UNIVERSITY OF AMSTERDAM

UvA-DARE (Digital Academic Repository)

Getting Data Subject Rights Right

A submission to the European Data Protection Board from international data rights academics, to inform regulatory guidance

Ausloos, J.; Veale, M.; Mahieu, R.

Publication date
2019

Document Version
Final published version

Published in
Journal of Intellectual Property, Information Technology and Electronic Commerce Law

License
Other

Link to publication

Citation for published version (APA):
Ausloos, J., Veale, M., & Mahieu, R. (2019). Getting Data Subject Rights Right: A submission to the European Data Protection Board from international data rights academics, to inform regulatory guidance. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, *10*(3), 283-309. https://www.jipitec.eu/issues/jipitec-10-3-2019/5031

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: https://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, P.O. Box 19185, 1000 GD Amsterdam, The Netherlands. You will be contacted as soon as possible.

UvA-DARE is a service provided by the library of the University of Amsterdam (https://dare.uva.nl)

Download date:08 9月 2026

Getting Data Subject Rights Right

A submission to the European Data Protection Board from international data rights academics, to inform regulatory guidance

by **Jef Ausloos, Michael Veale and René Mahieu**

© 2019 Jef Ausloos, Michael Veale and René Mahieu

Everybody may disseminate this article by electronic means and make it available for download under the terms and conditions of the Digital Peer Publishing Licence (DPPL). A copy of the license text may be obtained at http://nbn-resolving.de/urn:nbn:de:0009-dppl-v3-en8.

Recommended citation: Jef Ausloos, Michael Veale and René Mahieu, Getting Data Subject Rights Right, 10 (2019) JIPITEC 283 para 1.

Summary

We are a group of academics active in research and practice around data rights. We believe that the European Data Protection Board (EDPB) guidance on data rights currently under development is an important point to resolve a variety of tensions and grey areas which, if left unaddressed, may significantly undermine the fundamental right to data protection. All of us were present at the recent stakeholder event on data rights in Brussels on 4 November 2019, and it is in the context and spirit of stakeholder engagement that we have created this document to explore and provide recommendations and examples in this area. This document is based on comprehensive empirical evidence as well as CJEU case law, EDPB (and, previously, Article 29 Working Party) guidance and extensive scientific research into the scope, rationale, effects and general modalities of data rights.

A. Main Takeaways

1 The first half of this document lists recommendations for the four data subject rights mentioned in the EDPB's plan to draft guidelines: right of access (Article 15); right to rectification (Article 16); right to erasure (Article 17); and the right to restriction of processing (Article 18). The second half of this document takes a step back and makes recommendations on the broader issues surrounding the accommodation of data subject rights in general.We strongly advise the EDPB to consider the following points in its Guidance:

2 The interpretation and accommodation of data subject rights should follow established CJEU case law requiring an '**effective and complete protection** of the fundamental rights and freedoms' of data subjects and the '**efficient and timely protection**' of their rights.

3 The **right of access** plays a pivotal role in enabling other data rights, monitoring compliance and guaranteeing due process. Analysis of guidance, cases, and legal provisions indicates data controllers cannot constrain the right of access through unfair file format, scope limitations, boiler-plate response, and that where data sets are complex, they should facilitate tools to enable understanding.

4 The **right to erasure** is not accommodated by anonymising personal data sets. In case the same personal data is processed for different processing purposes some of which may not be subject to the right to erasure, data controllers should interpret erasure requests as a clear signal to stop all other processing purposes that are not exempted.

5 The **right to object** offers a context-dependent and individualised re-assessment of the relevant processing purposes, specifically in relation to the data subject's concrete situation. Data controllers' potential compelling legitimate interests should be detailed, publicly declared and foreseeable, in order to be able to override data subjects' clear desire to stop the respective processing operation.

6 The **right to restriction of processing** — currently ignored by most data controllers — should be prioritised in time and effectively 'freeze' any further processing operations. Information society services should offer this through an interface.

7 The **right to rectification** applies to opinions and inferences of the data controller, including profiling, and must consider that the vast majority of data is highly subjective.

8 (Joint) controllers have an **explicit duty to facilitate the exercise of data subject rights** and cannot require specific forms or legislative wording as a precondition for accommodating them.

9 **Restrictions or limitations** on how data rights are accommodated (eg rights and freedoms of others, excessiveness, repetitiveness) need to be foreseeable and interpreted narrowly and specifically in light of the concrete and specific right, data subject and context at hand.

B. Background

10 Data subject rights are of critical importance in the European data protection regime. Throughout all discussions of their scope and limits, it must be recalled that rights are not simply a way to police that sufficient data protection is occurring, but they are an intrinsic part of the fundamental right to data protection enshrined in the Charter of Fundamental rights, which states that:

> *Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*[1]

11 Data rights must, in general, be implemented with several observations of the Court of Justice of the European Union in mind.[2] The Court has held that one of the key objectives of data protection law is the **effective and complete protection** of the fundamental rights and freedoms of natural persons with respect to the processing of personal data.[3]

12 We can see this principle in operation in relation to data rights which are prerequisites to others. The Court held that the right of access is a pre-requisite to the 'rectification, erasure or blocking' of data, and thus the existence (and extent) of the right of access must allow effective use of other data rights.[4]

13 The Court has also held that provisions of data protection law must be interpreted as to give effect to the **efficient and timely protection** of the data subject's rights.[5] Furthermore, it is critical to consider data rights in light of the overarching principles of **transparency and fairness** in the GDPR. Data controllers are not permitted to frustrate data subjects in their attempts to benefit from the high level of protection that follows from their fundamental rights. Indeed, they have to both implement data rights[6] as well as facilitate the exercise of such rights.[7]

14 Relatedly, the Court has also highlighted that data protection should be understood within the framework of the **responsibilities, powers and capabilities** of a data controller.[8] As the European Data Protection Board has already pointed out, 'information society or similar online services that specialise in automated processing of personal data' are highly capable at classifying, transmitting and managing personal data in automated ways, and as a result[9] meet data rights in an effective, complete, efficient, and timely manner.

15 Finally, the Court has also linked the ability to effectively exercise data subject rights with the **fundamental right to effective judicial protection** in Article 47 Charter. Specifically, it stressed that 'legislation not providing for any possibility for an

1 Charter, art 8(2).

2 We refer to the Court of Justice as the *Court* in the remainder of this article.

3 Case C-131/12 *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* EU:C:2014:317 [53]; Case C-73/16 *Peter Puškár v Finančné riaditeľstvo Slovenskej republiky and Kriminálny úrad finančnej správy* EU:C:2017:725 [38].

