EUROPEAN UNION DATA PROTECTION LAW AND MEDIA EXPRESSION: FUNDAMENTALLY OFF BALANCE

DAVID ERDOS*

The European Data Protection Directive 95/46/EC requires all European Economic Area (EEA) jurisdictions to provide an equivalent regime protecting the privacy and other fundamental rights and freedoms of natural persons in relation to personal data processing, whilst also shielding media expression from the default substantive requirements as necessary to ensure a balance between fundamental rights. Through a comprehensive coding of the derogations set out in each jurisdiction's data protection laws, this paper provides the first systematic analysis of whether this has in fact been achieved. It is demonstrated that there is a total lack of even minimal harmonization in this area, with many laws providing for patently unbalanced results especially as regards the publication of sensitive information, which includes criminal convictions and political opinion, and the collection of information without notice direct from the data subject. This reality radically undermines European data protection's twin purposes of ensuring the free flow of personal data and protecting fundamental rights, an outcome which remains largely unaddressed by the proposed new Data Protection Regulation. Practical suggestions are proposed to ameliorate these troubling inconsistencies within the current process of reform.

* University Lecturer in Law and the Open Society and Fellow in Law, Trinity Hall, University of Cambridge. I would like to thank Jef Ansloos, Lionel Bently, John Erdos, Aleksandra Kuczerawy, Christopher Kuner, Christopher Millard, Giovanni Sartor and Brendan Van Alsenoy for giving feedback on a previous draft of this working paper, as well as Guy Edwards for his help in checking the quantitative coding presented here. I also acknowledge funding support from the Leverhulme Trust. Any errors remain my own.

The European Union Data Protection regime centred on framework Directive 95/46/EC sets out the standards to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with the respect to the processing of personal data" for all European Economic Area (EEA) Member States.[1] Its default provisions impose very severe restrictions on the right to free speech, including what has traditionally been understood to constitute this right's core, namely, the gathering, storing and imparting of information and ideas by the professional media (herein media expression). However, as regards media expression, Member States are obliged to provide derogations from the substantive provisions but "only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression"[2] or, in other words, only if "necessary for the purpose of balance between fundamental rights".[3] It is separately stipulated that the level of data protection must be equivalent in all Member States.[4] Even a casual examination of the realities, however, shows that these goals have not been achieved. This article sets out the first systematic study of formal statutory law on this issue across the EEA.

As highlighted by the recent Court of Justice of the European (CJEU) decision on the data protection obligations of Google vis-à-vis its indexing of public domain content on the web,[5] European data protection has from its inception had a largely antagonistic relationship with freedom of expression. This is particularly true as regards media expression. On the one hand, the media is not only responsible for "the collection and storage of huge amounts of personal information in the form of interviews, government and company records, as well as photographs and films"[6] but, at least within the private sector, it has been argued that "it is the media … which is capable of inflicting the gravest damage on the individual"[7] as a result of personal information processing. With the growth of ever more powerful processing capabilities, the potential to inflict severe, and sometimes unjustified, damage has only increased. At the same time, however, media entities not only play a key role within a democratic society, but data protection can constitute "a major obstacle to the production and publication of news and current affairs content".[8]

As already noted, these fundamental conflicts were not ignored during the drawing up of the EU Directive itself. However, twenty years on, anecdotal evidence indicates that the equivalent and balanced regime envisaged by this instrument has been far from achieved. Even the European Commission's Evaluation of the Implementation of the Data Protection Directive published in 2012 noted that the Directive's stipulations in this regard are "applied quite differently in the Member States".[9]

---

[1] Directive 95/46, art 1.
[2] Directive 95/46, art 9.
[3] Directive 95/46, recital 37.
[4] Directive, recital 8.
[5] C-131/12 *Google Spain; Google v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, EU:C:2014:317.
[6] P Keller, *European and international media law: liberal democracy, trade and the new media* (Oxford University Press 2011), 331.
[7] Great Britain, House of Lords, Select Committee on the European Communities, *20th Report: Protection of Personal Data* (HMSO 1993), 39.
[8] Keller (n 6) p. 337.
[9] See Annex 2 of European Commission Staff Working Paper Impact Assessment (SEC (2012) 72 FINAL) 13. These remarks were grounded in analysis produced in 2010 which, whilst interesting, was entirely qualitative, somewhat anecdotal and based only on an explicit examination of the laws in those States which joined the EU

This article provides the first comprehensive analysis of this pressing issue. It is based on an original data set which has collated, logically ordered and numerically coded outcomes found within the data protection law of each European Economic Area (EEA) jurisdiction. Following an introductory section which outlines the pan-European structure of data protection including vis-à-vis media expression, this methodology is outlined in section two. Section three then explores the comparative structure of media derogations within all EEA states, noting that whilst some have adopted discrete approaches to each substantive data protection provision, many others have adopted an identically worded derogation applicable to all or some of data protection's default substance. The particular derogations adopted within these latter cases are elucidated. Sections four to seven then provides a detailed analysis of the media derogations applicable to each of the core substantive elements of the European data protection regime. These results are integrated in section eight. Finally, section nine sets out the article's conclusions, together with some preliminary thoughts on the future shape of this legal framework.

It is found that, notwithstanding the binding nature of the requirements in both the Directive and human rights instruments such as the *EU Charter*, many Member States have failed to provide for an effective balance within their statutory law. Instead, countries in Northern European have tended to prioritize media freedom within their legal frameworks, whilst those in Eastern European and Latin counties have done likewise for data protection. Given that the Directive is predicated on ensuring data protection equivalency as a *quid pro quo* for also requiring that the free flow of personal data between Member States neither be prohibited nor restricted,[10] this reality poses a clear threat to the internal integrity of the pan-EU framework. Even more critically, it also undermines the effective and certain legal protection of fundamental human rights in Europe. Unfortunately, despite the push from 2012 onwards to replace the Directive with a new General Data Protection Regulation, there is little evidence that the proposals made to date will directly address the serious problems elucidated here. However, unless they do so, European data protection will likely remain fundamentally off balance.

I. THE DATA PROTECTION DIRECTIVE AND MEDIA EXPRESSION

A. The Default EU Data Protection Scheme

The EU Data Protection Directive 95/46/EC binds the 28 full members of the EU along with three associated countries (Iceland, Liechtenstein and Norway)[11] which taken together make up the EEA. It has a "breathtaking"[12] scope. As regards the private sector data "controllers", it applies to

---

before 2003. See D Korff, *Data Protection Laws in the EU: The Difficulties in Meeting the Challenges posed by Global Social and Technical Developments* (2010), 13-21 <http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_2_en.pdf>.

[10] Directive 95/46, art 1.2; recital 8.

[11] The application of the Directive here is based on the Agreement on the European Economic Area (OJ 1994 L 1). The precise relationship between the legal duties of these jurisdictions and both related legal provisions such as the EU Charter of Fundamental Rights and interpretations of the law by the Court of Justice of the European Union remains a matter of great complexity, the consideration of which is beyond the scope of this article.

[12] D. Bainbridge, *EC Data Protection Directive* (Butterworths 1996), 15.

any "processing" of "personal data" carried out either "wholly or partly by automatic means"[13] or as part of a cognate manual filing system "structured according to specific criteria relating to individuals so as to permit easy access to the personal data in question".[14] Notwithstanding its technical and abstruse nomenclature, "personal data" actually encompasses "any information relating to an identified or identifiable natural person ('data subject')".[15] Thus, "data" and "information" are treated synonymously and their conceptualization is wide enough to cover even innocuous details about an individual, such as a person's job title, irrespective of whether this is already in the public domain.[16] "Processing" encompasses "any operation or set of operations which is performed upon personal data … such as collection, recording, organisation, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction".[17] Finally, "controller" is defined as the natural or legal person which "alone or jointly with others determines the purposes and means of the processing of personal data".[18]

Controllers are generally obliged to ensure that any particular instance of data processing complies with the four core substantive elements of the EU Data Protection system which together include some eighteen different data protection provisions. In sum, these are structured as follows:

- *The Data Quality Principles (Provisions (i)-(v)):* Five broadly applicable and generally open-textured provisions setting out the default standards for good information handling including fairness, non-excessiveness and accuracy.
- *Transparency Rules (Provisions (vi)-(viii):* Three rules setting out requirements for ensuring transparency of processing for the data subject, namely, (vi) requirements to proactively provide information to the data subject when data is being collected directly from him (proactive direct transparency rule), (vii) similar duties in certain circumstances to proactively provide information to data subject even when data is being collected indirectly via a third party or the public domain (proactive indirect transparency rule) and (viii) requirements to provide much more extensive information to the data subject on request (retroactive transparency rule).
- *Sensitive Data Rules (Provisions (ix)-(xv)):* Special rules for ensuring that that data deemed sensitive generally cannot be processed by the private sector unless such a prohibition is waived in some way by the data subject. Rules apply to seven broad categories of data revealing, concerning or relating to information as to (ix) racial or ethnic origin, (x) political opinions, (xi) religious or philosophical beliefs, (xii) trade union membership, (xiii) health, (xiv) sex life and (xv) offences, criminal convictions and security measures.
- *Control Conditions (Provisions (xvi)-(xviii)):* Three conditions which impose additional substantive restrictions on the processing of data for a controller's own purposes but primarily have the function of ensuring that the other elements of the scheme are not undermined. These provisions stipulate (xvi) the need for a pre-specified legitimating ground

[13] Directive 95/46, art 3.
[14] Directive 95/46, recital 15.
[15] Directive 95/46, art 2 (a).
[16] C-101/01 *Criminal proceedings against Bodil Lindqvist,* EU:C:2003:596; C-73/07 *Tietosuojavaltuutettu v Satakunnon Markkinapörssi Oy and Satamedia Oy,* EU:C:2008:727.
[17] Directive 95/46, art 2 (b).
[18] Directive 95/46, art 2 (d).

for processing, (xvii) the requirements to provide a notification of data processing and (xviii) the need to restrict the export of data to countries lacking an adequate level of protection for such data.[19]

Member States retain a certain "margin for manoeuvre" regarding how the Directive, including these default elements, are to be transposed.[20] The particular law or laws which a controller must follow will generally depend upon which EEA country or countries he is established in and in the context of which establishment or establishments processing takes place.[21]

B. EU Data Protection and Media Expression

Although its boundaries are contestable, there is a consensus that the concept of media expression refers at least to the publication of journalistic material by the professional press together with those audiovisual entities which disseminate news periodically. All the four core substantive elements of EU Data Protection have the potential to exert a significant impact on such expression. Thus, although the data quality principles often enunciate standards which are "in the best traditions of good responsible journalism",[22] they nevertheless have a particularly wide scope and give the full force of law to provisions which have traditionally been seen as a matter of self-regulation only. If the proactive direct transparency rule is applied then, when collecting personal data from the data subject, "no undercover investigation by journalists will lawfully be possible"[23] even in relation to a story of great public importance and even when the data will be anonymised before publication. Meanwhile, the proactive indirect transparency rule would impose a duty of data subject notification when information is collected from third parties more onerous than that rejected as being required under the European Convention on Human Rights,[24] whilst that relating to retroactive transparency would require an even greater openness vis-à-vis media activity, thereby threatening both media autonomy and journalistic source confidentiality.[25] As regards the broad categories of data they regulate, the sensitive data rules would generally prohibit publication if the data subject objects. Given that processing of specially protected categories of information such as criminal conviction and political opinion lie at the heart of much media output, application of these

[19] It might be thought that the data security provisions in articles 16 and 17 of Directive 95/46 should also be included in this category. However, as the European Commission's Amended Proposal for a Council Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data Explanatory Memorandum (COM (92) 422 final) emphasised (at 37), these provisions were designed to be procedural as opposed to substantive since they are aimed only at ensuring that information is not subject to unauthorized processing, especially by third parties. This procedural understanding was confirmed by the CJEU in *Satamedia* (2008) at [64].

[20] Directive 95/46, recital 9.

[21] Directive 95/46, art 4. If the controller is not established in any EEA state but makes use of equipment on the territory of one or more Member State, then he must comply with national laws in each country or countries.

[22] Council of Europe, *Legislation and Data Protection: Proceedings of the Rome Conference on problems relating to the development and application of legislation on data protection* (Camera dei Deputati 1983), 72.

[23] S Rasaiah & D Newell, 'Data Protection and Press Freedom' (1997/98) 3 *Yearbook of Media and Entertainment Law* 232.

[24] *Mosley v United Kingdom* (48009/08) [2012] EMLR 1.

[25] Rasaiah & Newell (n 23), 234-236.

provisions would "radically restrict the freedom of the press".[26] Finally, whilst not so directly burdensome, the control provisions would nevertheless tie the media to formalized rules on data processing which, whilst perhaps common within other industries, would generally be seen as alien and intrusive by many within the journalistic sector.

In recognition of the need to establish an appropriate equilibrium between data protection and other fundamental values, the Directive did allow EEA Member States to provide certain derogations from these default positions. As previously stated, in relation to media expression, article 9 of the Directive states that Member States must provide derogations from any part of the substantive provisions of the Directive but "only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression".[27] Recital 37 of the Directive further stressed that the derogations adopted should be those "necessary for the purpose of balance between fundamental rights", whilst recital 8 more generally set out the overarching requirement that the level of data protection "must be equivalent in all Member States". In *Satamedia* (2008), the Court of Justice of the European Union addressed the interaction between journalistic expression and the data protection regime finding that "in order to achieve a balance between the two fundamental rights, the protection of the fundamental right to privacy requires that the derogations and limitations in relation to the protection of data … must apply only is so far as is strictly necessary".[28] The binding nature of this requirement to reconcile conflict fundamental rights has been strengthened by the inclusion of rights to privacy and data protection together with a right to freedom of expression[29] within the *EU Charter of Fundamental Rights*. According to Article 52 of this instrument, any limitations on rights must respect its "essence", comply with the principle of proportionality, be necessary and "genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others". Although neither the *European Convention on Human Rights* nor many national constitutions explicitly include a right to data protection itself,[30] it is clear these instruments do recognise both a right to freedom of expression and a right to privacy, similarly mandating that any legislative restriction on these rights be justified according to the same kind of proportionality principles.[31] In light of the binding nature of these requirements, it is important to explore to what extent national transposing laws do effectively balance or reconcile these conflicting rights.

[26] Lord Phillips of Worth Matravers in *Campbell v Mirror Group Newspapers* [2002] EWCA Civ 1373, [2003] QB 633 at [123].
[27] Directive 95/46, art 9
[28] *Satamedia*, above note 16 at [56].
[29] Charter of Fundamental Rights of the European Union (OJ 2010 C 83, p. 389), arts 7, 8 and 11.
[30] Although the European Convention on Human Rights excludes mention of this, some thirteen EU member states do include a right to data protection in their Constitution. See J Cannataci and J Misfud-Bonnici, 'Data Protection Comes of Age: The Data Protection Clauses in the European Constitutional Treaty' (2005) 14 *Information and Communications Technology Law* 8.
[31] See, as regards the European Convention on Human Rights, art 8 (Right to respect for private and family life) and art 10 (freedom of expression).

