 10 would appear permissive enough to allow for a derogation in favour of self-expression in any case.

requirements[245] found within the data protection principles themselves.[246] On the other hand, moving to the supervisory provisions, in light of the GDPR's data protection principle's new focus on controller accountability[247] and the lack of effective redress for serious problems highlighted in section 2.2, there is no case for exempting this activity from ultimate DPA oversight.[248] For much the same reason, it is also essential that data subjects retain an ability to take action to bring illegal publication relating to them to an end, as well secure compensation for any damage suffered as a result.[249]

Turning to the second issue, the clause's reference to Member States proactively taking action "by law" in this area and the CJEU's general insistence that domestic constitutional provisions should not in and of themselves trump provisions in EU law[250] both point to a requirement that Member States adopt specific legislation giving effect to the freedom of expression clause in this area. This legislation[251] should provide that private individuals processing for their own expressive purposes (but outside both the household exemption and the special expressive purposes derogation) should only be subject to a minimum of substantive and supervisory data protection requirements such as those set out above.[252] Nevertheless, especially given the freedom of expression clause's problematic lack of specificity, it must be recognised that some Member States

[245] *Ibid*, art. 5 (1) (f).

[246] On the other hand, in light of the generally much greater capabilities of social networking sites and other user generated content services, if and when these actors operate as joint controllers (and even if the other controller is an individual) it may not be inappropriate to subject them to the detailed rules which apply here.

[247] I*bid*, art. 5 (2).

[248] Nevertheless, given the fearsome nature of the powers given to DPAs under the Regulation, Member States should lay down "additional safeguards" for their exercise in this area as is permitted under art. 58 (4). It is, however, recognised that such safeguards would need to be drafted with care in order to avoid encroaching on DPA independence which is protected in both art. 8 of the *EU Charter* and art. 52 of the Regulation.

[249] This would require not only retention of the right to compensation (Regulation 2016/679, art. 82) but also at least some cognate to the rights to the rectification of inaccuracy and the erasure of other types of illegal data (*ibid*, arts. 16-17).

[250] C-11/70 *Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel* (1970), EU:C:1970:144..

[251] In reality, it seems likely and indeed important that any such legislation would attempt to deal with a wider range of expressive concerns than those canvassed in this article including the activities of organisations which facilitate (and, often mould, aggregate and push) private individual expression (e.g. social networking sites) as well as those which facilitate a wide variety of public expressive activities but do not themselves instantiate either individual expression or the special expressive purposes (e.g. search engines). However, any such provisions will need to be drafted with some care. Firstly, there may be a stronger case for subjecting organisations as opposed to private individuals to wider legal responsibilities since the former entities may be expected to have greater capacity to act. In any case, unless it is intended that this provision potentially impact the Regulation across the board, it will be important that the legislation requires the processing to raise specific rather than diffuse freedom of expression concerns. This is because, at an abstract level, any instance of data processing can be formally conceptualized as an exercise of freedom of expression and, therefore, the entirety of data protection may be seen to be in conflict with this. For more on this dilemma see David Erdos, "Freedom the Scylla of Restriction to the Charbydis of Licence? Exploring the Scope of the 'Special Purposes' Freedom of Expression Shield in European Data Protection" (2013) 52 (1) *Common Market Law Review* 119-154 at 145-148.

[252] In the interests of legal certainty, it would clearly be preferable to achieve such a result by providing individual publication with a blanket and categorical exemption from the detailed rules of data protection (noting that a somewhat more nuanced solution will be necessary as regards sensitive data). However, in light of the (rather problematic) discretion which this clause leaves to Member States, it is recognised that some may nevertheless elect to offer individual publication only an exemption from many of these rules (e.g. retrospective transparency) where in the particular circumstances it would not be reasonable to expected adherence to them.

will either not legislate at all or will only provide for excessively restrictive derogations.[253] In these circumstances, the need to interpret this clause as consistently as possible with respect for human rights should be recognised as overriding. Given this, DPAs (and courts) should draw on the general human rights standards present in each of the Member States to achieve a broadly cognate outcome. However, such a result would remain highly imperfect since, as with the current *Lindqvist* dicta, uncertainty about legal requirements would continue. This would result in tension not only with the GDPR's freedom of expression clause itself but also with overarching rule of law requirements set out in both the EU Charter and the European Convention.

6. Conclusions

Not only European data protection law itself but also the DPAs who act as its "guardians"[254] are charged with ensuring the "effective and complete protection of data subjects, in particular of their right to privacy".[255] This task has inevitably come into increasing tension with actors who publish (in the sense of disseminating to an indeterminate number) personal information relating to others. With the dramatic growth from the 2000s onwards firstly of blogs and then of social networking, these actors now include many millions of private individuals. Such individual publication poses an unprecedented interpretative challenge. This article sought to systematically investigate how DPAs in all 31 EEA Member States have responded to this and, from this uniquely comprehensive empirical base, consider how law and regulation may best evolve in the new era of the GDPR.