4 Case C434/16 *Peter Nowak v Data Protection Commissioner* EU:C:2017:994 [57]; Case C-553/07 *College van burgemeester en wethouders van Rotterdam v MEE Rijkeboer* EU:C:2009:293 [51].

5 Case C-49/17 *Fashion ID GmbH & CoKG v Verbraucherzentrale NRW eV* EU:C:2019:629 [102].

6 GDPR, art 25 ('Data protection by design and by default').

7 GDPR, art 12(2).

8 *Google Spain* (n 3) [38]; Case C136/17 *GC and Others v Commission nationale de l'informatique et des libertés (CNIL)* EU:C:2019:773 [37].

9 Article 29 Working Party, 'Guidelines on the Right to Data Portability (WP 242)' (13 December 2016) 12.

individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter.'[10] Technical and organisational arrangements, and arrangements of controllership, must be understood in light of this Article 47 obligation.

C. The Right of Access (Article 15)

16 The right of access has been integral to data protection laws since the very early days. It was already positioned as 'an essential minimum element in the protection of privacy' in two Council of Europe resolutions from the early 1970s.[11] The right of access is also explicitly recognised in international data protection instruments such as the OECD's 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,[12] and the Council of Europe's 1981 Convention.[13] Importantly, the OECD guidelines stress that data subjects have a right to have their personal data communicated to them (a) within a reasonable time; (b) at no (excessive) charge; (c) in a reasonable manner; and (d) in a readily intelligible form.

17 The right of access constitutes a cornerstone in achieving the effective and complete protection of the fundamental rights and freedoms of natural persons with respect to the processing of personal data. Firstly, this right can, in principle, be considered as **a *sine qua non* for meaningfully exercising other data subject rights** in Chapter III of the GDPR. More specifically, data subjects will only be able to properly consider whether to invoke their right to rectification (Article 16), erasure (Article 17), portability (Article 20) when they know what personal data is processed exactly, for what purposes, whom it was shared with, and so on. The 'enabling role' of the right of access was also repeatedly confirmed by the Court.[14] In effect, this means that any restrictions or conditions placed on or around the right to access have a knock-on effect on the entire data protection regime.

18 Secondly, the right of access is an important tool that private individuals can use **to monitor controllers' compliance** with the general principles governing the processing of personal data, notably Articles 5-6 of the GDPR. Compliance with core provisions of the regulation, such as purpose limitation, data minimisation, accuracy and storage limitation principles[15] will be easier to verify after obtaining access. This monitoring role of the right of access is explicitly recognised in recital 63 of the GDPR, which emphasises that

> *"a data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing."*

As such, the right of access effectively complements the data protection authorities mandate to monitor and enforce the application of the GDPR (Article 57(1) a), by enabling a broader number of stakeholders to verify GDPR compliance. Max Schrems' actions against Facebook provide a useful illustration of the effectiveness of this remedial function. After filing an access request with the company, Schrems received an enormous PDF file (including data thought to previously have been erased) and initiated proceedings before the Irish DPA. Among others, this access request served as a catalyst which eventually led the CJEU to invalidate the *Safe Harbour* decision.[16] This role is especially important given the under-resourced and over-burdened sate of many supervisory authorities.[17] It needs to be

10 Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* EU:C:2015:650 [95].

11 Council of Europe - Committee of Ministers, 'Resolution (73) 22 on the Protection of the Privacy of Individuals Vis-à-Vis Electronic Data Banks in the Private Sector' (26 September 1973); Council of Europe - Committee of Ministers, 'Resolution (74) 29 on the Protection of the Privacy of Individuals Vis-a-Vis Electronic Data Banks in the Public Sector' (20 September 1974).

12 OECD, Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013) [C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79], principle 13 on Individual Participation.

13 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (opened for signature 28 January 1981, entered into force 1 October 1985) 108 ETS, art 8. The convention was modernised in 2018 (Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (opened for signature 10 October 2018) 228 CETS) and the relevant provision can now be found in Article 9.

14 *Rijkeboer* (n 4) [51]; *Nowak* (n 4) [57].

15 GDPR, arts 5(1)(b–e).

16 *Schrems I* (n 10).

17 See generally European Data Protection Board, 'First Overview on the Implementation of the GDPR and the Roles and Means of the National Supervisory Authorities' (Report presented to the European Parliament's Civil Liberties, Justice and Home Affairs Committee (LIBE), 26 February 2019).

stressed however, that well-resourced supervisory authorities are key to the effective functioning of data rights.

19 The importance of the right of access is not restricted to those purposes explicitly mentioned in the recitals.[18] For example, the right of access also functions as a **due process** guarantee. Personal data is often collected to serve as input for making decisions about people. Such decisions range from which advertisement is shown, whether and under which conditions a loan is given, to whether one qualifies for social security. The right of access to personal data is historically also predicated on the idea that people should be empowered and able to assess and contest decisions made about them.[19] It is a response to these decisions being based on increasing collection and digitalisation of data relating to individuals.

I. Data Format of Access Requests

20 The format of data provided pursuant to the right of access is very important for the effective use of the right by the data subject. It should be considered that data subjects who exercise their rights have different legitimate reasons for doing so and that they have different backgrounds and capabilities. It follows that the data format which is most appropriate to these different situations must vary accordingly. We therefore recommend that **the layered approach** advocated by the A29WP in the context of privacy statements/notices,[20] should equally apply to information provided through Article 15 access requests. Following this insight, we analyse first (in the remainder of 3.1) the limits of relying on PDFs to provide access, the need to provide access to all data, and the benefits of doing so in a machine readable format; and second (in 3.2) why the complexity of data processing should not be accepted as an argument to limit the access to all data, but rather to put an obligation on the data controller to provide the conditions necessary to render the complex data intelligible.

21 In older data systems, where the number of points on any given individual was considerably smaller than it often is today, a simple print-out or summary would suffice to give the data subject oversight as to the content of the data undergoing processing.[21] **Today, however, many data systems collect such a large number of data points, that only a format that allows the data subject to analyse data themselves will allow them to have sufficient oversight over the data processing being undertaken**.

22 Firstly, it can and should be understood as part of the principle of fairness that a data controller should not transform data from the machine-readable format they hold it in[22] into a format that makes it more difficult for the data subject to navigate. Information society services *can only analyse the data they hold about individuals by virtue of its machine-readable nature*. To refuse individuals the same ability exacerbates the informational and power asymmetries that the right of access, and the fundamental right of data protection in general, seeks to rebalance.