II. METHODOLOGICAL APPROACH

A. Overview

This article seeks to systematically explore the different extents to which the national transposition of the Data Protection Directive in each Member State jurisdiction makes allowance for media expression both as a whole and also as regards particular aspects of the law. Such a task is best approached through a formal quantitative coding of the law. Although such a methodology would have been considered highly unusual only a decade ago, there is now a growing consensus that such "numerical comparative law can contribute to many core topics of comparative law"[32] including the study of regulation[33] and comparative human rights.[34] The specific standardized coding the article maps the strength in each jurisdiction of any and all derogations applicable to the media vis-à-vis the EU data protection scheme. The structure of Article 9 of the Directive itself aids this goal since, at the level of each individual data protection provision, it clearly provides for two outlying positions. On the one hand, a Member State may choose to provide no derogation at all from the provision, such that it remains 100 percent applicable. On the other, an absolute derogation may be provided whereby that the data protection provision in question is completely eliminated. In between these extremes, a wide variety of intermediary positions are also possible.

An inductive examination was made of any and all derogations applicable to media expression set out in the Data Protection Acts currently in force within all EEA Member State jurisdictions or, in other words, all 31 EEA Member States together with the special case of Gibraltar, a separate jurisdiction within the EU but one for which the UK Government remains responsible.[35] In most cases, reliance was placed on the English language versions of the legislation made available by the Data Protection Authority or other official government agency. However, in any case where the translation appeared to be potentially inaccurate or it was clear that relevant materials were unavailable in this format, a check was made with the original language version of the law. Based on this inductive analysis, the observed derogation outcomes were grouped at the individual data protection provision level into seven categories labelled (a) to (g) which were standardized so as to be identically defined not only between the different jurisdictions but also between the different provisions themselves. These derogation categories were ordered from high to low according to whether, and if so to what extent, data protection was still applicable in the media sphere. Given that the extreme categories here unequivocally represented respectively complete (1) substantive applicability of ordinary data protection provisions to the media and no (0) applicability, these categories were converted onto a notional 0, 1 scale such that (a) = 1, (b) = 0.83, (c) = 0.67, (d) = 0.5, (e) = 0.33, (f) = 0.17, (g) = 0. This assignment allowed for Member States to be allocated a score in relation to each individual data protection provision. Relevant scores were then combined in order to provide an overall measure of the continued relevance of each of the four substantive elements of EU data protection outlined above. Finally, these element level scores were combined to provide an overall representation of data protection in the media sphere. Whilst neither the overall nor

[32] M Siems, *Comparative Law* (Cambridge University Press 2014), 186.
[33] See, for example, Siems, Mathias, 'Regulatory Competition in Partnership Law' (2009) 58 *International and Comparative Law Quarterly*.
[34] See, for example, T Ginsburg, D Lansberg-Rodriguez and N Versteeg, 'When to Overthrow your Government: The Right to Resist in the World's Constitutions' (2013) 60 *UCLA Law Review*.
[35] See art 355 (3) of the Treaty on the Functioning of the European Union.

necessarily even the element level results map precisely to the seven standardized categories defined at individual provision level, the use of a standardized scale still enables these scores to represent the extent to which substantive data protection remains applicable vis-à-vis media expression both as regards the regime as a whole and as regards particular elements of it. Thus, an advantage of the micro-foundational approach adopted is that it allows for comparison of data protection outcomes at every level from the most general, right down to that of individual provisions.[36]

B. Ordered Categories and the Standardized Scale

The seven categories, ordered from complete to no applicability of data protection and with values ranging from 1 to 0, are listed and defined in Table One below.

Table One: Ordered Categories Measuring the Extent of Continued Applicability of European Data Protection vis-à-vis Media Expression

Category & Scale Point	Summary	Precise Definition (with Examples in Italics)
(a) / 1	No derogation	No derogation provided at all from the default general minimum set out in the Directive.
(b) / 0.83	Minimal derogation	Either (i) no media exemption set out but only a special interpretative provision which provided a gloss but did not supplant the particular data protection provision in question or (ii) an exemption is provided but this is limited to a narrow aspect of the provision in question. *Examples: As regards (i), Italian law does not exempt the media from compliance with the data quality principles but certain legal provisions including a specially drafted Code of Practice do set out special interpretative provisions in the media's favour.[37] As regards (ii), Romanian law requires the media to comply with the general rules as regards ensuring retroactive transparency of data processing on request from the data subject except in so far as the confidentiality of journalistic sources would be affected.[38]*
(c) / 0.67	Rule Restricted Exemption	A wide-ranging media exemption is provided from the particular provision in question so long as the processing falls within specific pre-defined circumstances and/or complies with specific pre-determined rules. *Example: Luxembourg law provides a media exemption from the general requirement to retroactively disclose information to the data subject but only if media entity allow for access instead through "the intermediary of the Commissioner Nationale pour la Protection des Donneess in the presence of the Conseil de Presse or his representative, or the Chairman of the Conseil de Presse duly called upon".[39]*

[36] A study is in progress examining how data protection legislation has actually been applied via-à-vis the media in each EEA jurisdiction. The standardized approach adopted here should aid systematic comparison between these two datasets.

[37] Italy, Personal Data Protection Code, sec 163.3; Italy, Code of Practice Concerning the Processing of Personal Data in the Exercise of Journalistic Activities.

[38] 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 (as amended), art 13.6.

[39] Luxembourg, Coordinated Text of the Law of 2 August 2002 on the Protection of Persons with regard to the Processing of Personal Data (as modified), sec 29 (3).

(d) / 0.5	Strict Public Interest Exemption	An overarching media exemption is provided but this is subject to compliance with a test which, whilst open-textured, is based on a strictly objective analysis of where the public interest lies. *Example: Bulgarian law provides the media with an exemption from certain data protection provisions but only "to the extent to which it does not violate the right to privacy of the person to whom such data relate".*[40]
(e) / 0.33	Permissive Public Interest Exemption	An overarching media exemption is provided but this requires compliance with an open-textured public interest test which, whilst imposing significant duties on the media, is phrased so as to be more permissive than a strictly objective test would be. *Example: United Kingdom law exempts media entities from compliance with a range substantive data protection provisions so long as the media entity "reasonably believes that, having regard in particular to the special importance of the public interest in freedom of expression, publication would be in the public interest" and that it also "reasonably believes that, in all the circumstances, compliance is incompatible" with this purpose.*[41]
(f) / 0.17	Minimal Inclusion	Either (i) data protection law excludes much of media data processing unconditionally from the provision in question but subjects some other types of media expression data processing to it only to a limited extent or (ii) an overarching exemption is provided for the media subject only to compliance with a test of minimal substantive content. *Examples: As regards (i), Dutch law provides the media with a complete exemption from all of the sensitive data rules element, subject only to the requirement that the processing is "necessary" for journalistic purposes.*[42] *As regards (ii), in Germany the media is generally entirely exempted from the fourth data quality principle which requires that data be accurate and, where necessary, up-to-date (provision iv).*[43] *Nevertheless, under the federal Data Protection Act, if reporting by Deutsche Welle (the German equivalent of the BBC World Service) "infringes the privacy of an individual",*[44] *a person may make a request to that any "inaccurate data be corrected". Similarly, the German Interstate Treaty on Broadcasting and Telemedia establishes that, as regards other broadcasters, if a person is "negatively affected in his interests meriting protection" by inaccurate journalistic processing, he may demand either its "correction" or the addition of his "own statement of appropriate length".*[45]
(g) /0	Complete Exclusion	An absolute and unconditional media expression derogation is provided from the particular data protection provision in question.

III. COMPARATIVE STRUCTURE OF THE MEDIA DEROGATIONS

A. Specific or Generally Applicable Derogations

The law of a number of jurisdictions sets out a multiplicity of specific derogations in favour of the media based on divergent tests which are then made applicable to different aspects of the data protection regime. In these cases, it is appropriate to analyse the nature of these tests during discussion of relevant data protection provision in question. In a significant number of other jurisdictions, however, an identically worded clause is made applicable to all, or at least most, of the substantive data protection provisions from which a derogation is provided. In these cases, it makes sense to analyse the clause at the outset and then cross-refer to this during the subsequent specific

[40] Bulgaria, Law for the Protection of Personal Data, art 5 (7).
[41] United Kingdom, Data Protection Act 1998, sec 32 (1) (emphasis added).
[42] Netherlands, Personal Data Protection Act, art 3 (1).
[43] Directive 95/46, art. 6(1)(d).
[44] Germany, Federal Data Protection Act (BDSG), sec 41 (3). For completeness it should be noted that it is also stated that if *Deutsche Welle*'s journalistic processing "leads to the publication of counter-statements by the data subject, these counter-statements shall be added to the recorded data and retained for the same length of time as the data themselves" (sec 41 (2)).
[45] Germany, Interstate Treaty on Broadcasting and Telemedia 2010, art 47 (2).

discussion. These cross-references will be designated by the placing of an asterisk (*) next to the name of the country concerned. The generally applicable derogations are principally outlined immediately below. However, in two jurisdictions (Estonia and Malta), the wording of this clause renders unclear which data protection provisions it seeks to modify or even eliminate. These cases will, therefore, be separately addressed in sub-section B below.

Three jurisdictions (*Finland,[46] *Norway[47] and *Sweden[48]) exempt the media completely and unconditionally from all the substantive data protection provisions. Austrian and the Icelandic law generally provides likewise, except in relation to all (*Austria[49]) or some (*Iceland[50]) of the data quality principles. *Lithuanian law also sets out an absolute and unconditional exemption but restricts this its ambit to the transparency rules (provisions (vi)-(viii)), the notification of processing rule (provision xvii) and data export condition (provision (xviii)).[51] All these countries are coded into category g/0 in relation to the provisions controlled by these clauses.

The laws of a large number of jurisdictions (*Gibraltar, *France, *Ireland, *Latvia, *Poland and the *United Kingdom) set out a broadly applicable permissive derogation based on the public interest which, therefore, falls within category e/0.33 of our ordered scale. French law sets out professional journalistic derogation from provision (iv) of the data principles element, the transparency rules element (provisions (vi)-(viii)), the sensitive data element (provisions (ix)-(xv)) and the data export condition (provision (xviii)) so long as processing is "according to the ethical rules of this profession".[52] Polish law exempts the media from compliance with all the substantive data provisions except where "the freedom of information and dissemination considerably violates the rights and freedoms of the data subject".[53] Gibraltan, Irish and UK law set out a derogation which is available so long as

> (a) the processing is undertaken [solely] with a view to the publication of any journalistic, literary or artistic material, (b) the data controller reasonably believes that, having regard in particular to the special importance of the public interest in freedom of expression, [such] publication would be in the public interest, and (c) the data controller reasonably believes that, in all the circumstances compliance with that provision would be incompatible with *inter alia* journalistic purposes.[54]

This derogation is applied in all cases to the data quality principles (provisions (i)-(v)), transparency rules (provisions (vi)-(viii)) and sensitive personal data rules (provisions (ix)-(xv)), the legitimating ground condition (provision (xvi)) and, in the Gibraltan and UK case only, also the data export condition (provisions (xviii)). Gibraltan law also applies this derogation to the requirement to provide a notification of data processing (provision (xvii)), whilst Irish law exempts the media

[46] Finland, Personal Data Act, sec 2 (5).
[47] Norway, Personal Data Act, sec 7.
[48] Sweden, Personal Data Act, sec 7.
[49] Austria, Federal Act Concerning the Protection of Personal Data (DSG), sec 48.
[50] Iceland, Act on the Protection of Privacy as regards the Processing of Personal Data, art 5.
[51] Lithuania, Law on the Legal Protection of Personal Data, art 8.
[52] France, Law on Information Technology, Data Files and Civil Liberties, art 67.
[53] Poland, Act on the Protection of Personal Data 1997 (as amended), art 3.a.2.
[54] Gibraltar, Data Protection Act 2004, s. 13; Ireland Data Protection Act, sec 22A; UK, Data Protection Act 1998, sec 32. The parts added in square brackets reflect additions inserted into the Gibraltan and Irish legislation only.

unconditionally from this requirement. Latvia sets out a full media exemption from proactive transparency rules (provisions (vi) and (vii)), all but the last provision in the sensitive personal data element (provisions (ix)-(xiv)) and the legitimating ground requirement (provision xvi) but states that in applying this "the rights of persons to the inviolability of private life and freedom of expression shall be observed".[55] A different exemption is provided from the requirement to provide a notification of data processing (provision xvii) which will be analysed separately below.

One country, *Bulgaria, sets out a broadly applicable derogation which because of its incorporation of a clearly objective, public interest test is placed within category d/0.5. More specifically, the law here provides a media data processing exemption from the proactive aspects of the transparency rules (provisions (vi)-(viii)), the sensitive data rules (provisions (ix)-(xv)) and the control conditions (provisions (xvi)-(xviii)) "to the extent to which such processing does not violate the right to privacy of the person to whom the data relate".[56]

The laws of three countries (*Croatia, *Czech Republic and *Spain) provide no media derogation at all from any part of the data protection scheme. All these countries are therefore placed in category a/1 in relation to each data protection provision. *Hungary is coded similarly on all the data protection provisions except the proactive transparency rule when collecting information directly from the data subject (provision (vi)) where a derogation is provided as outlined below.

B. Malta and Estonia: Derogations of Unclear Scope and Meaning

In almost all cases, it is easy determine which data protection provisions any media derogation applies to. Indeed, in the vast majority of cases, this is made explicit. However, in two cases (*Estonia and *Malta), this is far from the case. Section 11 (2) of the Estonian Personal Data Protection Act provides that:

> Personal data may be processed and disclosed in the media for journalistic purposes without the consent of the data subject, if there is predominant public interest therefore and this is in accordance with the principles of journalism ethics. Disclosure of information shall not cause excessive damage to the rights of the data subject.

To the extent that this provides for a qualified exemption from data protection provisions, it is reasonably clear that this clause imposes a strict public interest test based on judicial consideration of the "predominant" interest and therefore should be placed in category d/0.5. However, save from providing that consent is not required in these cases, the clause does not explicitly set out from which data protection provisions a qualified exemption may be provided. Matters are made even more complex by the fact that Estonia has transposed the requirements of the Directive in a highly idiosyncratic way. A close analysis of the Estonian data protection regime indicates the way it has

[55] Latvia, Data Protection Act, art 5. This article further states that those processing for journalistic purposes must act in accordance with the Law on Press and Other Mass Media. However, analysis of this non-data protection specific media regulation is outside the scope of this article.
[56] Bulgaria, Law for the Protection of Personal Data, art 4 (2); art 5 (7); art 36a(7).

implemented the sensitive personal data rules (provisions (ix)-(xv))[57] and the proactive transparency rule when collecting information directly the data subject (provision (vi))[58] depends on a presumption that consent will be obtained in these cases. A similar presumption applies in Estonian law in relation to the need for a legitimating ground for processing (provision (xvi)).[59] Meanwhile, whilst no similar presumption applies in relation other transparency rules (provisions (vii)-(viii)), in these cases the Act does allow for a restriction where otherwise this may "damage rights and freedoms of other persons".[60] This also establishes a similar strict, public interest test to that detailed above. Therefore, in relation to all of these provisions, Estonian law is coded into category c/0.5. In contrast, as will be seen, compliance with the default data quality principles (provisions (i)-(v)), the data export condition (provision (xviii)) and the notification of processing condition (provision (xvii)) does not intrinsically depend on obtaining the consent of the data subject and nor is any other derogation set out. Therefore, in these cases Estonian law is coded into category a/1.