The article's empirical survey focused on both a questionnaire of EEA DPAs (answered by approximately three quarters of national regulators) and a systematic review of guidance on this issue on their websites (which was found in almost 60% of cases). The data gathered indicated that regulators have generally adopted a strict interpretation of the law here, with almost all holding that that any publication of third party personal information falls outside the law's personal exemption. Moreover, not only do most regulators hold that publication in the general social networking context requires full compliance with default data protection, but approximately half even state that such activity requires data subject consent. Even when individual publication is targeted towards the collective public, many DPAs are reluctant to apply the special expressive purposes derogation unless this activity is clearly akin to that of professional journalism. On the other hand, a number of DPAs do explicitly seek to apply data protection with regard for freedom of expression in context of individual publication, and a few have even adopted the extreme position of seeking to exempt individuals from responsibility in this area entirely. Nevertheless, on the whole, DPA interpretations appear, at least theoretically, to impose unreasonable and disproportionate burdens on individual's free expression rights here and, due to their severe disjuncture with social realities, run the risk of 'having a domestic' with vast swathes of individuals online.

Looking to the future, the GDPR provides an opportunity to develop a more consistent, reasonable and realistic approach, taking into account both competing rights and also the limited capabilities which can reasonably be expected of private individuals. Firstly, building on recital 18, the interpretation of the personal exemption should be expanded to cover instances of individual publication which do not pose a serious *prima facie* risk of infringing the core rights – for example to

[253] As noted in section 2.2 above, even in the area of the special expressive purposes some Member States have failed to set out a derogation in their statutory law.
[254] C-518/07 *Commission v Germany* (2010) at [23].
[255] C-131/12 *Google Spain* (2014) at [38].

privacy and reputation - which data protection is dedicated to upholding. Secondly, in line with Recital 153's recognition of need to interpret the special expressive purposes derogation[256] "broadly",[257] private individuals should not be discriminated against on account of a lack of professional status. Instead, any individual activity which aims to disseminate a message to the collective public, whether of an academic, artistic, journalistic or literary nature, should fall within this permissive but not unqualified derogation. Third, individual publication which is concerned only or at least very predominantly with self-expression and a general freedom to converse should be protected by the Regulation's new freedom of expression clause. This clause should also provide for a balancing of rights whilst also guaranteeing adherence to data protection's core substantive and supervisory provisions. Such a tripartite reconciliation of the law with competing rights and capabilities here would contextually integrate individual publication into the data protection framework. The next task would be to make such integration effective in practice, an undertaking which surely must involve engagement not only with individuals themselves but also with the services which facilitate (and often mould and aggregate) their publication activities. Whilst the scale of the challenge this all presents could hardly be over-estimated, anything less would fail to do justice to Europe's twin commitments to upholding both freedom of expression and the right to the protection of personal data in an ever more complex digital age.

Acknowledgements

I am very grateful for feedback from Jef Ausloos, Frederik Borgesius, Daphne Kellner and Brendan Van Alsenoy, the Data Protection Authorities (DPAs) who participated in the 2013 questionnaire, the large number of research assistants who helped especially with the collection of material for the DPA website review and the British Academy which provided funding for it under their small grant scheme. Full responsibility for all elements of the study rests with me alone including any errors.

Author Information

David Erdos is University Lecturer in Law and the Open Society in the Faculty of Law and WYNG Fellow in Law at Trinity Hall, University of Cambridge.

Appendix: Quantitative Data From EEA DPA Questionnaire and Website Review

N.B. Values in *brackets* signify a quasi-standard response imputed from the DPA's free-text answer. They are not included in Charts One and Two above which are based on the standard responses only.

	DPA Questionnaire Scenarios (A – D scale)		**DPA Website Individual Publication Guidance (1 – 3 scale)**
	Blogger	**Social Networker**	
Austria	*(C)*	D	Uncoded
Belgium	B	D	3
Bulgaria	A	A	-

[256] Regulation 2016/679, art. 85 (2).
[257] *Ibid,* recital 153.

Croatia	-	-	-
Cyprus	D	D	3
Czech Republic	C	D	1
Denmark	-	-	2
Estonia	B	D	3
Finland	B	*(A)*	1
France	C	D	3
Germany - Federal	C	C	-
Germany - Brandenburg	B	B	-
Germany - Mecklenburg	C	D	-
Germany – Rhineland-Pfaltz	*(B)*	C	-
Germany - Schleswig-Holstein	C	D	3
Gibraltar	A	A	-
Greece	C	C	2
Hungary	C	D	-
Iceland	-	-	1
Ireland	C	C	1
Italy	B	C	3
Latvia	C	D	3
Liechtenstein	C	C	-
Lithuania	C	C	Uncoded
Luxembourg	C	D	3
Malta	B	A	3
Netherlands	-	-	2
Norway	-	-	3
Poland	C	*(A)*	-
Portugal	C	D	-
Romania	-	-	-
Slovakia	A	*(A)*	-
Slovenia	*(Midpoint)*	A	1
Spain	-	-	3
Spain - Catalonia	C	C	2
Sweden	*(B)*	*(C)*	2
UK	-	-	1