23 **In particular, data controllers should not transform data from common machine-readable formats (eg JSON, CSV) into PDF formats.** Portable document format, or 'PDF', is a file *designed for printing, not for analysis*. The A29WP recognised this in their guidance on the right to portability, stating that

> *As an example, providing an individual with .pdf versions of an email inbox would not be sufficiently structured. E-mail data must be provided in a format which preserves all the meta-data, to allow the effective re-use of the data. As such, when selecting a data format in which to provide the personal*

18 Case C434/16 *Peter Nowak v Data Protection Commissioner* EU:C:2017:582, Opinion of AG Kokott [39].

19 See Alan F Westin and Michael A Baker, *Databanks in a Free and Fair Society* (Quadrangle Books 1972), which argues for the introduction of the right of access based on due process argument, and which was very influential on the development of data protection law, also in Europe.

20 Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (11 April 2018) 19–20.

21 This is not to say that many systems have not been considerably complex in relation to subject access rights for many decades, see eg Graham Greenleaf and Roger Clarke, 'Database Retrieval Technology and Subject Access Principles' (1984) 16 The Australian Computer Journal.

22 In its Guidelines on Transparency, the A29WP (Article 29 Working Party, 'Guidelines on transparency under Regulation 2016/679' (n 20) 25) refers to Recital 21 of Directive 2013/37/EU for a definition: 'A document should be considered to be in a machine-readable format if it is in a file format that is structured in such a way that software applications can easily identify, recognise and extract specific data from it. Data encoded in files that are structured in a machine-readable format are machine-readable data. Machine-readable formats can be open or proprietary; they can be formal standards or not. Documents encoded in a file format that limits automatic processing, because the data cannot, or cannot easily, be extracted from them, should not be considered to be in a machine-readable format. Member States should where appropriate encourage the use of open, machine-readable formats.'

data, the data controller should consider how this format would impact or hinder the individual's right to re-use the data.[23]

24 Because PDFs are designed for printing, they are notoriously difficult to extract data from — so much so, that table extraction from PDFs is an *academic area of study*, which researchers even deploy neural networks and deep learning for in an attempt to solve.[24] Transforming data into PDFs unwantedly **only disadvantages the data subject** and forecloses analysis opportunities. Even formats such as HTML, ODF, ODT, XLSX or DOCX are more reusable and can be parsed by machines.

25 Furthermore, **PDFs score extremely poorly for individuals who need accessible information online**. Individuals who require or are assisted by accessible information include those with cognitive disabilities, those with vision impairments, those with physical disabilities and those with hearing impairments.[25] A study of 100 blind screen-reader users found that inaccessible PDFs were one of the main causes of frustration while browsing the Web.[26] Accessible PDFs in practice are rarely found, are difficult to create and often require consultants and in-depth planning and expert knowledge.[27] In general **PDFs are not tools that lends themselves to accessibility across the population**.[28] In the authors' experience, many data controllers provide screenshots of databases as visible to their support staff — a format which is both unable to be re-used by the data subject, and totally inaccessible to visually impaired users. The guidance should be very clear that screenshots in general are not an appropriate manner of providing access rights for services which rely heavily on the automatic processing of personal data, such as information society services.

26 The common practice of limiting access to the data that is visible through the interfaces, which is available to support staff has other limiting implications for the right of access. First, not all the personal data processed in a system may be visible through the interface used for day-to-day operations. Second, support staff may only have access to a subset of all the systems in which personal data is processed**. Just because personal data is not used in a day-to-day business practice by frontline workers, it is not an appropriate reason to exclude it from access.** If data is held, it falls within the scope of the right to access.

27 A specific area of concern in this regard is 'deleted' data. In many common implementations of database software, the processing operation that is commonly referred to as 'deleting' merely changes a label attached to a data-point. For example, an individual may have pressed a 'delete' button on a social media post, or an old address may seem 'deleted' when overwritten with a new address, but that does not necessarily mean associated data is deleted from the controller's servers. While this practice may, depending on the circumstances, be appropriate, it is important to stress that such data still exists in the system, and therefore falls under the reach of the right of access to personal data. On websites and apps today, this data may have even been typed and then deleted (without ever having pressed 'submit' or 'send'), or only partially uploaded (from the user's point of view), yet still retained by the data controller.[29]

23 Article 29 Working Party, 'Guidelines on the right to data portability (WP 242)' (n 9) 14.

24 See generally Shah Khusro and others, 'On Methods and Tools of Table Detection, Extraction and Annotation in PDF Documents' (2015) 41 Journal of Information Science 41. For a recent example of a neural network powered PDF parsing tool, see L Hao and others, 'A Table Detection Method for PDF Documents Based on Convolutional Neural Networks' (April 2016) 2016 12th IAPR Workshop on Document Analysis Systems (DAS) 287.

25 cf Gian Wild and Daniel Craddock, 'Are PDFs an Accessible Solution?' in *Computers Helping People with Special Needs* (Lecture Notes in Computer Science, Klaus Miesenberger and others eds, Springer International Publishing 2016) 355.

26 Jonathan Lazar and others, 'What Frustrates Screen Reader Users on the Web: A Study of 100 Blind Users' (2007) 22 International Journal of Human–Computer Interaction 247.

27 Erin Brady and others, 'Creating Accessible PDFs for Conference Proceedings' in *Proceedings of the 12th Web for All Conference* (W4A '15, New York, NY, USA, ACM 2015).

28 ibid.

29 Drew Harwell, 'Start a Post, Then Delete It? Many Websites Save It Anyway.', Washington Post (18 December 2018) <https://www.washingtonpost.com/technology/2018/12/18/start-post-then-delete-it-many-websites-save-it-anyway/> accessed 17 November 2019; Tony Romm, 'Facebook Says a New Bug Allowed Apps to Access Private Photos of up to 6.8 Million Users', Washington Post (14 December 2018) <https://www.washingtonpost.com/technology/2018/12/14/facebook-says-new-bug-allowed-apps-access-private-photos-up-million-users/> accessed 17 November 2019; Steven Englehardt and others, 'No Boundaries: Exfiltration of Personal Data by Session-Replay Scripts' (Freedom to Tinker, Centre for Information Technology Policy, Princeton University, 15 November 2017) <https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/> accessed 17 November 2019.