The nature of the media derogation within the Maltese Data Protection Act presents even more challenging interpretative difficulties. Sections 6 (1)-(3) of this Act states that:

> (1) Subject to the following provisions of this article, nothing in this Act shall prejudice the application of the European Convention Act relating to freedom of expression, or the provisions of the Press Act relating to journalistic freedoms.
> (2) Notwithstanding the provisions of subarticle (1) the [Data Protection] Commissioner shall encourage the drawing up of a suitable code of conduct to be applicable to journalists and to the media to regulate the processing of any personal data and the code of conduct shall provide appropriate measure and procedures to protect the data subject, having regard to the nature of the data.
> (3) In the absence of such a code of conduct, the Commissioner may establish specific measures and procedures to protect the data subjects; in such a case journalists and the media are to comply with measures and procedures so established.

The language in s. 6(1) stating that, apart from s. 6 itself, the data protection scheme shall not "prejudice" either the Press Act or the European Convention Act is clearly strong since, following the definition of this provided in the Oxford English Dictionary, it could imply that the provisions should not even "bias" the application of these provisions. Whilst most of the provisions of the Maltese Press Act do not directly conflict with data protection legislation,[61] the First Schedule of the European Convention Act does repeat verbatim the wording of Article 10 (1) in the European Convention which establishes a broad right to freedom of expression, including the imparting and receipt of information without interference by public authority, which is in clear tension with data protection requirements. On the other hand, Article 10 (2)'s specific validation of permissible interferences with this right in order to safeguard the rights of others (which in principle could include their data protection rights), further complicates the picture. Moreover, the rest of s. 6

[57] Estonia, Personal Data Protection Act, sec 12 (4).
[58] Estonia, Personal Data Protection Act, sec 12 (3).
[59] Estonia, Personal Data Protection Act, sec 14 (1).
[60] Estonia, Personal Data Protection Act, sec 20 (1) (1); sec 15 (2) (5).
[61] Sec 46 of the Maltese Press Act does place certain limits on the disclosure of journalistic sources as a result of legal processes. This could be seen to be in direct tension with the requirement to disclose information to data subjects on request. This is an aspect of the transparency provisions dealt within the next section.

demonstrates a clear intention not to exclude media activity absolutely and unconditionally from the data protection regime. To date, however, no code of conduct nor formal measures and procedures have yet been drawn up, although the Data Protection Commissioner has produced general guidance on street photography[62] and more generally acknowledged that in the absence of a code he does have an obligation to specific measures and procedures.[63] Overall, it seems that the purpose of the scheme set out in section 6 was to establish a general expectation that ordinary data protection provisions would not be applicable to media expression so long as certain minimum standards were complied with. Given this, it is most appropriate to place Maltese law within category e/0.33 in relation to all the substantive data protection provisions.

IV. MEDIA EXPRESSION AND THE DATA QUALITY PRINCIPLES (PROVISIONS (i)-(v))

The five data quality principles are set out in article 6 of the Directive and provide that personal data must be:

i. processed fairly and lawfully,
ii. collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes,
iii. adequate, relevant and not excessive,
iv. accurate and, where necessary, kept up to date,
v. kept in a form that permits identification of data subjects for no longer than is necessary.

With three exceptions discussed below, Member State law has adopted an identical approach as regards the availability of media derogations in relation to all of the above principles. The law of some eighteen jurisdictions (Belgium, *Bulgaria, *Croatia, Cyprus, *Czech Republic, *Estonia, Greece, Hungary, *Latvia, Liechtenstein, Lithuania, Luxembourg, Netherlands, Portugal, Romania, *Slovakia, Slovenia and *Spain) apply the principles without restriction to the media and, therefore fall within category a/1. Italian law falls within category b/0.83 since it applies the principles to the media but set out a special interpretative provisions in its favour. Thus, section 136.3 of the Personal Data Protection Code provides when data are communicated or disseminated in the exercise and for the sole purpose of the journalistic profession

> the limitations imposed on freedom of the press to protect the rights [instantiated in the data protection regime] … in particular, concerning the materiality of the information with regard to facts of public interest, shall be left unprejudiced. It shall be allowed to process the data concerning circumstances or events that have been made known either directly by the data subject or on account of the latter's public conduct.

On the other hand, the media are not exempted from the data quality principles and are additionally subject to a legally binding Code of Practice Concerning the Processing of Personal Data in the

[62] Malta, Data Protection Commissioner, *Data Protection and Street Photography* [2013] <http://idpc.gov.mt/dbfile.aspx/Data_Prot_and_Street_Photography.pdf>.
[63] Malta, Data Protection Commissioner, *Annual Report* 2005, 6 <http://idpc.gov.mt/dbfile.aspx/Annual%20Report%202005.pdf>.

Exercise of Journalistic Activities (Data Protection Journalism Code)[64] which reiterates in a modified form many of the data quality principles.[65] No EEA state has adopted a derogation here in the form of either category c/0.67 or category d/0.5. The law of six jurisdictions (Austria, *Gibraltar, *Ireland, *Poland, *Malta and the *UK) set out a more permissive public interest derogation here which, therefore, falls within category e/0.33. In Austria, whilst media expression is presumptively subject to compliance with the data quality principles[66] the Act also then states that media use of data for journalistic purposes "shall be legal insofar as this is required to fulfil the information requirements of the media companies, media services and their operatives in the exercise of their right to free speech pursuant to art. 10 para. 1 of the European Convention on Human Rights".[67] Especially given the lack of direct mention of permissible interferences with freedom of expression under article 10 (2) of the Convention, this wording effectively grants the media considerable leeway before the law imposes substantive data protection requirements on them through recourse to the data quality principles. In excluding much media processing unconditionally from the data protection principles but subjecting other types of processing to certain limited elements, one jurisdiction (Denmark) falls within category f/0.17. Here, general data protection law grants journalistic expression an absolute exemption from all the substantive data protection provisions it sets out.[68] However, a sector-specific piece of data protection legislation, the Law on Mass Media Information Databases establishes that publicly available mass media electronic information databases "may not hold information that cannot be legally published in the mass media",[69] that they must delete, correct or update information which is "false or misleading"[70] and that they also "may not hold information whose disclosure would be contrary to the ethics of journalism".[71] The first requirement instantiates the lawfulness aspect of provision (i) whilst the second aspect includes elements of provision (iii). Meanwhile, the last invocation of journalistic ethics overlaps at least to an extent with most of the data quality principles, albeit with a heavy emphasis on media self-regulation.[72] However, rather undercutting these protections, databases used internally by the mass media are excluded these requirements.[73] Meanwhile, whilst publicly available information databases are

[64] This Code was issued by the Italian Data Protection Authority in 1998 following discussion with the media. Its legally binding status is governing by sec 139 and sec 12 of the Italian Personal Data Protection Code.
[65] The Code's provisions reiterating the need to rectify inaccurate data (art. 4) and that journalists may keep data as long as is necessary for the relevant professional purposes (art. 2.4) clearly map on to principles three and five. Other key provisions include those relating the collection of data, protection of human dignity and non-discrimination (all relevant to principle one) and the need to actively assess the materiality or otherwise of information (relevant to principle one and three).
[66] Austria, Federal Act Concerning the Protection of Personal Data (DSG), s. 48 (1).
[67] Ibid, s. 48 (2).
[68] Danish, Act on the Processing of Personal Data 2000 (as amended), s. 2.
[69] Denmark, Lov om massemediers informationsdatabaser 1994, sec 3 (8) (translated from Danish).
[70] Ibid, sec 3 (9) (this section also states that such a requirement applies when a previously mentioned judgment has been modified, the prosecution in a previously mentioned case has been abandoned or when a prosecution results in acquittal. These additions appear to be further specifications of when continued information dissemination would be "misleading" (*vildledende*).
[71] Ibid, sec 3 (8) (translation from Danish).
[72] See Danish Press Council, Sound Press Ethics (n.d.) (http://www.pressenaevnet.dk/Information-in-English/The-Press-Ethical-Rules.aspx) (accessed 25/11/14).
[73] The only relevant stipulations placed on such databases is that if they are electronic in nature then they can only be "made available to anyone other than mass media journalists and editorial staff" who further "should not access or use the information database for anything other than journalistic or editorial work" (sec 2 (4)). These provisions can be seen as a very partial instantiation of the second data quality principle.

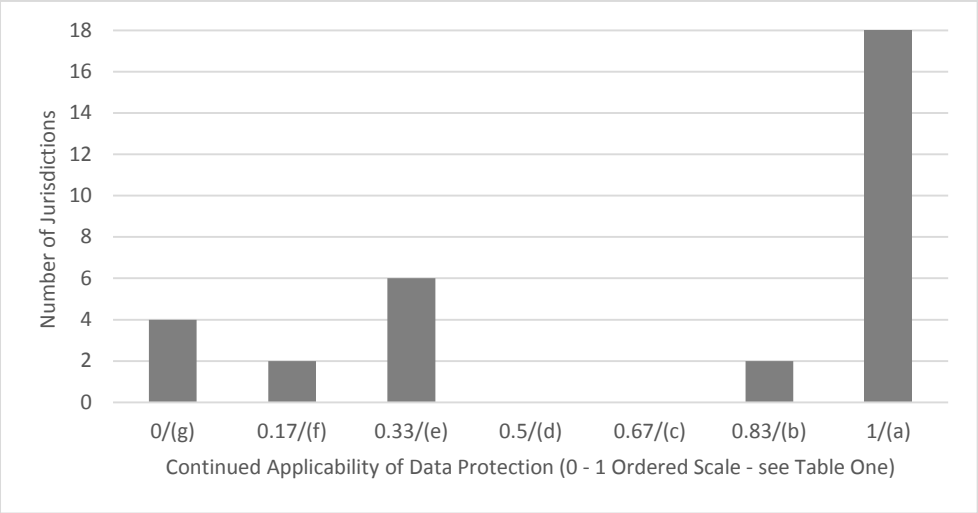
defined as databases made publicly available by the mass media "which make use of electronic data processing in connection with the dissemination of news and other information",[74] the Act also fully excludes databases which only include already published text, images, periodicals, audio or video programs so long as the information database has been unchanged in relation to the original publication. These fall instead within the Danish Media Liability Act.[75] The law of three countries (*Finland, *Norway and *Sweden) exclude the media entirely from the principles and, therefore, fall within category g/0.

Turning to the three exceptional cases, *French law provides no derogation at all in relation to the principles (i)-(iv) and, therefore, falls within category a/1 here. In relation to principle (v), however, a coding of e/0.33 is recorded since an exemption is available so long as processing is "according to the ethical rules of this [the journalistic] profession".[76] Meanwhile, the clause in the Icelandic Act relating to the media provides it with a full exemption from principles (ii), (iii) and (v), thereby placing it within category g/0 here. This clause additionally states that principles (i) and (iv) "shall apply" [77] whilst also stating that "[t]o the extent necessary to reconcile the right to privacy on the one hand and freedom of expression on the other, derogations can be made from provisions in the Act in the interest of journalism, art or literature".[78] Taken together, this wording appears to establish a strict or fully objective public interest balancing test as regards these two provisions; a coding of d/0.5 is, therefore, recorded. Finally, German law generally exempts the media from compliance with all the substantive data protection provisions.[79] However, some entities, namely *Deutche Welle* (the German equivalent of the BBC World Service) and other broadcasters regulated under the Interstate Treaty on Broadcasting and Telemedia, are subject to a very partial extent to certain aspects of data protection including a qualified version of principle (iv). Under the German federal Data Protection Act, if reporting by *Deutsche Welle* "infringes the privacy of an individual" this person "may request that inaccurate data be corrected".[80] Meanwhile, as regards other broadcasters, when in relation to inaccurate journalistic processing a person is "negatively affected in his interests meriting protection", he may demand either its "correction" or the addition of his "own statement of appropriate length".[81] Given this, German law is coded as f/0.17 in relation to principle (iv) and g/0 in relation to the other principles. The final scores for these three countries on the data quality principles element are 0.87 for France, 0.14 for Iceland and 0.03 for Germany. However, especially since these scores are so similar to categories (b), (f) and (g) respectively, it is

[74] Ibid, sec 1 (2) (translated from Danish).
[75] Ibid, sec 1 (1). It should be noted that, whilst not mandating the various other stipulations mentioned above, this Media Liability Act 1998 does repeat the same language that such content must be conformity with sound journalistic ethics. See Denmark, Media Liability Act 1998 (as amended), sec 34 <http://www.pressenaevnet.dk/Information-in-English/The-Media-Liability-Act.aspx>.
[76] France, Law on Information Technology, Data Files and Civil Liberties, art 67.
[77] Iceland, Act on the Protection of Privacy as Regards the Processing of Personal Data, art 5.
[78] Ibid.
[79] Germany, Federal Data Protection Act, sec 41 (1); Germany, Interstate Treaty on Broadcasting and Telemedia, art 57 (1).
[80] Germany, Federal Data Protection Act, sec 41 (3). Sec 41 (2) also states that if *Deutsche Welle*'s journalistic processing "leads to the publication of counter-statements by the data subject, these counter-statements shall be added to the recorded data and retained for the same length of time as the data themselves".
[81] Germany, Interstate Treaty on Broadcasting and Telemedia 2010, art 47 (2).

appropriate in relation to Chart One below which provides a summary of the results here to round these into the nearest applicable category.

Chart One: Media Expression and the Data Quality Principles



V. MEDIA EXPRESSION AND THE TRANSPARENCY RULES (PROVISIONS (vi)-(viii))

A. Proactive Transparency (provisions (vi)-(vii))

Whilst a general presumption of openness is seen as an intrinsic aspect of fairness under the data quality provision (i) considered above, [82] the Directive complements this by establishing a specific rules requiring data controllers to proactively provide data subjects with information as to their identity, the purposes of the processing and any further information necessary to guarantee fair processing in respect of the data subject.[83] When information is collected directly from the data subject, a rule applies that this information must be provided at the time of collection in all circumstances.[84] In contrast, as regards indirect collection of information (e.g. via a third party or from the public domain) the information should be provided "at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed"[85] but not if this "would involve a disproportionate effort or disclosure is

[82] Directive 95/46, recital 38.

[83] Directive 95/46, arts 10 and 11. Many countries have transposed the language of the Directive directly in to their law. Others however have specified certain sometimes wide-ranging categories of information which they consider must be provided to data subjects either in all or only certain circumstances. Whilst clearly interesting, an analysis of this diversity is beyond the scope of this article.

[84] Directive 95/46, art 10.

[85] It might be thought that this rule only stipulates that the media must provide this information at the time of publication. However, the Directive defines 'third party' broadly as any natural or legal person other than the data subject, the controller or somebody processing on behalf or operating under the direct authority of controller (arts 2 (e) and (f)). According to Rasaiah and Newell (n 23) this means that "'publication' to the public is unlikely to be 'first disclosure'. Aside from sources checked in the course of compiling the report, this might have been from freelance journalists to news editor of the newspaper; staff journalists to freelance sub-editor; photographer to newsagency; reporter to independent programme producer" (232).

expressly laid down by law" so long as "appropriate safeguards" are in place.[86] This latter stipulation has been interpreted very differently by the Member States. Some have required provision of information in all cases, others allow a reliance on impossibility or disproportionate effort only in limited circumstances or subject to sometimes onerous conditions, whilst a third group allow for such a reliance without the application of any further safeguards at all.[87]

Turning to the approach of Member States to the application vis-à-vis the media of the proactive direct transparency rule when information is directly sourced from the data subject (provision (vi)), six jurisdictions (*Croatia, *Czech Republic, Romania, *Slovakia, Slovenia and *Spain) set out no media derogation and, therefore, fall within category a/1. Hungarian law includes a minimal exemption from this provision which, therefore, falls within category b/0.83. In sum, in situations where personally informing the data subject is either impossible or the cost is excessively high, this provision allows data controllers to choose instead to disclose to the world at large a wide range of information including the event of data collection, its scope, its purpose, the duration of its processing, possible controllers authorised to acquire knowledge of the data and information on the data subjects' rights and legal redress opportunities.[88] The laws of three jurisdictions (Greece, Italy and Liechtenstein) set out rule-bound exemptions which fall within category c/0.67. Greek law declares that journalists can be exempted from this provision but only when their collection of information "refers to public figures".[89] In Italy, the Data Protection Journalism Code states that journalists "must identify themselves, their profession and the purposes of collection, unless this may endanger their safety or otherwise make it impossible for them to carry out their journalistic activity" but then further adds that "they must refrain from subterfuge and harassment".[90] In some tension with the wording of the Directive, Liechtenstein extends to all types of controller the possibility to claim an exemption if provision of the information to the data subject is either "impossible" or "would involve disproportionate efforts".[91] It is left unclear whether impossibility is confined to technical impossibility or extends to a wider notion which would allow the purpose of processing, such as a need to collect data covertly, being taken into account. In any case, the idea of the effort of information provision being itself disproportionate does not obviously relate to situations where data is gathered through direct interaction with the data subject. In two jurisdictions (*Bulgaria and *Estonia) an exemption is provided based on an objective, public interest test as defined by category d/0.5. Eight jurisdictions (*France, *Gibraltar, *Ireland, *Latvia, Luxembourg, *Malta, *Poland and *UK) set out a more permissive public interest exemptions which, therefore, fall within category e/0.33. Luxembourg law provides that the rule does not apply "if its

[86] Ibid, art 11.2. The Directive also adds that such an exemption is not applicable where such information provision is impossible. Since a number of Member States, perhaps incorrectly, treat this situation as a mere example of a disproportionate effort circumstance arising, it will generally not be analysed separately.

[87] Presumably on the, albeit rather tenuous, basis that compliance with the rest of the data protection scheme constitutes the "appropriate safeguards" required by this clause in the Directive.

[88] Hungary, Act CXII of 2011 on Informational Self-Determination and Freedom of Information, sec 20 (4). Whilst traditional media activities are not explicitly excluded from this provision, it wording appears only to fit the, albeit probably only indirect collection of personal data, resulting from activities such as CCTV and perhaps street mapping services.

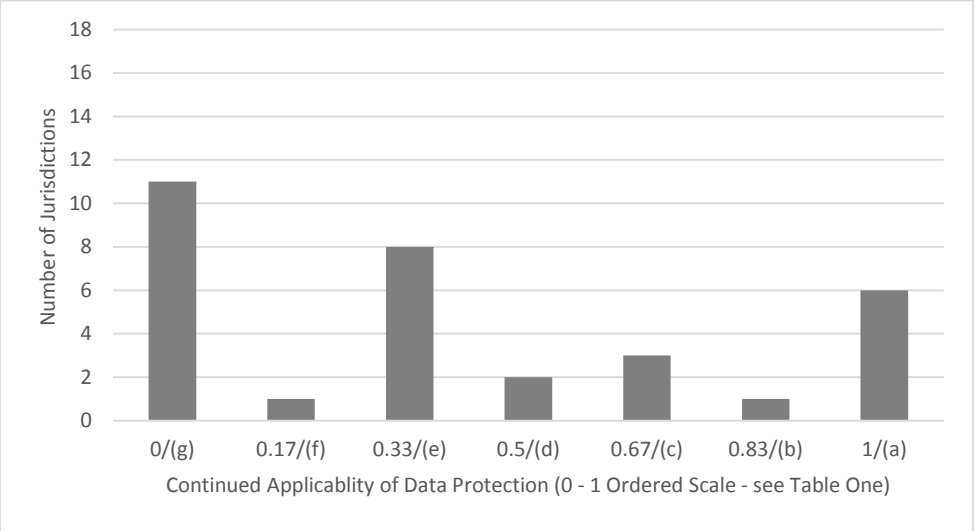
[89] Greece, Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data (as amended), art 11.5.

[90] Italy, Data Protection Journalism Code, art 2.1. The complete prohibition on subterfuge (*artifici*) is particularly far-reaching.

[91] Liechtenstein, Data Protection Act, art 5 (4).

application would compromise the collection of data from the data subject"[92] but then adds a general rider that the exemption only applies "in as far as … necessary to reconcile the right to privacy to the rules governing freedom of expression".[93] Belgium law sets out an exemption based on a test of minimal substantive content which, therefore, falls within category b/0.17. In sum, the media need not provide the specified information if this would "interfere with the collection of data from the data subject".[94] Finally, eleven countries (*Austria, Cyprus,[95] Denmark,[96] *Finland, Germany,[97] *Iceland, *Lithuania,[98] the Netherlands,[99] *Norway, Portugal[100] and *Sweden) exempt the media from compliance with these rules on an unconditional basis and therefore fall within category g/0. These results are summarized in Chart Two below.

Chart Two: Media Expression and Proactive Direct Transparency Rule



A very similar pattern emerges when the derogations from the proactive transparency rule applicable to cases of indirect collection of data are examined (provision (vii)). Six jurisdictions (*Croatia, *Czech Republic, *Hungary, Liechtenstein, Slovenia and *Spain) require the media to comply with the Directive's basic provisions here in full and, therefore, fall within category a/1. Whilst this list overlaps considerably with that set out for direct collection, such a similarity hides

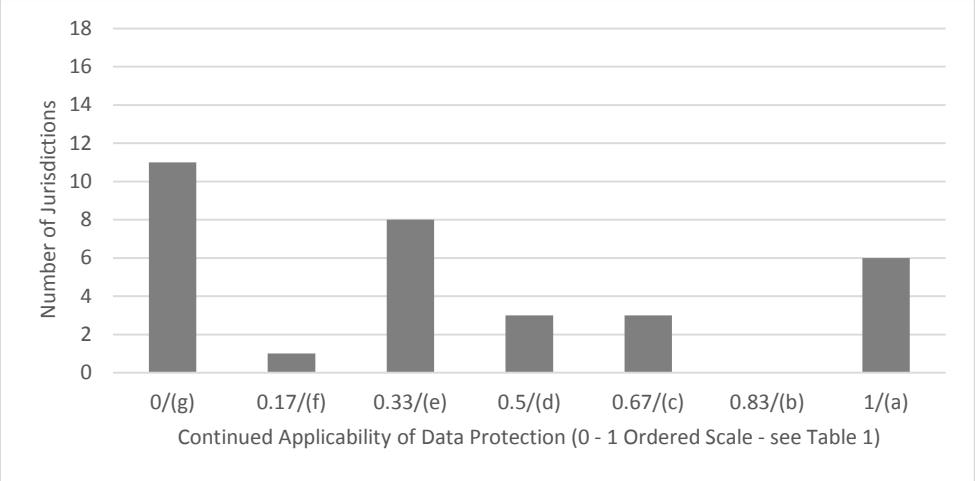
[92] Luxembourg, Coordinated Text of Law of 2 August 2002 on the Protection of Persons with regard to the Processing of Personal Data, art 9 (c).
[93] Ibid, art 9. The article further states that the provisions are "[w]ithout prejudice to provisions laid down in the Law of 8 June 2004 on freedom of expression in the media". Again, the stipulations of this general media statute are outside the scope of this article.
[94] Belgium, Data Protection Act, sec 3 (3) (b).
[95] Cyprus, Processing of Personal Data (Protection of Individuals) Law, sec 11 (5)
[96] Denmark, Compiled Version of the Act on Processing of Personal Data, sec 2.
[97] Germany, Federal Data Protection Act, s. 41; Germany, Interstate Treaty on Broadcasting and Telemedia, art 57 (1).
[98] Lithuania, Law on the Legal Protection of Personal Data, art 8.
[99] Netherlands, Personal Data Protection Act, art 3 (1).
[100] Portugal, Art on the Protection of Personal Data, art 10 (6).

significance internal divergence within the grouping in this latter case. Two jurisdictions (Croatia and Liechtenstein) provide that, without any particular safeguards being adopted, such information need not be provided if to do so would constitute a disproportionate effort.[101] In Spain, suspension requires either that such informing to be impossible or for it to be the view of the national Data Protection Authority (DPA) or a corresponding regional DPA that compliance with the rule would be disproportionate.[102] In the Czech Republic the information may only not be provided if "such data are necessary to exercise the rights and obligations ensuring from special Acts" or the controller "is processing exclusively lawfully published personal data".[103] Even these limitations are removed if the legitimating ground relied upon is that the processing is "essential for the protection of the rights and legitimate interests" either of himself or another person.[104] As explored below, this would appear to be the only legitimating ground in Czech law relevant to media expression. In Hungarian law, the requirement to provide information applies on an identical basis to that governing the direct collection of data considered above. Slovenian law requires that the information be provided to data subjects in all circumstances.[105] No jurisdictions fall within category b/0.83 here. Three jurisdictions (Greece, Italy and Romania) set out category c/0.67 rule-bound exemptions. The Greek exemption is identical to that it sets out in the case of direct collection considered above.[106] In Italy, the provision in the Data Protection Journalism Code requiring the media to provide information unless this makes it "impossible for them to carry out their journalistic activity" [107] leaves it ambiguous as to whom the information needs to be provided to. Given that the general Italian Data Protection Act does not grant the media an exemption from the general transparency provisions,[108] a strict interpretation would be that this information needs to be provided to the data subject here and not merely to any third party who may be supplying data. In any case, this Code additionally requires that "[i]f personal data are collected from data banks used by editorial offices, publishing companies must inform the public at least twice a year, through advertisements, of the existence of such data banks" including the address at which they can apply to exercise their data protection rights.[109] Romanian law provides an exemption only where compliance "might affect the confidentiality as to the source of the information".[110] Three jurisdictions (*Bulgaria, *Estonia and Slovakia) set out exemptions are provided based on an objective, public interest test of a form set out in category d/0.5. In the case of Slovakia, an exemption is available so long as processing is "necessary … for the purposes of informing the public

[101] Croatia, Personal Data Protection Act, art 7(4) and Liechtenstein, Data Protection Act, art 5 (4).
[102] Spain, Organic Law 15/10000 of 13 December on the Protection of Personal Data, sec 5 (5). Interestingly, no such stipulation applies if the processing is deemed to be for "for historical, statistical or scientific purposes". It should be noted that according to sec 5 (4) of the Spanish law the actual provision of information to data subject need only take place within three months of its initial recording.
[103] Czech, Consolidated Version of the Personal Data Protection Act, art 11 (3). It is unclear whether the media could point to a "special Act" regulating their processing.
[104] Ibid, art 5 (2) (e). The law governing legitimating conditions will be explored in a later section of the article.
[105] Slovenia, Personal Data Protection Act, art 19 (3).
[106] Greece, Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data (as amended), art 11.5. Interestingly, the general rules governing transparency in the case of indirect collection of data exclude any mention of an exemption on the grounds of disproportionate effort being possible.
[107] Italy, Data Protection Code for Journalism, art 2.1.
[108] Italy, Personal Data Protection Code, sec 13.
[109] Italy, Data Protection Journalism Code, art 2.2.
[110] 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 13.6.

by means of mass media" but not if the processing "violates the data subject's right to protection of his personal rights and privacy".[111] Eight jurisdictions (*Gibraltar, *France, *Ireland, *Latvia, Luxembourg, *Malta, *Poland and the *UK) set out more permissive public interest exemptions in a form falling with category e/0.33. These are identical to that governing direct collection considered above, with the exception of Luxembourg where the media can avoid providing information here not only when this would "compromise the collection of data" but also when this would compromise "a planned publication, or public disclosure in any form whatsoever of the said data, or would provide information that would make it possible to identify the sources of information".[112] Again, however, Luxembourg law provides that this exemption only applies "in as far as it is necessary to reconcile the right to privacy to the rules governing freedom of expression".[113] Similarly to the case of direct collection, Belgium law falls within category f/0.17 since the exemption here depends on a test with minimal substantive content. In sum, as long as the rule "interferes with the collection of data", "interferes with intended publication" or "provides indications as to the sources of information", the media may avoid complying.[114] Under the same legal provisions as that concerning direct collection considered above, eleven countries (*Austria, Cyprus, Denmark, *Finland, Germany, *Iceland, *Lithuania, the Netherlands, *Norway, Portugal and *Sweden) exempt the media from compliance with these rules on an unconditional basis and therefore fall within category g/0. These results are summarized in Chart Three below.

Chart Three: Media Expression and Proactive Indirect Transparency Rule



[111] Slovakia, Act on the Protection of Personal Data, sec 10 (3) (a). It is additionally stated that the exemption is not available "if such processing of personal data without consent of the data subject[,] is prohibited by a special Act or an international treaty binding for the Slovak Republic".
[112] Luxembourg, Coordinated Text of the Law of 2 August 2002 on the Protection of Persons with Regard to the Processing of Personal Data, art 9 (d).
[113] Ibid, art 9.
[114] Belgium, Data Protection Act, art 3 (3) (b).

B. Retroactive Transparency (provision (viii))

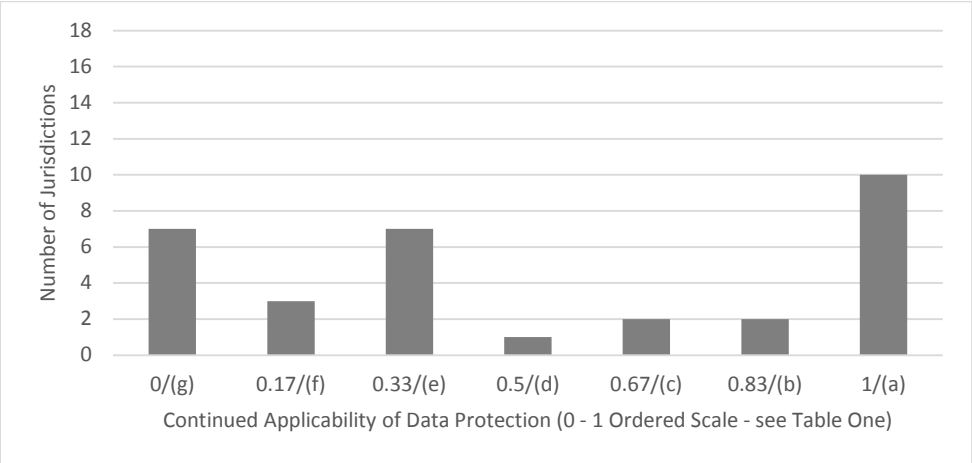
In addition to complying with the proactive transparency rules, controllers are also subject to a retroactive transparency rule (provision (viii)) under which they must on request supply data subjects "at reasonable intervals and without excessive delay or expense"[115] with much more extensive information about their processing operations together with communication "in an intelligible form of the data undergoing processing".[116]