A social network is asked for to provide a copy of all data held about an individual, which includes posts, lists of friends, advertising interests and the history of log-ins to the site. Because all of this data is processed automatically by the social network, and readily available to the social network in a machine readable format, the social network is obliged not to render it less machine readable or accessible to individuals with visual impairments by placing it into a PDF file or a similar format complicating machine readability, such as an image or screenshot.

Proposed Example

II. Rendering 'Raw', Necessarily Complex Data Intelligible

28 Often, data is necessarily complex. Datasets include, for example, those which record varied data subject activity over time, such as their interaction with information society services. Such interactions may not be classed within a single variable (eg clicked, played, watched) but may consist of multiple bundled and nested variables, some with multiple values.

29 **Complexity of data should not be a reason not to provide the 'raw', maximally complex, data upon request.** However, it may be a reason to develop a layered approach for individuals who may not be able to parse the dataset.

30 In many cases, raw data will likely be represented within the data controller in a flexible format such as JSON. A JSON file is simply a way of arranging a text file in a human-readable, yet machine-parseable, way as to describe a flexible data object. For example, the below is an entry from John Smith, which contains some biographical information about John.


```
{
 "firstName": "John",
 "lastName": "Smith",
 "age": 27,
 "phoneNumbers": [
  {
   "type": "home",
   "number": "212 555-1234"
  },
  {
   "type": "mobile",
   "number": "123 456-7890"
  }
 ],
 "children": [],
 "spouse": null
}
```


Example of a JSON file extract

31 Observe that, for example, in a JSON a nested structure is present: more than one telephone number is provided, and if John Smith had children, these children could be a similar data record to John's own, nested in the 'children' key. **This format is not tabular, and to convert it to tabular data would generally lose information.** This is because each record might have different 'keys' (think columns in a table), and a different number of values for each key (think cells).

32 To illustrate the policy challenges, and guidance requirements, of datasets such as those in JSON format, we will provide a truncated extract from an access request to a popular music service and data controller, *Spotify*. Spotify provided telemetry data to one of the authors in mid-2018 on the basis of a data access right. The telemetry data Spotify held from the previous six months alone amounted to 845 megabytes of plain text files (TXT files in JSON structure). The following entry appears to relate to the adding of a single song ('No Man is Big Enough for My Arms' by *Ibeyi*) to a playlist. The actual entry for this single action was 171 lines long, only 66 illustrative lines are reproduced here.


```
{
    "pid": {
      "description": "",
      "value": "1217"
    },
    "time": {
      "description": "",
      "value": "1525786006.15"
    },
    "message": {
      "item_uri": {
        "description": "URI of item that was added and only the first if multiple.",
        "value": "spotify:track:3nPOISgqtO1hl7nNxAZi7K"
      },
      "source": {
        "description": "The view uri which led to add to playlist.",
        "value": "\u0003\u0001\u0000\u0001\ufffdDd\ufffdo\ufffd\ufffd\u0012\ufffdt'\
          ufffd\u0006Ey\ufffd\ufffd\ufffd\ufffd\ufffd\ufffd\u000f}\ufffd\u001bLi\u0012\
        ufffdO\u0019\ufffdp\ufffd\ufffd\ufffd\ufffd4\ufffd\ufffddX\u0002\ufffd\ufffd\
          ufffd`"
      },
      "message_version": {
        "description": "",
        "value": "4"
      },
      "playlist_uri": {
        "description": "The uri of playlist added to or null.",
        "value": "\u0003\u0001\u0000\u0001O\ufffd/&\ufffdE.\ufffd@\ufffd\
u001a\ufffd\ufffd\ufffd\ufffd\ufffd\"\ufffd\ufffd\u0005\u0014f\ufffd\ufffd\ufffd5f\
```

ufffd\ufffd\ufffd\ufffd\ufffd\ufffd\ufffd\ufffd\ufffd\ufffd\u001c\u0011\ufffdY[\ufffd\

ufffd\ufffd\ufffd\u0011\ufffdn<\u007fN\ufffdb\ufffd\u0015\ufffd\u0017Y\ufffd'p\

ufffd\ufffd\ufffd\r2"

},

"time": {

"description": "Unix timestamp",

"value": "1525786006"

},

"number_items": {

"description": "Number of items added.",

"value": "1"

},

"context_source": {

"description": "URI representing action context source",

"value":

"\u0003\u0001\u0000\u0001\ufffd\u0003\ufffd\ufffd\ufffd\ufffd\ufffd\ufffd\u000e\

u0013\ufffd|\ufffd\ufffd\ufffdP\ufffd>\ufffd:\ufffd2\ufffd\ufffd~?\ufffd\ufffd2\ufffd\

u0007\ufffd\u0012,'&\ufffd\ufffdMM}\ufffd\ufffdOP\ufffd\ufffd\ufffd\ufffdc\ufffdV\f\

ufffd:\ufffd\ufffd\r\ufffdY*\ufffdN\ufffd\ufffd\tU"

}

},

"rid": {

"description": "",

"value": "7795720745"

},

"identData": {

"ip_addr": {

"description": "public IP address of the connected node",

"value":

"\u0003\b\u0000\u0001\ufffd\ufffdw\ufffd\ufffd\ufffdZWI\ufffd\ufffd\ufffd\

ufffd^u\ufffd\ufffd*\ufffd:\ufffd\ufffd\ufffd\ufffd\ufffdv\ufffd\ufffd\ufffdx\ufffd\

ufffd?{\ufffd\u0006\ufffd\ufffd"

},

"conn_country": {

"description": "the country looked up with GeoIP by the AP",

"value": "GB"

},

"tcp_port": {

"description": "public TCP port of the connected node",

"value": "59918"

},

"platform": {

"description": "platform of the connected node",

"value": "iOS 11.3 (iPhone9,1)"

},

"version": {

"description": "",

"value": "10"

},

}

}

Extract from the Spotify Telemetry Data provided to one of the authors

33 Some of this data comes with a relatively clear description, such as:

- the country chosen by the user at registration time ('GB')
- Number of items added ('1')
- platform of the connected node ('iOS 11.3 (iPhone9,1)')

34 Other data are less clear or completely opaque, such as:

- client revision number ('845100696')
- connection ID assigned by the AP ('28539029148205306')
- rid ('7795720745')

35 Some data is technically obfuscated. For example:

- public IP address of the connected node ('\u0003\b\u0000\u0001\ufffd\ufffdw\ufffd\ufffd\ufffdZWI\ufffd\ufffd\ufffd\ufffd^u\ufffd\ufffd*\ufffd:\ufffd\ufffd\ufffd\ufffd\ufffdv\ufffd\ufffd\ufffdx\ufffd\ufffd?{\ufffd\u0006\ufffd\ufffd')