Turning to media derogations available here, ten jurisdictions (*Bulgaria, *Croatia, Cyprus, *Czech Republic, Estonia, Greece, Hungary, *Latvia, *Slovakia, Slovenia and *Spain) apply this law in full to media processing and are coded within category a/1. Italy[117] and Romania[118] fall within category b/0.83 since they set out only a very narrower derogation protecting any confidentiality as to the sources of information held by journalists. Luxembourg and Portugal fall within category c/0.67 since they set out a full exception based on compliance with strict rules, namely, that the controller agrees to allow the Data Protection Authority vicarious access to the data on the data subject's behalf. [119] One jurisdiction (*Estonia) provides an exemption based on a strict public interest test and therefore falls within category d/0.5. Seven jurisdictions (*France, *Gibraltar, *Ireland, Liechtenstein, *Malta, *Poland and the *UK) provide a category e/0.33 exemption which is related to but more permissive than a strict public interest test. In Liechtenstein, the law allows for a refusal, restriction or deferral of information provision if "the personal data provides information as to its source", "access to drafts of publications would have to be granted", "the public's freedom to form an opinion would be compromised" or if the file "is being used exclusively as a personal work aid" by an individual journalist as opposed to a wider group within a media organisation.[120] Three countries fall within category f/0.17 since the exemption they set out is not universally absolute but either only stipulates a minimal substantive content (Belgium) or even excludes large swathes of the media unconditionally from compliance (Denmark and Germany). In Belgium, an exemption is provided not only where this would "provide indications as to the sources of information" but also where compliance would "interfere with intended publication".[121] In Denmark, the Law on Mass Media Information Databases 1994 provides that in relation to publicly available information databases, data subjects must be given "written notice of the information recorded in the database relating to him unless it is associated with excessive difficulties to obtain

[115] Directive 95/46, art 12 (a).
[116] Ibid, art 12. The definition of automated individual decisions is given in art. 15.
[117] Italy, Personal Data Protection Code, sec 138.
[118] Romania, Law No. 677/2001 on the Protection of Individual with Regard to art 12.6
[119] Thus, s. 29 (3) of the Luxembourg Coordinated Text of the Law of 2 August 2002 on the Protection of Persons with regard to the Processing of Personal Data not only provides a full exemption from disclosure of sources but also states that other data "must be accessed through the intermediary of the Commissioner Nationale pour la Protection des Donnèes in the presence of the Conseil de Presse or his representative, or the Chairman of the Conseil de Presse duly called upon." Art 11.3 of the Portuguese Act on the Protection of Personal Data establishes a similar rule, with art 11.4 adding that if this might prejudice freedom of expression and information or the freedom of the press, the Authority will only inform the data subject of any measures taken as a result.
[120] Liechtenstein, Data Protection Act, art 13. Interestingly, all but the last of these exemptions is limited to "periodically published" media organs. However, as this article is exploring the strength as opposed to the scope of the free speech derogation in data protection, this issue will not be further pursued.
[121] Belgium, Data Protection Act, sec 3.

the information".[122] However, not only are such individuals only entitled to the communication of such information at yearly intervals[123] but, as detailed above, the definition of such databases excludes both databases use internally and even public databases only including already published material which fall within the scope of the Danish Media Liability Act. In Germany, as detailed above, only *Deutsche Welle* and broadcasters regulated by the Interstate Treaty on Broadcasting and Telemedia are subject to substantive data protection provisions. As regards *Deutsche Welle*, the federal Data Protection Act establishes that if reporting "infringes the privacy of the individual, this person may request information about the recorded data relating to him/her on which the reporting was based". However, such a request may be refused if "the data allow the identification of persons who are or were professionally involved as journalists in preparing, producing or disseminating broadcasts", "the data allow the identification of the supplier or source of contributions, documents and communications for the editorial part" or if "disclosure of the data obtained by research or other means would compromise *Deutsche Welle*'s journalistic duty by divulging its information resources".[124] The provision governing other broadcasters is even more permissive. Here, the Interstate Treaty on Broadcasting and Telemedia states that, whilst a person who is "negatively affected in his interests meriting protection" may "demand information on the underlying data storage about his person", such information may be denied not only if the data would allow conclusions on either "persons who were involved in the preparation of production or transmission" or "the person of the sender or of the guarantor of contributions, documents and communications for the editorial section" but also "if its provision would prejudice the journalistic task of the broadcaster by exploring the information gathered".[125] Finally, seven countries (*Austria, *Finland, *Iceland, *Lithuania, the Netherlands,[126] *Norway and *Sweden) exempt the media unconditionally from compliance with this rule and therefore fall within category g/0. Chart Four below summarises these results.

Chart Four: Media Expression and the Retrospective Transparency Rule



[122] Denmark, Lov om massemediers informationsdatabaser, sec 11 (1).
[123] Ibid, sec 11 (2).
[124] Germany, Federal Data Protection Act, sec 41.
[125] Germany, Interstate Treaty on Broadcasting and Telemedia, art 47 (2) and similar wording in art 57 (2).
[126] Netherlands, Personal Data Protection Act, art 3 (1).

VI. MEDIA EXPRESSION AND THE SENSITIVE INFORMATION RULES (PROVISIONS (ix)-(xv))

In addition to requiring compliance with the other elements of the data protection regime, the Directive stipulates greatly increased protection when data falls within a category which it deems to be sensitive due to its relationship with intimate private life and/or the possibility of unfair discrimination. In sum, this element includes seven provisions restricting the processing of data:

(ix) revealing racial or ethnic origin
(x) revealing political opinions
(xi) revealing religious or philosophical beliefs
(xii) revealing trade-union membership
(xiii) concerning health
(xiv) concerning sex life, and
(xv) relating to offences, criminal convictions and security measures.

These categories of data are intended to be largely exhaustive.[127] As regards last data category (provision xv), the Directive's rule, which is subject to no mandatory exceptions, is that the processing may only be carried out "under the control of official authority".[128] In relation to the first six categories of data (provisions (ix)-(xv)), the Directive's starting point is that processing must be prohibited.[129] However, in these cases, Member States are required to provide exclusions from this ban in a number of very restricted circumstances. Only two of these, that the "data subject has given his explicit consent to the processing" and that "the processing relates to data which are manifestly made public by the data subject" have clear application to the media activities.[130] Moreover, as regards explicit consent, the Directive adds that the ban should remain in place where Member State law provides that the prohibition "may not be lifted by the data subject's giving his consent".[131] Member States are also to determine processing operations likely to "present specific risks to the rights of freedoms of data subjects" and mandate that they be subject to a checking procedure by the DPA prior to such processing beginning.[132] As will be seen, some have interpreted this provision as allowing, in effect, the imposition of a licensing system for the processing of sensitive data, at least when computerised means are used. Overall, and unsurprisingly, the actual default rules governing the processing of sensitive data continue to differ considerably.

Turning to the derogations available to the media here, with two exceptions (Italy and *Latvia) discussed below, Member States have adopted an identical approach vis-à-vis all the data categories. The law in nine jurisdictions (*Croatia, *Czech Republic, Hungary, Liechtenstein, Lithuania, Portugal, *Slovakia, Slovenia and *Spain) fail to provide for any media derogation and

[127] Art 8.6, Directive 95/46 does state, without further elaboration, that Member States "shall determine the conditions under which a national identification number or any other identifier of general application may be processed". This very specific issue is outside the broad scope of interest of this article. Art 8.5 of the Directive also empowers Member States to specially protect data relating to administrative sanctions and judgments in civil cases on the same basis as data relating to offences, criminal conditions and security measures. Many of these additional classes of data could in any case be considered to fall within a very broad interpretation of provision (xv) and so will not be separately analysed.
[128] Directive 95/46, art 8.3.
[129] Directive 95/46, art 8.1.
[130] Directive 95/46, art 8.2.
[131] Directive 95/46, art 8.2 (a).
[132] Directive 95/46, art 20.

therefore must be classified within category a/1. However, this commonality hides very significant divergences as to the general circumstances when the ban on processing sensitive data in the private sector may be lifted as a result either of the data subject's explicit consent or his manifestly putting this information into the public domain. In Hungary, there is no public domain exception and any consent must be writing.[133] Spanish law excludes any mention of controlling group (xv) data vis-à-vis the private sector. However, as regards the other groupings, it also excludes a public domain exemption and further requires that religious or philosophical belief, political opinion and trade union membership data processing requires written consent.[134] In Lithuania, consent must be in a "form giving an unambiguous evidence of the data subject's free will"[135] and, in addition, a prior DPA check must take place if sensitive data is to be processed on computer.[136] In Portugal, a DPA prior check must take place if consent is being relied upon[137] and the public domain exception is restricted to circumstances where consent for the particular processing in question can be "clearly inferred" from this.[138] In Slovenia, the public domain exemption only applies if the data subject "publicly announces them without any evident or explicit purpose of restricting their use"[139] and consent must "as a rule be in writing".[140] In Slovakia, consent must always be in writing[141] and, in any case, no exemption is provided from the stipulation that group (xv) data may only be processed "by a person entitled to it by a special Act".[142] Croatian law sets out a full explicit consent and public domain exception for data within groups (ix)-(xiv) but as regards group (xv) data it simply states that such data must be "solely controlled by the competent authorities".[143] Czech law states as regards consent that the controller must be able to prove its existence "during the whole period of processing".[144] Liechtenstein law provides a full explicit consent and public domain exemption as broad as that set out as a minimum default in the Directive.[145] There are no jurisdictions in category b/0.83. The provisions in four jurisdictions (Belgium, Greece, Luxembourg and Romania) set out a media exemption based on the satisfaction of certain pre-determined rule-based criteria and, therefore, fall within category c/0.67. The Greek provisions are particularly onerous. Here, a permit must be requested from the DPA which is to be exceptionally granted but only when "[p]rocessing concerns data pertaining to public figures", "that such data are in connection with the holding of public office or the management of third parties' interests", "processing is absolutely necessary in order to ensure the right to information on matters of public interest, as well as within the framework of literary expression" and "provided that the right to protection of privacy and family

[133] Hungary, Act CXII of 2011 On Informational Self-Determination and Freedom of Information, sec 5 (2)(a).
[134] Spain, Organic Law 15/1999 of 13 December on the Protection of Personal Data, art. 7. The article adds that "[f]iles created for the sole purpose of storing personal data which reveal the ideology [political opinion], trade union membership, religion, beliefs , racial or ethnic origin or sex life remain prohibited".
[135] Lithuania, Law on the Legal Protection of Personal Data, art 2 (11).
[136] Ibid, art 33.1.1. Processing for very limited purposes such as internal administration is excluded from this requirement.
[137] Portugal, Act on the Protection of Personal Data, art 7 (2).
[138] Ibid, art 7 (3) (c). This could be a live issue for the media especially as regards data revealed publicly on social networking sites and the like.
[139] Slovenia, Personal Data Protection Act, art 13 (5).
[140] Ibid, art 13 (1).
[141] Slovakia, Act on the Protection of Personal Data, art 9 (1).
[142] Ibid, art 8 (3).
[143] Croatia, Personal Data Protection Act, art 8 (2).
[144] Czech Republic, Consolidated version of the Personal Data Protection Act, art 9 (a).
[145] Liechtenstein, Data Protection Act, art 18 (c).

life is not violated in any way whatsoever".[146] In Belgium, an exemption is provided "if the processing relates to personal data which has apparently been made public by the data subject or which is closely related to the public nature of the data subject or of the facts in which the data subject is involved".[147] In Luxembourg, any data must either "have manifestly been made public by the data subject himself" or be "directly related to the public life of the data subject or the event in which he is involved in a deliberate manner".[148] In Romania, it is necessary that the data are "manifestly made public by the data subject or are closely related to the public figure quality of the person concerned or the public nature of the facts involved".[149] Three jurisdictions (*Bulgaria, Cyprus and *Estonia) are placed within category d/0.5 here since they set out an open-textured exemption based on a strict public interest test. In Cyprus, this exemption applies "as long as the right to privacy and family life are not violated".[150] Six jurisdictions (*France, *Gibraltar, *Ireland, *Malta, *Poland and the *UK) set out a more permissive public interest exemption which therefore falls within category e/0.33. Two countries fall within category f/0.17 since the exemption set out is not universally unconditional but either has minimal substantive content (Netherlands) or excludes large swathes of media activity absolutely from these provisions (Denmark). In the Netherlands, an exemption is granted so long as the processing is "necessary" for journalistic purposes.[151] In Denmark, the Law on Mass Media Information Databases provides that in relation to publicly available mass media electronic information databases "[i]nformation on individuals' purely private matters, including information on race, religion, political, fraternal, sexual, criminal record, health, serious social problems and the abuse of stimulants and the like, should not be stored in the information database after three years from the event that gave rise to the database entry or, if such a date cannot be fixed, three years after the information was entered into the database".[152] However, these provisions do not apply if "there is such an interest that the information is publicly available that concern for the individual's interest in ensuring that the information is erased should give way to the interest in freedom of information".[153] Even more critically, as outlined above, the definition of publicly available information databases excludes not only internal databases used by the mass media but also databases which only include already published text, images, periodicals, audio or video programs which fall within the Danish Media Liability Act.[154] Six jurisdictions (*Austria, *Finland, Germany,[155] *Iceland, *Norway and *Sweden) exclude the media unconditionally from these provisions and therefore fall within category g/0. Turning to the two

[146] Greece, Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data (as amended), art 7 (2) (g). It should further be noted that under Greek data protection law a permit must even be obtained if processing data on the basis of consent (which in any case must be written) (art 7 (2) (a)) or when such processing is justified by the fact that it relates to data which are manifestly made public by the data subject (art 7 (2) (c)).

[147] Belgium, Data Protection Act, art 3 (3) (a).

[148] Luxembourg, Data Protection Act, art 9 (a). The exemption also only applies in so far as "necessary to reconcile the right to privacy with the rules governing freedom of expression".

[149] 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 11.

[150] Cyprus, Processing of Personal Data (Protection of Individuals) Law, sec 6 (2) (i).

[151] Netherlands, Personal Data Protection Act, art 3 (2).

[152] Denmark, Lov om massemediers informationsdatabaser, sec 8(3) (translated from Danish).

[153] Ibid, art 8 (4).

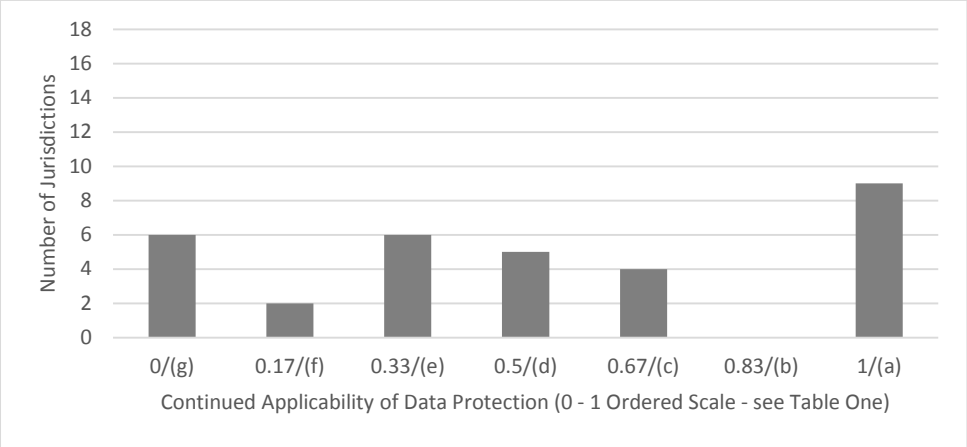
[154] Ibid, sec 1 (1). This latter Act makes no provision for specially protecting sensitive groupings of information.

[155] Germany, Federal Data Protection Act, sec 41; Germany, Interstate Treaty on Broadcasting and Telemedia, art 57 (1).

exceptional cases, *Latvian law does not provide any exemption the prohibition on private sector processing of data relating to offences, criminal convictions and security measures but does provide a permissive public interest exemption from the other sensitive data rules. It therefore must be coded a/1 in relation to provision (xv) and e/0.33 in relation to provisions (ix)-(xiv). Meanwhile, in Italy, whilst the media are exempted from the general regime governing sensitive data,[156] the Data Protection Journalism Code restricts the processing of health and sex life data (groups xiii and xiv) via specific rule-bound provisions in the form of category c/0.67, whilst also requiring adherence to an objective, public interest test of a category d/0.5 type when using any sensitive data, including data falling within the other five categories outlined above. Thus, the Code states that "[i]n referring to the health of an identified or identifiable person, journalists must respect his/her dignity, right to privacy and decorum especially in cases of severe or terminal diseases; they must avoid publishing analysis data of exclusively clinical interest"[157] and also that journalists "must avoid reporting the sex life of any identified or identifiable person".[158] However, as a partial caveat it is stated in both cases that "[p]ublication is allowed for the purpose of ensuring that all material information is disclosed and by respecting a person's dignity, if such person plays an especially important social or public role".[159] More generally, the Code provides that when processing sensitive data "journalists must ensure the right to information on facts of public interest, by having regard to the materiality of such information, and avoid any reference to relatives or other persons who are not involved in the relevant events"[160] and also that ""[i]n exercising the rights and duties related to freedom of the press, journalists must respect a person's right to non-discrimination on account of his/her race, religion, political opinions, sex, personal circumstances, bodily or mental condition".[161] The combined Latvian and Italian scores for the sensitive data rules is 0.43 and 0.55 respectively. However, for the purposes of Chart Five below which summarizes the results within this element, these scores have been rounded into the nearest whole category of d/0.5.

[156] Italy, Personal Data Protection Code, s. 137.
[157] Italy, Data Protection Journalism Code, art. 10.1.
[158] Ibid, art. 11.1.
[159] Ibid, arts. 10.2 and 11.2.
[160] Italy, Data Protection Journalism Code, art. 5. The article adds a caveat for the media by stating that "[w]ith regard to data concerning circumstances or events that have been known either directly by the persons concerned or on account of their public conduct, the right to subsequently provide proof of the existence of lawful justification deserving legal protection is hereby left unprejudiced".
[161] Italy, Data Protection Journalism Code, art. 9.

Chart Five: Media Expression and the Sensitive Data Rules



VII. CONTROL CONDITIONS ELEMENT (PROVISIONS (xvi)-(xviii))

Complementing the provisions detailed above, the Directive also includes three further provisions which, whilst imposing obligations of a substantive nature on data controller's own processing operations, are primarily designed to ensure that the other substantive elements of the scheme are not undermined. These subsidiary provisions, and the media derogations from them, are considered in this section.

A. Legitimating Ground Condition (provision (xvi))

Under the Directive personal data may not be processed unless one or more of legitimizing grounds set out in article 7 are satisfied. Although the first of these is data subject consent, this article also sets out five other potential grounds. Whilst these are generally also quite restrictive, the sixth ground is open-textured, legitimising processing which is "necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection".[162] The inclusion of such an all-encompassing condition underscores the fact that, in contrast to article 8 of the Directive regulating sensitive data, it is not the purpose of article 7 to provide for a special regime for data processing. Rather, by specifying in a closed and structured form "the grounds on which personal data may lawfully be processed",[163] its aim is to undergird compliance with the fair and lawful processing and legitimate purposes requirements in the first and second data quality principles (provisions (i) and (ii)) considered above.

Turning to the derogations set out for the media, twelve jurisdictions (Belgium, *Croatia, Cyprus, *Czech Republic, France, Greece, Hungary, *Lithuania, Luxembourg, Portugal, Slovenia and *Spain) do not provide for any derogation and, therefore, fall within category a/1. Many of these

[162] Directive 95/46, art 7 (f).
[163] European Commission (n 19), 16.

countries also set out the legitimating grounds using slightly different wording to that the Directive, often thereby prioritising the use of the first condition of data subject consent in some way.[164] Spanish law goes much further by generally preventing the open-textured condition being relied upon when data are communicated to third parties unless that data in question have been collected from publicly available sources.[165] Liechtenstein law falls within category b/0.83 since it does not exempt the media from the need to satisfy a legitimating condition but rather glosses this by stating that in applying the sixth open-textured condition "the overriding interests of the processing person shall in particular be taken into account where the processing person … processes data on a professional basis for the sole purpose of publication in the editorially-controlled section of a published media organ".[166] Two jurisdictions (Italy and Romania) provide an exemption which is available only if certain specific circumstances or rules as defined by category c/0.67 are satisfied. In Italy, the media are excluded from compliance with the general legitimating grounds,[167] but must adhere to provisions as regards the materiality of information,[168] protection of a person's residence,[169] protection of children[170] and protection of personal dignity[171] set out in the Data Protection Journalism Code. In Romania, an exemption is only available when and in so far as data is "manifestly made public by the data subject or are closely related to the public figure quality of the personal concerned or the public nature of the facts involved".[172] Three jurisdictions (*Bulgaria, *Estonia and Slovakia) provide for an exemption based on an objective, public interest test and, therefore, fall within category d/0.5. Whilst Slovakian law does not set out a precise cognate of the sixth open-textured provision, it does specifically authorise processing "necessary … for the purpose of informing the public by means of mass media" unless if "by processing of personal data for such purpose the controller violates the data subject's right to protection of his personal rights and privacy".[173] Six jurisdictions (*Gibraltar, *Ireland, *Latvia, *Malta, *Poland and the *UK) include a more permissive, public interest exemption in their law as set out in category e/0.33. No countries

[164] This is sometimes coupled with language which explicitly sets a somewhat higher threshold to the use of alternative legitimating conditions. For example, the Greek Data Protection Act not only sets out a presumption that data consent will be obtained (art 5 (1)) but also provides that the open-textured equivalent of article 7(1)(g) in the Directive may only be utilized when processing is "absolutely necessary" for the purposes of a legitimate interest (art 5 (2) (e)).

[165] Spanish, Organic Law 15/1999 of 13 December on the Protection of Personal Data, art 11. These provisions were recently held to be invalid by the CJEU in C-468/10 and C-469/10 *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and another v Administración del Estado*, EU:C:2011:777.

[166] Liechtenstein, Data Protection Act, art 17.2 (d).

[167] Italy, Personal Data Protection Code, sec 171.2. Again, interpretation of this exemption is complicated by the fact that, similarly to Spain, general use of the open-textured condition is excluded if processing involves "dissemination of the data" (sec 24 (f)) unless the processing "concerns data taken from public registers, documents or records that are publicly available, without prejudice to the limitations and modalities laid down by laws, regulations and Community legislation with regard to their disclosure and publicity" (sec 24 (c)).

[168] Italy, Data Protection Journalism Code, art 6.

[169] Ibid, art 3.

[170] Ibid, art 7.

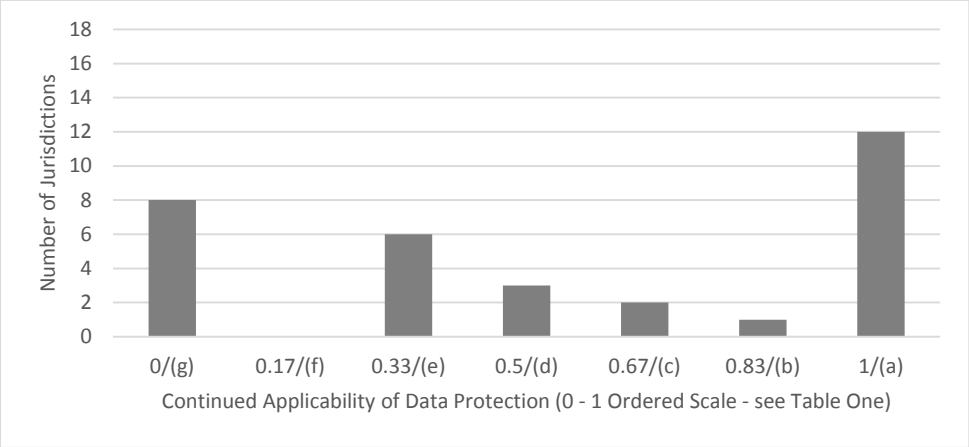
[171] Ibid, art 8.

[172] 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 11.

[173] Slovakia, Act on the Protection of Personal Data, sec 10 (3) (a). This provision also stipulates that such an exemption is also not available "if such processing of personal data without consent of the data subject is prohibited by a special Act or an international treaty binding for the Slovak Republic".

fall within category f/0.17. Finally, eight jurisdictions (*Austria, Denmark,[174] *Finland, Germany,[175] *Iceland, Netherlands,[176] *Norway and *Sweden) provide for an unconditional media exemption here and, therefore, fall within category g/0. These outcomes are summarized in Chart Six below.

Chart Six: Media Expression and the Legitimating Ground Provision



B. Notification of Processing Condition (provision (xvii))

Section IX of the Directive generally requires the controller to provide the DPA with a registration of their processing operations, the details of which are then to be placed on a public register.[177] At a minimum, such registration must include at least the name and address of the controller, the purpose or purposes of processing, the category of categories of data subject and the data or categories of data relating to them which are processed, the recipients or categories of recipient to whom the data might be disclosed, proposed transfers of data to third countries and a general description of measures taken to ensure security of processing.[178] Member States need not require such registration where the data controller appoints an independent personal data protection official or where the processing has been specified in detail and is deemed unlikely "to affect adversely the rights and freedoms of data subjects" or where the processing of data is not computerized.[179] However, even in these cases, Member States are obliged to ensure that controllers provide a notification to any person on request including the information which would otherwise be on the public register.[180] These provisions were designed to instantiate the two core control purposes of providing a basic minimum of openness in data processing, thus undergirding the first data principle's fair and lawful processing requirements, and providing a structure "to serve

[174] Denmark, Compiled Version of the Act on Processing of Personal Data, sec 2.
[175] Germany, Federal Data Protection Act, s. 41; Germany, Interstate Treaty on Broadcasting and Telemedia, art 57 (1).
[176] Netherlands, Personal Data Protection Act, art 3 (1).
[177] Directive 95/46, art 21.2. In order to ensure that the relevant measures are not undermined, notification related to the security of processing is excluded from this publicity requirement.
[178] Directive 95/46, art 19.
[179] Directive 95/46, art 18.
[180] Directive 95/46, art 21.3.

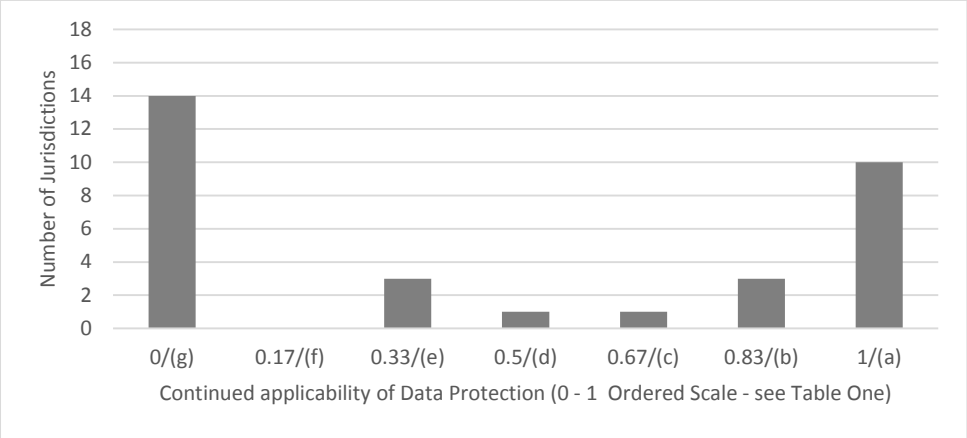
as the basis for selective monitoring of the legitimacy of processing operations by the supervisory authority".[181]

As regards the media derogations available, ten jurisdictions (*Croatia, Cyprus, *Czech Republic, *Estonia, Greece, Portugal, Romania, Slovakia, *Spain and the *UK) set out no special provision in favour of the media here and, therefore, fall within category a/1. In almost all these countries either all or at least the vast majority of computerized processing is subject to registration with the national DPA. However, in Estonia, registration is only required when processing sensitive data[182] and, even in these cases, data controllers may alternatively notify the DPA of the appointment of an independent data protection officer.[183] Provisions in Denmark, France and Latvia provide only for exemptions of a very narrow scope and, therefore, fall within category b/0.83. In Denmark, the Law on Mass Media Information Databases requires that the mass media notify the DPA of all internal editorial mass media electronic information databases and that the latter publish an annual list of these. Publicly available mass media information databases are also subject to notification both to the DPA and the Press Council.[184] Databases which only include already published text, images, periodicals, audio or video programs are excluded from these requirements.[185] In France the media must notify the DPA of the appointment of an independent Data Protection Officer and that person must maintain a register of processing carried out by the data controller.[186] In Latvia, an exemption is only available if no data on a person's health or offences, criminal convictions and administration violation cases are to be processed and if no data are to be transferred outside the EEA.[187] In Liechtenstein a general exemption is provided for but this is dependent on compliance with specific pre-defined category c/0.67 rules, specifically, that files "are being used by journalists exclusively as a personal work aid" or "used exclusively for publication in the editorially-controlled section of a periodically-published media organ" but in this case not if data is "disclosed to third parties without the knowledge of the data subjects". [188] *Bulgaria provides an exemption here on the basis of an objective, public interest test as defined in category d/0.5. *Gibraltar, *Malta and *Poland provide for an exemption based on a more permissive public interest test as set out in category e/0.33. No jurisdiction falls within category f/0.17. Fourteen jurisdictions (*Austria, Belgium, *Finland, Germany,[189] Hungary,[190] *Iceland,

[181] European Commission (n 19), 28.
[182] Estonia, Personal Data Protection Act, sec 27.
[183] Ibid, sec 30. Such a person must keep a register of processing carried out by the data controller (s. 30 (3)). However, in tension with the Directive, there appears to be no requirement placed on either these data controllers, or others not subject to registration, to make such information available to any member of the public on request.
[184] Denmark, Lov om massemediers informationsdatabaser, sec 3 and sec 6. In both cases the notifiable information is of a rather narrower than that required generally under the information notification requirement.
[185] Ibid, sec 1 (1).
[186] France, Data Protection Act, art 67.
[187] Latvia, Personal Data Protection Law, sec 21 (2) (3) and sec 21 (3).
[188] Liechtenstein, Data Protection Ordinance, art 4.
[189] Germany, Federal Data Protection Act, sec 41; Germany, Interstate Treaty on Broadcasting and Telemedia, art 57 (1).
[190] Hungary, Act CXII of 2011 on Informational Self-Determination and Freedom of Information, sec 65 (3) (g). It should be noted that the exemption is not only limited to media service providers (a question concerning the definitional scope of the media which is outside the purview of this article) but is limited to processing "which

*Ireland, Italy,[191] *Lithuania, Luxembourg,[192] Netherlands,[193] *Norway, Slovenia[194] and *Sweden) grant the media an unconditional exemption here and therefore are placed in category g/0. These results are summarised in Chart Seven below.

Chart Seven: Media Expression and the Notification of Processing Requirement



C. Data Export Condition (provision (xviii))

Article 25 of the Directive requires that Member States generally ensure that personal data cannot be transferred to a country outside the EEA unless than country ensures an "adequate level of protection" in relation to that data. Apart from "where otherwise provided by domestic law governing particular cases", Member States are required under article 26 to provide that this rule is not applicable when at least one of certain restrictive criteria is satisfied such as unambiguous data subject consent or the necessity of transfer on "important public interest grounds". The provision as a whole was intended to ensure that the pan-EU scheme for protecting personal data could not be "nullified by transfers to other countries in which the protection provided is inadequate"[195] and in most EEA States is secured through strict bureaucratic arrangements overseen by the DPA. Given the intrinsically global nature of many data processing operations, the provision can impose a variety of additional substantive duties on data controllers including potentially restricting the circumstances in which information can be subject to worldwide electronic publication.[196]

exclusively serve their own information activities". This could be read as imposing certain restrictions on the use of this exemption.