- URI representing action context source ('\u0003\u0001\u0000\u0001\ufffd\u0003\ufffd\ufffd\ufffd\ufffd\ufffd\ufffd\u000e\u0013\ufffd|\ufffd\ufffd\ufffdP\ufffd>\ufffd:\ufffd2\ufffd\ufffd~?\ufffd\ufffd2\ufffd\u0007\ufffd\u0012,'&\ufffd\ufffdMM}\ufffd\ufffdOP\ufffd\ufffd\ufffd\ufffdc\ufffdV\f\ufffd:\ufffd\ufffd\r\ufffdY*\ufffdN\ufffd\ufffd\tU')

36 Both of these variables are among several in the text which are filled with 'escaped' Unicode characters with no clear representation (eg '\ufffd'). Even when these are removed, we could not understand the meaning of these sequences. If there is a decoding mechanism for these variables, it was not provided to the data subject. The specific song that was added was only accessible through the Spotify identifier, which can be resolved manually through the Spotify App, and requires further interaction with the service (and, of course, further data collection on this interaction by Spotify).

37 Whereas it is important for data controllers to be able to provide *all* personal data they have on a data subject in raw format, it is equally important that they ensure data subjects can easily access and understand such data (Article 12(1)). This is particularly important with regard to data controllers of complex data-ecosystems as illustrated above. We therefore recommend the EDPB to stress that **accommodating the right of access should – where needed – include the tools rendering the entire data-set understandable.** Put differently, the layered approach heavily advocated by the A29WP in the context of privacy statements/notices,[30] equally applies to subject specific information provided through Article 15 access requests.

30 Article 29 Working Party, 'Guidelines on transparency under Regulation 2016/679' (n 20) 19–20.

38 In some cases, the risk of processing, and the requirement for the data controller to facilitate rights and design data protection into processing systems, may require a bespoke exploration interface to be designed for such complex datasets. However, particularly if the guidance determines that some data controllers would not be required to create such tools, **it is key that they release data in a format which allows such tools to be made by third parties**. This requires, for example, that the datasets (such as the Spotify example above) are **stable** in their format (so that analysis tools made by civil society do not break), **well-documented** (so that faithful analysis tools can be created), and **not contingent on hidden datasets for understanding** (such as reference dataset linking song names to identifiers).

III. Opinions and Inferences

39 The fact that opinions and inferences can qualify as personal data has been confirmed by the CJEU, which noted that the term 'any information' in the definition of personal data includes information that is 'not only objective but also subjective, in the form of opinions and assessments, provided that it 'relates' to the data subject'.[31] The test of whether data 'relates' to an individual is satisfied where it is linked to a person 'by reason of its content, purpose or effect'.[32]

40 Access to opinions about individuals can become contentious in cases where those opinions are expressed in a professional context by third parties, such as written or oral evidence provided as part of a human resources dispute, yet recorded on a file about individuals. In those cases, it is an instance of 'mixed personal data' and should be navigated as such. This is dealt with later in this document.[33]

41 **Opinions or inferences formed of the data subject by the data controller, however, should not merit a similar exemption**. In practice, these inferences can range from a quantitative or 'predictive' assessment of employment performance using manual or automated surveillance tools[34] to profiling of data subjects by information society services.[35] Access to these opinions and inferences is key to a variety of other rights and obligations in the GDPR, such as rectification, objection, erasure, as well as the broad assessment of fairness and non-discrimination.[36] **Access rights are pre-requisites to so many other potentially applicable rights and checks, that providing them is key to effective oversight and the principle of transparency**.

42 It is worth noting that **two recent relevant CJEU cases, *YS and Others*[37] and *Nowak*,[38] do not clearly map onto issues of access to inferences in the digital economy**. Because both concern the Data Protection Directive, they do not distinguish *profiling* from other forms of opinion-forming. In particular, recital 72 of the GDPR emphasises that:

> *Profiling is subject to the rules of this Regulation governing the processing of personal data, such as the legal grounds for processing or data protection principles.*[39]

Profiling is defined as:

> *any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*[40]

43 Profiling is seen as an activity which increases the risk of data processing to data subjects rights and freedoms, indicated by, for example, significant decisions based (even in non-solely automated ways) on profiling triggering the requirement for a data protection impact assessment.[41] The A29WP, in guidance endorsed by the EPDB, list '[e]valuation or scoring, including profiling and predicting' as a criterion for the determination of high-risk processing.[42]

31 *Nowak* (n 4) [34].

32 ibid [35].

33 See section 3.4.

34 See generally Ifeoma Ajunwa and others, 'Limitless Worker Surveillance' (2017) 105 Calif L Rev 735; Lilian Edwards and others, 'Employee Surveillance: The Road to Surveillance is Paved with Good Intentions' (SSRN Scholarly Paper, 18 August 2018).

35 See generally Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking For' (2017) 16 Duke Law & Technology Review 18.

36 GDPR, recital 71.

37 Joined Cases C141/12 and C372/12 *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S* EU:C:2014:2081.

38 *Nowak* (n 4).

39 GDPR, recital 72.

40 GDPR, art 4(4).

41 GDPR, art 35(3)(a).

42 Article 29 Working Party, 'Guidelines on Data Protection

44 Neither *Nowak* or *YS and Others* can be easily construed as profiling, as both were cases of manual, rather than automated, processing. Legal analysis of the type in *YS and Others* would not fall under the profiling definition. It also seems doubtful that a traditional examination, such as that in *Nowak*, would fall under the concept of profiling (unless it was marked automatically). Consequently, we have not seen the Court provide judgements clearly analogous to profiling. Profiling is therefore a distinct activity which distinguishes many inferences and opinions made in the context of the digital economy from existing case-law: it is a situation where risk is heightened and the need to provide strong data protection is also heightened.

45 Furthermore, when executing an access right, where inference is a human understandable score or category, **context must be provided as to the alternatives that the individual could have been categorised as**. This is important for rights such as rectification where they apply in this context, or assessing whether such categorisations are potentially discriminatory, as without this knowledge, they would not know the alternative options available.