[191] Italy, Personal Data Protection Code, sec 37 (journalism excluded from listing of types of processing requiring notification).

[192] Luxembourg, Coordinated Text of the Law of 2 August 2002 on the Protection of Persons with Regard to the Processing of Personal Data, art 12 (2) (d).

[193] Netherlands, Personal Data Protection Act, art 3 (1).

[194] Slovenia, Personal Data Protection Act, art 7 (3).

[195] European Commission (n 19), 34.

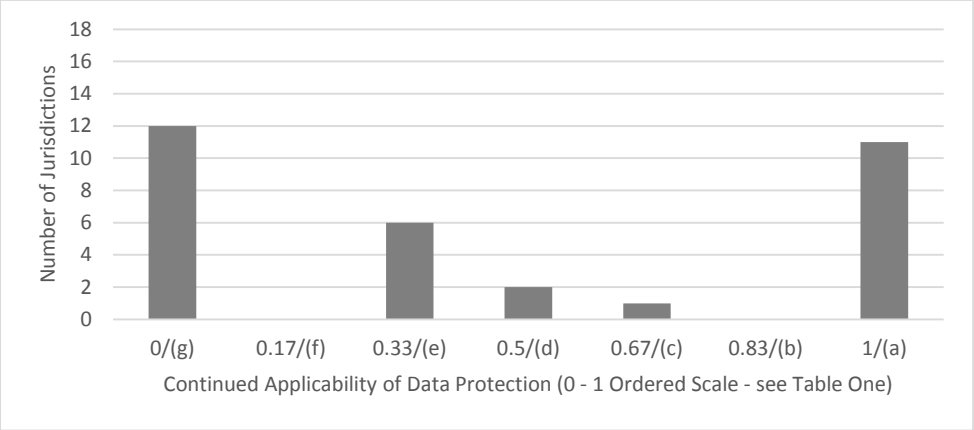
[196] At least as regards individuals posting material on the internet, the CJEU in *Lindqvist* (2003) appeared to restrict the circumstances in which an individual would themselves be responsible for a transfer of data when they uploaded information onto an internet server maintained by a hosting provider established within the EU

Turning to the derogations available for the media here, eleven jurisdictions (*Croatia, Cyprus, *Czech Republic, Greece, Hungary, *Ireland, *Latvia, Liechtenstein, Portugal, *Slovakia and *Spain) do not set out any special provisions and, therefore, fall within category a/1. Most of these countries require that at least the great majority of transfers are notified to the DPA and, absent the transfer country itself or the particular protections utilized (e.g. contractual undertakings) having already been explicitly held adequate, subject to a prior authorization procedure.[197] Others are rather more liberal[198] including one (Ireland) which places a strong emphasis on data controllers themselves establishing that the adequacy standard has been met in relation to any particular transfer.[199] No national provisions fall within category b/0.83. Romanian law falls within category c/0.67 since the exemption here depends on certain pre-defined conditions being met, namely that "the data were made public expressly by the data subject or are related to the data subject's public quality or to the public character of the fact's he/she is involved in".[200] *Bulgaria and *Estonia set out an exemption based on an objective, public interest test defined in category d/0.5. In six jurisdictions (*France,*Gibraltar, Luxembourg, *Malta, *Poland, and the *UK) an exemption is available on the basis of a more permissive public interest test which falls within category e/0.33. The Luxembourg provision is particularly light touch since the only restriction set out is that it applies only "in as far as … necessary to reconcile the right to privacy to the rules governing freedom of expression".[201] No national provisions fall within category f/0.17. Twelve jurisdictions (*Austria, Belgium,[202] Denmark,[203] Finland,[204] Germany,[205] *Iceland, Italy,[206] *Lithuania, Netherlands,[207] *Norway, Slovenia[208] and *Sweden) exclude the media unconditionally from this provision and therefore fall within category g/0. These results are summarized in Chart Eight below.

(at [72]). Nevertheless, this narrower holding has not altered the general understanding which DPAs have adopted to the relationship between global publication and the transfer regime. For example, the UK Information Commissioner's Office states clearly that a data controller will be liable for an international transfer when information is "loaded onto the internet with the intention that the data be accessed in a third country" and a transfer then takes place (UK, Information Commission's Office 'The eighth data protection principle and international transfers' (2010) <https://ico.org.uk/media/for-organisations/documents/1566/international_transfers_legal_guidance.pdf>.

[197] See for example, Cyprus, Processing of Personal Data (Protection of Individuals) Law, sec 9 (1) and Portugal, Act on the Protection of Personal Data, art 19 (3). The exact requirements, however, do differ.
[198] For example, in Spain, it would appear that only the prior authorization requirement applies and not the general requirement of specific notification of transfers (Spain, Organic Law 15/1999 of 13 December on the Protection of Personal Data, arts 33 & 34).
[199] Ireland, Data Protection Act, sec 11.
[200] Romania, Data Protection Act. art 29.6.
[201] Luxembourg, Coordinated Text of the Law of 2 August 2002 on the Protection of Persons with Regard to the Processing of Personal Data, art 9. The article further states that exemption is "[w]ithout prejudice to provisions laid down in the Law of 8 June 2004 on freedom of expression in the media". The stipulations of this general media statute, however, are outside the scope of this article.
[202] Belgium, Data Protection Act, art 3 (3).
[203] Denmark, Compiled Version of the Act on Processing of Personal Data, sec 2.
[204] Finland, Personal Data Act, sec 2 (5).
[205] Germany, Federal Data Protection Act, sec 41; Germany, Interstate Treaty on Broadcasting and Telemedia, art 57 (1).
[206] Italy, Personal Data Protection Code, sec 137 (1) (c).
[207] Netherlands, Personal Data Protection Act, art 3 (1).
[208] Slovenia, Personal Data Protection Act, art 7 (3).

Chart Eight: Media Expression and the Data Export Provision



VIII. INTEGRATED RESULTS

Given that the previous sections have now outlined the approaches taken vis-à-vis the media to all the substantive data protection provisions, it is possible to compile a comprehensive picture of the derogations in each EEA jurisdiction's law both in relation to each of the four substantive elements of EU data protection and as regards this regime as a whole. Since, with a few minor deviations, Member States have adopted the same internal approach to all the provisions within the data quality principles and sensitive data elements respectively, Charts One and Five above have effectively already provided such a comprehensive picture in relation to these two elements which, moreover, can still be based directly on our seven ordered categories. In relation to the other two elements and the results as a whole, however, the divergences of result between the provisions means that the numerical scores generated no longer precisely map on to the ordered categories. Despite this, the existence of our standardized 0, 1 scale still ensures that these scores similarly represent the extent to which that aspect of data protection remains applicable vis-à-vis the media. Charts Nine and Ten below provide a summary of the numerical scores for the transparency rules and control conditions respectively, rounded to the nearest 0.1.

Chart Nine: Media Expression and the Transparency Rules

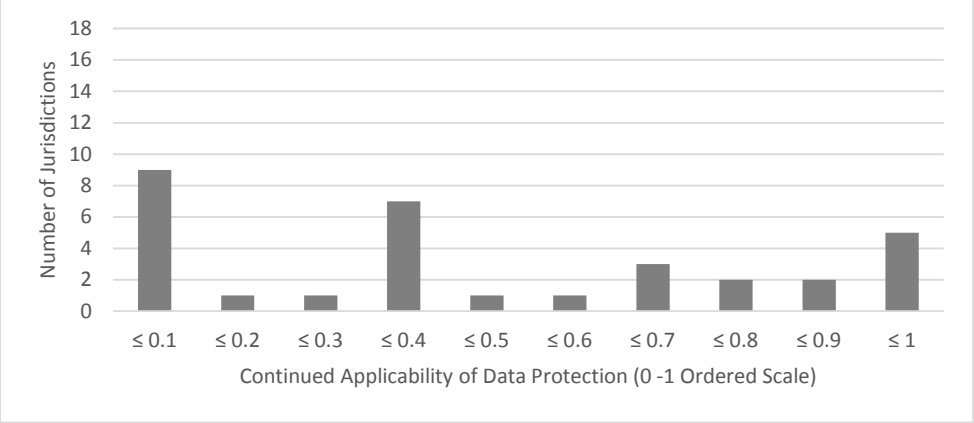
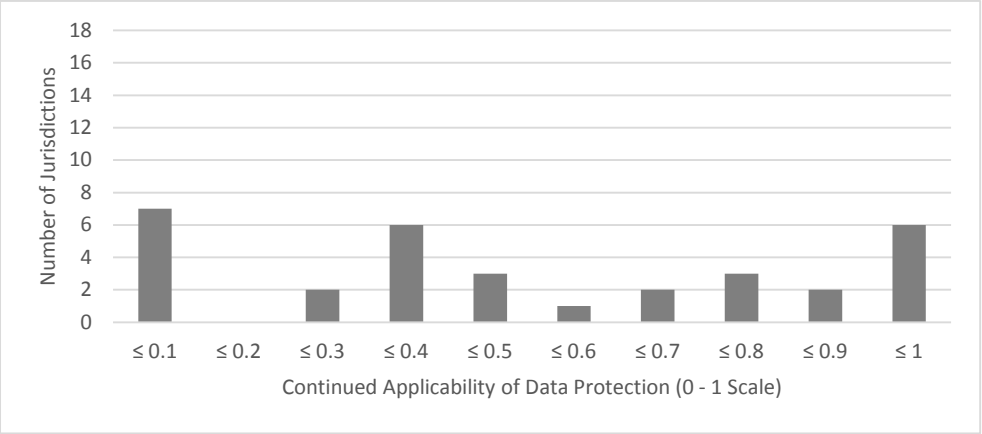


Chart Ten: Media Expression and the Control Rules



These four charts highlight the serious divergence of approach between the EEA States here. Only in relation to the data quality principles (Chart One) have even a slight majority (56%) of Member States adopted the same approach, in this case that the principles should remain fully applicable even in the media sphere. There is no evidence of any overarching European pattern in relation to the sensitive data rules (Chart Five), the transparency rules (Chart Nine) or the control conditions (Chart Ten). Instead, there is some evidence of a clumping not only in the middle but also at the extremes of both full and no protection. Even at the individual provision level, it is striking that, aside from the data quality principles, there is no case where a majority of states have been coded into the same category. Moreover, the provisions which come nearest to this – the legitimating ground condition (provision (xvi)) (38% placed in category a/1), notification of processing condition (provision (xvii)) (44% placed in category g/0) and data export condition (provision (xviii)) (38% placed in category g/0) – point less to a commonality of approach than to evidence of a polarized outcome. For example, whilst as regards provision (xviii), 38% of states are placed in category g/0, 34% are placed in the polar opposite category of a/1.

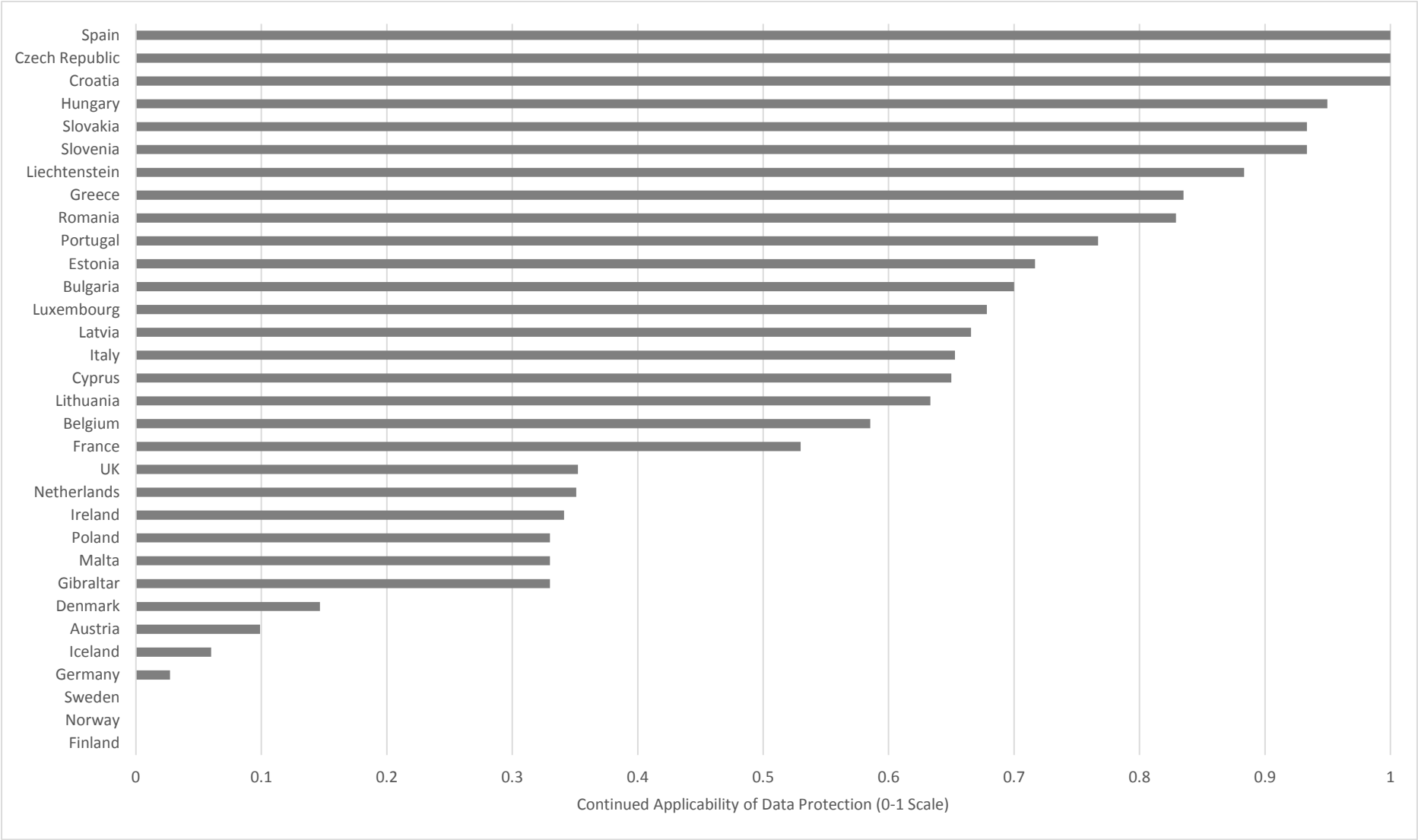
Finally, and most crucially, the analysis of the derogations from each of the data protection elements must be combined in order to come up with an overall measure of extent to which the European data protection regime remains applicable even vis-à-vis media expression. As highlighted at the beginning of sub-section 1.2, all of the core elements of EU data protection have the potential to significantly impact the media. Nevertheless, it must be recognised that the three control provisions are mainly designed to perform the subsidiary function of supporting the other data protection elements. Therefore, whilst the control element should not be excluded from the analysis entirely, it would also be wrong to give it the same emphasis as the three primary elements. To reflect this, in drawing up the final measure, the four data protection elements were weighed according to a 3:3:3:1 ratio, the control element being the last category. Clearly, any approach to weighing data protection elements and provisions inevitably reflects value judgments. Nevertheless, it should be emphasised that adopting alternative approaches to combining the results make almost no overall difference.[209] Chart Eleven overleaf summarises these final results for each EEA

[209] To check the stability of the overall result, four models were run, namely (i) the model as outlined, (ii) a model weighing the four data protection elements equally, (ii) a model simply averaging all eighteen data

jurisdiction. This chart usefully highlights evidence of an interesting and striking pattern within Europe. In sum, within a few exceptions, the laws of Eastern and Latin European countries provide little or no formal derogation for the media, whilst Northern European countries tend to grant extensive or even absolute derogations in this area. At the same time, and relatedly, these results strongly confirm the total absence of even a minimal harmonisation or consensus across Europe as a whole.

protection principles, (iv) a model giving double weighting to the data protection rules elements (regarding transparency and sensitive data) and treating the other elements equally. The models resulted in very similar average scores: (i) 0.54, (ii) 0.53, (ii) 0.54 and (iv) 0.51. Moreover, as regards the relative position of the jurisdictions, the alternative models resulted in at most two countries shifting by more than two positions as compared with the model eventually used. These were the Netherlands and Slovenia in the case of (ii), Lithuania and Portugal in the case of (iii) and the Netherlands in the case of (iv).