46 The EDPB should, however, be aware that a particular challenge exists in practice as **many data controllers do not explicitly infer human-understandable data about the data subject, but infer data which is used to shape and sort them, which only machines can 'understand'**. For example, a common tool in this area is the 'embedding', where data records are plotted as 'points' in such a way that the distance between them is an indicator of their similarity or dissimilarity to each other. This is a common practice in advertising and recommender systems.[43]

47 An embedding is a simple but important technology. Imagine 10,000 users, and each has 10 characteristics which are known about them, such as their age, location, and so on. This is a 10,000 x 10 table. An embedding turns these users into **vectors of geometric points**. Many methods, including neural networks, are possible to do this. The end product is a table with 10,000 rows, but with, for example, three columns instead, each of which contains a number between -1 and 1. It would be possible to plot these 10,000 points on a 3D scatter plot, and the idea is that 'similar' users are clustered together. In practice, the number of dimensions is much larger — often thousands — but the concept is the same. In 1000D space, rather than 3D space, many more nuanced characteristics can be caught: for example, on some dimensions, users might be clustered in practice by language, while in others, they might be clustered by ethnicity, and in others, by interests. Yet each column is not a clear variable such as this: it is the emergent property of 'similarity' which is important, and therefore the columns are not interpretable without the rows to understand what the clusters mean in practice.

48 In embedding systems, how individuals are being profiled, and the opinions formed about them, are **not in some human-readable inference**, but are instead based on their **proximity and similarity to others**.[44] The Guidance must address how individuals can access the way they are being profiled in such systems. In particular, it must be emphasised that **this is a dataset of personal data, not an automated decision system** as per GDPR Article 22.

Each individual is attached to a record of hundreds or thousands of data points that place them in relation to other individuals, and which has been calculated in advance, ready for use at a later stage. The automated system is simply looking at the distance between the co-ordinates of one individual and another, and that would be the 'logic' of the processing. **The data points are not the logic of processing, and therefore the data points fall wholly within the right of access**.

49 In particular, it is concerning that data controllers are seeking to use complex processing, such as embeddings, in order to practically render access rights unhelpful in understanding the ways individuals are being profiled, and opinions formed against them.

Impact Assessment (DPIA) and Determining Whether Processing is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679 (WP 248 Rev.01)' (4 October 2017) 9.

43 See for example the description of the system used by Pinterest at Stephanie deWet and Jiafan Ou, 'Finding Users Who Act Alike: Transfer Learning for Expanding Advertiser Audiences' in *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining* (KDD '19, New York, NY, USA, ACM 2019).

44 See further Solon Barocas and Karen Levy, 'Privacy Dependencies' [2019] Washington Law Review.

A social network uses vector embeddings to assess the similarity between two data subjects. These embeddings are stored alongside a user ID. According to the layered approach, the entire vector for that user should be provided (so that the data subject can compare to other data subjects if they wish) regardless of what the controller believes the utility of this to the data subject to be, but also, a system to help users understand what these embeddings mean for them, such as the nature of the other individuals they are clustered near, should be provided.

Proposed Example

A political party has categorised a data subject as a 'Pragmatic Liberal' using a machine learning classifier. In the access request, the data controller lists all possible other classifications for this individual, so that the data subject understands this opinion within its context.

Proposed Example

IV. Mixed Personal Data' Should Only Justify Refusal in Limited Cases

50 Much personal data relate to more than one person. This includes, for example, data such as:

- reputation systems, where a rating relates to the rated and the rater;
- ambiently collected data, such as from sensors or 'smart speakers';
- message data, which relates to the sender and recipient, and may also mention and relate to third parties;
- data as part of a professional duty or relationship, such as notes taken by a medical professional about a patient.

51 This data often causes challenges when the right of access is invoked.It is important to note that significant case-law in this area exists from the European Court of Human Rights, which has, in general, favoured the individual seeking access to data over third parties seeking to limit its release. In *Gaskin*, the ECtHR ruled that just because no consent had been obtained from all third parties in the data, it did not mean that it could not be released, and that there was a need for an independent authority to exist to make the final call; otherwise there would have been a breach of Article 8 of the Convention.[45] In *Társaság a Szabadságjogokért v Hungary*, the claim by a member of parliament that a complaint submitted to the Constitutional Court could not be subject to a document release request by an NGO because it included personal data was in violation of Article 10 of the Convention, on the grounds that individuals in public life should not be able to stop the genuine disclosure of documents on the basis that their opinions on public matters constituted private data which could not be disclosed without consent.[46]

52 In the UK, the Court of Appeal has ruled that even where a third party has refused to consent to data released on the basis of an access request, that does not mean there is a rebuttable presumption against release, but that the case should be balanced on importance and merits.[47]

The Information Commissioner also counsels in this direction, stating that:

> *depending on the significance of the information to the requester, it may be appropriate to disclose it even where the third party has withheld consent.*[48]

53 Furthermore, the focus on the above is that the **data controller should seek consent from third parties in an access request**. A data controller should not have a blanket policy to refuse to seek such consent. For an information society service, where such a process can be easily automated, that is especially true.

A data subject requests the rating information from individuals on a ratings platform. The data controller retains such data. The data controller has an obligation to ask the relevant raters for consent to release this data, rather than refuse the data subject access to this data. The controller then must assess, with reference to the significance of the information to the requester, whether this data should be released. Such an assessment must not be a blanket policy, but must co#nsider individual circumstances.

Proposed Example

V. Access to Sources and Recipients of the Data

54 While discussion of the right of access mostly focuses on the right to access the data itself, it is important to stress that the right, on the basis of

45 *Gaskin v United Kingdom* [1990] EHRR 36.

46 *Társaság a Szabadságjogokért v Hungary* App no 37374/05 (2009).

47 *DB v General Medical Council* [2018] EWCA Civ 1497 [70].

48 Information Commissioner's Office, 'Subject Access Code of Practice' (9 June 2017) 40.

Article 15(1)(a–f) also encompasses the obligation on data controllers to provide additional information regarding the processing of data. Of particular importance in relation to the data subject's ability to monitor the controller's compliance with data protection legislation, as well as her ability to effectively exercise her other data subject rights are the right to know the recipients, as well as the sources of the data undergoing processing.

In line with these goals and building on the earlier position taken by A29WP,[49] **the provided information should include the actual named sources and actual named recipients of the data subject's personal data in particular**. Without such information, data subjects are not able to know where and how their personal data has been disseminated. Currently only a very small proportion of data controllers provides such data when requested.[50]

VI. Responses to Access Requests Need to be Specific and Tailored

55 Controllers very frequently accommodate (at least part of) access requests by reciting generic information already available in the privacy policy/notice/statement. This clearly appears from the combined empirical work of the authors, as well as the many personal experiences from other data subjects. Article 15(1) lists eight categories of information that can be requested, on top of the actual personal data being processed. When asked for some of this information in an individual access request, controllers will often answer in a very generic way. This is highly problematic in light of the different functions of the right of access (eg enabling the exercise of other rights, evaluating compliance), and its relation to the information obligations under Articles 13-14.

56 Whereas Articles 13-14 can be considered *ex ante* obligations on controllers' shoulders, Article 15 is an *ex post* right of data subjects. In other words, Articles 13-14 contain transparency requirements that need to be complied with by controllers upfront, and necessarily need to relate to *all* potential data subjects. **The added value of Article 15 is that it provides the possibility for individual data subjects to learn more about their particular situation upon request**. This also follows from the Court's case law in *Nowak*[51] and *Rijkeboer*[52].

57 The issue is illustrated by the way in which Facebook responds to access requests: With respect to information about the data categories that Facebook holds about Mr. XYZ: this depends on how he uses the Facebook Products. The data categories and their sources are clearly set out in our Data Policy (accessible via *https://www.facebook.com/policy.php*)

58 Even when specifically asked *not* to simply recite their privacy policy, Facebook still does. When explicitly requested to provide 'a complete and detailed overview of all the different ways personal data have been and will be processed (not your general privacy policy, but a list of which of my data were used for which concrete purpose) as well as the exact lawful ground (art.6 (1) GDPR) for each processing purpose', Facebook responds:

59 We understand that Mr XYZ would like a complete and detailed overview of all the different ways in which his personal data have been processed and will be processed, including the legal basis relied on by Facebook. Whilst Mr XYZ indicates he does not seek our "general privacy policy", we'd like to clarify that the information requested by him is detailed in this document and our legal bases fly out.

60 Facebook's response is problematic because:

a) it refers to its privacy policy, which manifestly does *not* link exactly what personal data is used for exactly what purpose and under what lawful ground each individual purpose falls.

b) it fails to provide a tailored answer to the data subject in particular, who wishes to know what exact information was collected for what purposes and under what lawful ground, for his particular situation.

61 In light of the above, we strongly recommend the EDPB to make it very clear in their guidelines that **the right of access in Article 15 requires controllers to tailor the information to the specific situation of the data subject making the request**. This means that each data subject can ask, for example: (a) what exact purposes their specific personal data has been processed for; (c) the exact (categories of) recipients their personal data has been disclosed to; and (g) what source their specific personal data were obtained from.

49 Article 29 Working Party, 'Guidelines on transparency under Regulation 2016/679' (n 20) 37.

50 René LP Mahieu and others, 'Collectively Exercising the Right of Access: Individual Effort, Societal Effect' (2018) 7 Internet Policy Review.

51 *Nowak* (n 4) [56].

52 *Rijkeboer* (n 4) [69].

D. The Right to Erasure (Article 17)

I. Anonymisation as Erasure is Inadequate

62 Anonymisation is often considered a valid way to evade the applicability of the GDPR. Indeed, as recognised in Recital 26, data protection rules should not apply to 'anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable'. In its 2014 Opinion on anonymisation techniques, the A29WP also stressed that 'anonymisation results from processing personal data in order to irreversibly prevent identification'.[53]

63 The GDPR incorporated the A29WP's Opinion as well as CJEU jurisprudence[54] when stating that anonymisation of personal data entails making it irreversibly impossible to identify the data subject, having regard to *all the means likely reasonably to be used*.[55] This test does not only depend on the relevant context and circumstances of each individual case,[56] its outcome can also change over time.[57] In order to assess whether or not a dataset is truly anonymous, one will reasonably have to take into account the risk of re-identification over time.[58] When the data

53 Article 29 Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (10 April 2014)."authority":"Article 29 Working Party","event-place":"Brussels","abstract":"In this Opinion, the WP analyses the effectiveness and limits of existing anonymisation techniques against the EU legal background of data protection and provides recommendations to handle these techniques by taking account of the residual risk of identification inherent in each of them.\nThe WP acknowledges the potential value of anonymisation in particular as a strategy to reap the benefits of 'open data' for individuals and society at large whilst mitigating the risks for the individuals concerned. However, case studies and research publications have shown how difficult it is to create a truly anonymous dataset whilst retaining as much of the underlying information as required for the task. In the light of Directive 95/46/EC and other relevant EU legal instruments, anonymisation results from processing personal data in order to irreversibly prevent identification. In doing so, several elements should be taken into account by data controllers, having regard to all the means "likely reasonably" to be used for identification (either by the controller or by any third party

54 Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* EU:C:2016:779 [46]. In this case, the Court agreed with the AG that anonymisation hinges on whether 'identification of the data subject was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant.'

55 Recital 26 (both in the GDPR and Directive 95/46 before that). Also see: Article 29 Working Party, 'Opinion 4/2007 on the Concept of Personal Data' (Article 29 Working Party 20 June 2007) 15; Article 29 Working Party, 'Working Document on the Processing of Personal Data Relating to Health in Electronic Health Records (EHR)' (15 February 2007) 29; Article 29 Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (n 53) 5 et seq; Pagona Tsormpatzoudi, 'Eksistenz D7.4 Intermediate Report for D7.5' (Deliverable, CiTiP 27 November 2015) 14.

56 Important factors to take into account in this regard are: Who will the 'anonymised' dataset be shared with? How will it be processed? What other data will/might it be combined with? What are the means that a likely attacker would have? See also Article 29 Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (n 53) 10."event-place":"Brussels","abstract":"In this Opinion, the WP analyses the effectiveness and limits of existing anonymisation techniques against the EU legal background of data protection and provides recommendations to handle these techniques by taking account of the residual risk of identification inherent in each of them.\nThe WP acknowledges the potential value of anonymisation in particular as a strategy to reap the benefits of 'open data' for individuals and society at large whilst mitigating the risks for the individuals concerned. However, case studies and research publications have shown how difficult it is to create a truly anonymous dataset whilst retaining as much of the underlying information as required for the task.\nIn the light of Directive 95/46/EC and other relevant EU legal instruments, anonymisation results from processing personal data in order to irreversibly prevent identification. In doing so, several elements should be taken into account by data controllers, having regard to all the means "likely reasonably" to be used for identification (either by the controller or by any third party

57 Particularly in the long run, Narayanan and others explain there is no technical basis for believing de-identification techniques will be effective. Arvind Narayanan and others, 'A Precautionary Approach to Big Data Privacy' in Serge Gutwirth and others (eds), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection* (Law, Governance and Technology Series, Springer Netherlands 2016). Similarly, Barocas and Nissenbaum explain '[a]s data sets become increasingly linked, anonymity is largely impossible to guarantee in the future.' Solon Barocas and Helen Nissenbaum, 'Big Data's End Run around Anonymity and Consent' in *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (Cambridge University Press 2014).