Chart Eleven: Media Expression and the EU Data Protection Regime



IX. CONCLUSIONS AND REFORM

As the the results of this empirical survey have indicated, within the area of media expression, the formal data protection law within EEA jurisdictions currently display extreme diversity. This is clearly troubling from at least two perspectives - the integrity of the pan-European nature of the regime and the effective realisation of fundamental human rights. Turning to the internal integrity aspect first, the EU Directive is designed to establish a common system of data protection across Europe in which Member States are obliged to neither restrict nor prohibit the free flow of personal data for data protection reasons[210] and, so long as data processing is only taking place within the context of an establishment in another Member State, also to desist from applying their own data protection law to a controller's activities. As Recital 8 of the Directive states, such a system requires that "the level of protection of the rights and freedoms with regard to the processing of such data … be equivalent in all Member States". However, this study has conclusively indicated that once data processing falls within what a Member State defines as media freedom of expression, then evidence of even minimal harmonization, let alone equivalency, proves elusive. What is illegal to collect, store and publish under one country's data protection law is perfectly legal under the data protection law of another. In the context of the exponential growth of new internet services, this hole in the system of harmonization is far from trivial. Thus, although detailed consideration of the scope of media expression is outside the scope of this article, it bears notice that activities as diverse as publication of a vast database of criminal records searchable by name, social security number of geographical location[211] and the rolling out a map service including street-level images of identifiable individuals[212] have been held in some parts of the EEA to fall within the scope of the derogations found within Article 9 of the Directive. Moreover, often it is the Member States with the most substantively lax approach to regulation of such specially protected expression who also adopt the broadest understanding of its scope.[213] In any case, it is also undeniable that even as regards core media activity "data processing is now inseparable from news production".[214] Extreme legislative diversity provides a near blueprint for the evasion of even perfectly legitimate national restrictions. This naturally encourages a wider interpretation of the circumstances where a cross-border data controller will be deemed to be established in multiple Member States. Such a result was exemplified by the decision of national DPAs to subject Google Street View to the data protection laws of each of the Member States in which it was operating.[215] Whilst understandable from the perspective of protecting national regimes, such a fissiparous result

---

[210] Directive 95/46, art 1.1.

[211] Radio Sweden, "Demand for law change after Lexbase launch" (2014) <http://sverigesradio.se/sida/artikel.aspx?programid=2054&artikel=5768451>.

[212] Gräslund, Göran, 'Debatt viktig om grundläggande rättigheter [Debate on important fundamental rights]' DIalog (June 2010) <http://www.datainspektionen.se/Documents/magasindirekt/magasindirekt-10-01.pdf>.

[213] See the data presented in D. Erdos, 'Exploring the Expansive yet Diverse Interpretative Stance of European Data Protection Authorities as regards Freedom of Expression on the "New Media"' (forthcoming) *European Law Review*.

[214] Keller (n 6), 331.

[215] For the full out of such an approach see Electronic Privacy Information Center, Investigations of Google Street View (2010) <http://epic.org/privacy/streetview/>

certainly detracts from the aim of creating a common European data protection space which is "not limited to minimal harmonisation but amounts to harmonisation which is generally complete".[216]

Even more worryingly, many of the outcomes observed clearly fail to do justice to the fundamental rights which are engaged. The European data protection scheme has the self-avowed objective of ensuring that, "with respect to the processing of personal data", "the fundamental rights and freedoms of natural persons, and in particular their right to privacy" are protected.[217] Media processing of personal data can undoubtedly pose a serious threat both to an individual's right to privacy and to a range of other individual rights such as non-discrimination and the right to reputation. The disturbing events concerning the hacking and blagging of private personal data which prompted the setting up in the UK of the Leveson Inquiry into the Culture, Practices and Ethics of the Press in 2011 is but a singular instance of this.[218] Media processing also poses in a particularly acute form a tension between data protection and freedom of expression. Therefore, the essential thrust of the Directive in mandating a "balance between fundamental rights" here is undoubtedly correct.[219] Nevertheless, a large number of Member States have manifestly failed to set out such a balance in statutory law, with outcomes ranging from subjecting the media to entirely inappropriate peremptory rules to completely erasing all individual's substantive data protection rights once they come into conflict with media expression. In democratic societies whose structures are purportedly underpinned by an open discussion on all matters of public concern,[220] it is self-evidently shocking that, irrespective of the public interest engaged, the media might be legally incapable of processing data which falls within broadly defined sensitive information categories unless the data subject himself is deciding to make this public or has explicitly agreed to the processing. Similarly, it is clearly unacceptable that in all circumstances the media might be unable to collect any personal data from the data subject without being explicit about this collection. However, as section 6 and section 5.1 of this article have elucidated, this is respectively the rule which 28% and 19% of the EEA jurisdictions' data protection laws set out. Similarly, given the purposes of the pan-European data protection regime, it cannot be right to exempt the media from any substantive data protection liability irrespective of its impact on the data subject and no matter how unfair their processing of personal data might be. However, that anarchic result is the reality in the data protection laws of Finland, Norway, Sweden and, at least as regards the Press, also Germany.[221]

Since 2012, Europe has been debating a proposal from the European Commission to replace the existing Data Protection Directive with a new General Data Protection Regulation.[222] This was prompted by concern that continuing disparities between Member States had resulted in a "fragmented legal environment which has created legal uncertainty and uneven protection for

---

[216] C-468/10 and C-469/10 *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF)* at [29].
[217] Directive 95/46, art 1.
[218] United Kingdom, Leveson Inquiry, *An Inquiry into the Culture, Practices and Ethics of the Press: Report*, London: Stationary Office (2012).
[219] Directive 95/46, recital 42.
[220] *Thorgeirson v Iceland* (1992) 14 EHRR 843 at [68].
[221] Such a complete exemption remains a demand of many of those lobbying on behalf of the European media. See European Newspaper Publishers' Association, "Newspaper publishers warn of risk to press freedom and distribution in proposed EU Data Protection Regulation" (2013) <http://www.enpa.be/en/news/newspaper-publishers-warn-of-risk-to-press-freedom-and-distribution-in-proposed-eu-data-protection-regulation_109.aspx>.
[222] European Commission, *Proposal for a General Data Protection Regulation*, COM (2012) 11 final.

individuals" and also "unnecessary costs and administrative burdens for businesses".[223] Vice-President Viviane Reding even stressed the need for a "more coordinated approach at EU level" vis-à-vis new 'media' activities such as "online mapping services including pictures of streets and people's homes".[224] Despite this, there is little evidence that this proposal will ameliorate the fragmentation, legal uncertainty and uneven protection which have arisen under Article 9 of the Directive as analysed here. To the contrary, the Commission's suggested replacement of Article 9 which is found in Article 80 of its proposed Regulation adopted even more discretionary language requiring Member States to provide derogations in this area not "only in so far as necessary"[225] but rather simply "in order to reconcile"[226] the fundamental rights engaged. This abandonment of the necessity standard was reversed by the European Parliament's legislative resolution of 12 March 2014 which proposed mandating Member States to provide derogations "whenever it is necessary in order to reconcile the right to the protection of personal data with the rules governing freedom of expression in accordance with the Charter of Fundamental Rights of the European Union".[227] Similarly, the Council has now suggested requiring Member States to provide derogations "if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information".[228] Despite this, there is little reason to think that the simple retention of the necessity standard in the new Regulation, of even the explicit reference to the Charter found in the Parliament text, would make much difference to the extremely fissiparous *status quo*.[229] In contrast to this, in January 2013 the European Commission's High Level Group on Media Freedom and Pluralism did state that, in the light of the evolving nature of the European media landscape, it was "particularly important to adopt minimum harmonization rules covering cross-border media activities on areas such as … data protection".[230] Given the present political climate, however, such

[223] European Commission, *Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century*, COM (2012) 9 final, 7.

[224] Reding, Viviane, 'Privacy matters - Why the EU needs new personal data protection rules [speaking notes]' (2010) <http://europa.eu/rapid/press-release_SPEECH-10-700_en.htm?locale=en>.

[225] Directive 95/46, art 9.

[226] Proposed Regulation (n 222), art 80.

[227] European Parliament, *Legislative Resolution of 12 March 2014 on the Proposal for a General Data Protection Regulation* <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN&ring=A7-2013-0402>. In referring to a general reconciliation between data protection and freedom of expression, the Parliament's wording also clearly expanded the scope of this clause well beyond journalism and similarly special forms of expression. For an analysis of some of the conceptual difficulties of this approach see D Erdos, 'From the Scylla of Restriction to the Charybdis of Licence? Exploring the Scope of the "Special Purposes" Freedom of Expression Shield in European Data Protection' (2015) 52 *Common Market Law Review* 144-151.

[228] Council of the EU, Document 15395/14 (Annex) (19 December 2014), art 80.2 <http://data.consilium.europa.eu/doc/document/ST-15395-2014-INIT/en/pdf>.

[229] In this regard, it should be noted that, during the final reading on the Parliament's Resolution, the Rapporteur on the Regulation Jan Albrecht MEP stated "The existing data protection law already provides for reconciliation of data protection and freedom of expression by the Member States, which is exactly what we ensure in Article 80. Nothing will change for journalists in this regard, and the same is true for other special professions, for example researchers and archivists." European Parliament, *Debates*, 11 March 2014 <http://www.europarl.europa.eu/sides/getDoc.do?type=CRE&reference=20140311&secondRef=ITEM-013&language=EN> . This conservative statement may partly be explained by the strong pressure which media organisations were exerting at this time for a complete and absolute exemption from the Regulation.

[230] European Commission, High Level Group on Media Freedom and Pluralism, *A Free and Pluralistic Media to Sustain European Democracy* (2013) <https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/HLG%20Final%20Report.pdf)>.

a specific, sectoral initiative seems at best a project for the longer-term. Nevertheless, in the light of the findings of this article, it is imperative that any new European data protection framework explicitly lays down in the main body of the text not only that Member States must adopt derogations in their law vis-à-vis media expression but that such derogations not only meet a threshold of necessity but also genuinely provide for an effective and proportionate balancing between fundamental rights in this area. Member States should credibly commit to ensuring that such thresholds are met within their law, an obligation which would be aided by at least informal consultation amongst themselves during the process of transposition. Ultimately, these requirements should be subject to monitoring and, if necessary, enforcement by the European Commission and Court of Justice of the European Union.[231] Action along these lines would go some way to addressing the currently seriously deficient interface between European data protection and journalistic expression. Absent such reform, however, this interface will remain fundamentally out of balance, undermining the development of a common information space, certainty in the law and the secure enjoyment of individual human rights in Europe.

[231] Or in the case of the affiliated EEA members, the EFTA Surveillance Authority and the EFTA Court.

Appendix One: Applicability of EU Data Protection Provisions vis-à-vis Media Expression (cf. Table One)

	A . Data Quality Principles					B. Transparency Rules			C. Sensitive Data Rules							D. Control Conditions			
Jurisdiction	1. Fair & lawful	2. Specific, legitimate & compatible	3. Adequate, relevant & not excessive	4. Accurate	5. Temporal minimization	6. Proactive Direct Transparency	7. Proactive Indirect Transparency	8. Retroactive Transparency	9. Race or ethnic origin	10. Political opinions	11. Beliefs	12. Trade Union Membership	13. Health	14. Sex Life	15. Criminal & Security	16. Legitimating Ground	17. Processing Notification	18. Data Export	Overall Measure
Austria	0.33	0.33	0.33	0.33	0.33	0	0	0	0	0	0	0	0	0	0	0	0	0	0.10
Belgium	1	1	1	1	1	0.17	0.17	0.17	0.67	0.67	0.67	0.67	0.67	0.67	0.67	1	0	0	0.59
Bulgaria	1	1	1	1	1	0.5	0.5	1	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.70
Croatia	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1.00
Cyprus	1	1	1	1	1	0	0	1	0.5	0.5	0.5	0.5	0.5	0.5	0.5	1	1	1	0.65
Czech Republi	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1.00
Denmark	0.17	0.17	0.17	0.17	0.17	0	0	0.17	0.17	0.17	0.17	0.17	0.17	0.17	0.17	0	0.83	0	0.15
Estonia	1	1	1	1	1	0.5	0.5	1	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	1	0.5	0.72
Finland	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.00
France	1	1	1	1	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	1	0.83	0.33	0.53
Germany	0	0	0	0.17	0	0	0	0.17	0	0	0	0	0	0	0	0	0	0	0.03
Gibraltar	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33
Greece	1	1	1	1	1	0.67	0.67	1	0.67	0.67	0.67	0.67	0.67	0.67	0.67	1	1	1	0.84
Hungary	1	1	1	1	1	0.83	1	1	1	1	1	1	1	1	1	1	0	1	0.95
Iceland	0.5	0	0	0.5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.06
Ireland	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0	1	0.34
Italy	0.83	0.83	0.83	0.83	0.83	0.67	0.67	0.83	0.5	0.5	0.5	0.5	0.5	0.67	0.67	0.67	0	0	0.65
Latvia	1	1	1	1	1	0.33	0.33	1	0.33	0.33	0.33	0.33	0.33	0.33	1	0.33	0.83	1	0.67
Liechtenstein	1	1	1	1	1	0.67	1	0.33	1	1	1	1	1	1	1	0.83	0.67	1	0.88
Lithuania	1	1	1	1	1	0	0	0	1	1	1	1	1	1	1	1	0	0	0.63
Luxembourg	1	1	1	1	1	0.33	0.33	0.67	0.67	0.67	0.67	0.67	0.67	0.67	0.67	1	0	0.33	0.68
Malta	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33
Netherlands	1	1	1	1	1	0	0	0	0.17	0.17	0.17	0.17	0.17	0.17	0.17	0	0	0	0.35
Norway	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.00
Poland	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33
Portugal	1	1	1	1	1	0	0	0.67	1	1	1	1	1	1	1	1	1	1	0.77
Romania	1	1	1	1	1	1	0.67	0.83	0.67	0.67	0.67	0.67	0.67	0.67	0.67	0.67	1	0.67	0.83
Slovakia	1	1	1	1	1	1	0.5	1	1	1	1	1	1	1	1	0.5	1	1	0.93
Slovenia	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0.93
Spain	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1.00
Sweden	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.00
UK	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	1	0.33	0.35