58 eg due to the development of ICTs and/or likelihood of identification through future combining with other databases. Article 29 Working Party, 'Opinion 05/2014 on

controller has no *a priori* means of distinguishing between anonymous and personal data in a mixed dataset, it will need to treat the entire set as personal data.[59]

64 We believe **data controllers often confuse anonymisation with erasure, and this creates a range of challenges**.

65 Firstly, many data formats in the modern digital economy **simply cannot be anonymised**. This is substantiated by an overwhelmingly rich and growing body of literature.[60] Indeed, in an online environment, with ever-increasing data processing capabilities, no guarantees can be given that any data-point might be (re-)connected to an identifiable natural person in the future. We therefore agree with the A29WP's 2014 Opinion stating that anonymised datasets can still present residual risks to data subjects,[61] and believe it is much more useful to look at **anonymisation as a sliding scale rather than a binary**.[62] Erasure, on the other hand and when

Anonymisation Techniques' (n 53) 8–9."event-place":"Br ussels","abstract":"In this Opinion, the WP analyses the effectiveness and limits of existing anonymisation techniques against the EU legal background of data protection and provides recommendations to handle these techniques by taking account of the residual risk of identification inherent in each of them.\nThe WP acknowledges the potential value of anonymisation in particular as a strategy to reap the benefits of 'open data' for individuals and society at large whilst mitigating the risks for the individuals concerned. However, case studies and research publications have shown how difficult it is to create a truly anonymous dataset whilst retaining as much of the underlying information as required for the task.\ nIn the light of Directive 95/46/EC and other relevant EU legal instruments, anonymisation results from processing personal data in order to irreversibly prevent identification. In doing so, several elements should be taken into account by data controllers, having regard to all the means "likely reasonably" to be used for identification (either by the controller or by any third party Also see: Douwe Korff, 'Data Protection Laws in the EU: The Difficulties in Meeting the Challenges Posed by Global Social and Technical Developments' (Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments, European Commission - DG Justice 2010) 48.

59 The A29WP gives the example of internet access providers who can generally not know what IP address does and does not allow identification. Article 29 Working Party, 'Opinion on Personal Data' (n 55) 16–17.

60 See generally (including the many references in): P Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57 UCLA Law Review 1701; Douwe Korff and Ian Brown, 'Comparative Study on Different Approaches to New Privacy Challenges , in Particular in the Light of Technological Developments' (Final Report, 20 January 2010) 28; Arvind Narayanan and Vitaly Shmatikov, 'Myths and Fallacies of "Personally Identifiable Information"' (2010) 53 Communications of the ACM 24; Paul M Schwartz and Daniel J Solove, 'PII Problem: Privacy and a New Concept of Personally Identifiable Information, The' (2011) 86 NYU L Rev 1814; Mario Viola de Azevedo Cunha, 'Review of the Data Protection Directive: Is There Need (and Room) For a New Concept of Personal Data?' in Serge Gutwirth and others (eds), European data protection: in good health? (Springer 2012); Yves-Alexandre de Montjoye and others, 'Unique in the Crowd: The Privacy Bounds of Human Mobility' (2013) 3 Scientific Reports 1376; Arvind Narayanan and Edward W Felten, 'No Silver Bullet: De-Identification Still Doesn't Work' [2014] White Paper; Barocas and Nissenbaum (n 57); Narayanan, Arvind, 'What Should We Do about Re-Identification? A Precautionary Approach to Big Data Privacy' (*Freedom to Tinker*, 19 March 2015) <https://freedom-to-tinker.com/blog/randomwalker/what-should-we-do-about-re-identification-a-precautionary-approach-to-big-data-privacy/> accessed 24 February 2016; Yves-Alexandre de Montjoye and others, 'Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata' (2015) 347 Science 536; Antoinette Rouvroy, '"Of Data and Men". Fundamental Rights and Freedoms in a World of Big Data' (11 January 2016) 21; Sophie Stalla-Bourdillon and Alison Knight, 'Anonymous Data v. Personal Data—a False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data' (2017) 34 Wisconsin International Law Journal 284; Luc Rocher and others, 'Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models' (2019) 10 Nat Commun 1.

61 Article 29 Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (n 53) 4."authority":"Article 29 Working Party","event-place":"Brussels","abstract":"In this Opinion, the WP analyses the effectiveness and limits of existing anonymisation techniques against the EU legal background of data protection and provides recommendations to handle these techniques by taking account of the residual risk of identification inherent in each of them.\nThe WP acknowledges the potential value of anonymisation in particular as a strategy to reap the benefits of 'open data' for individuals and society at large whilst mitigating the risks for the individuals concerned. However, case studies and research publications have shown how difficult it is to create a truly anonymous dataset whilst retaining as much of the underlying information as required for the task.\nIn the light of Directive 95/46/EC and other relevant EU legal instruments, anonymisation results from processing personal data in order to irreversibly prevent identification. In doing so, several elements should be taken into account by data controllers, having regard to all the means "likely reasonably" to be used for identification (either by the controller or by any third party

62 See (the references in): Nadezhda Purtova, 'The Law of

executed properly, *is* a binary and data controllers should in principle be required to irretrievably remove all personal data from their system rather than merely anonymising it.

66 Secondly, it is important to remember that, since data protection is an intent-agnostic regime (see further section 9.4, this document) **there are many motivations for erasure**. Some of these concern confidentiality, which (proper) anonymisation may help to meet. Yet these are not all the concerns a data subject might have. Since its origins, data protection law has also — arguably primarily — been seen as a regime for regulating the imbalances that emerge from informational power.[63]

67 Informational power is tied up with notions of 'group' or 'categorical' privacy.[64] An individual, for example, may not wish for information to be known and processed around a community, neighbourhood or demographic she is part of.[65] She may wish to erase data not to obscure herself, but to obscure the groups she constitutes from a data controller she does not favour or trust. **Anonymisation instead of erasure disempowers her**. It states that her data can still be utilised, valorised, for example 'anonymised' into machine learning models,[66] while she has specifically stated she no longer wants that data to be accessible to the data controller in any form.

Anonymisation can thus be used to *disempower* data subjects. Anonymisation may prevent individuals 'from understanding, scrutinising, and questioning the ways in which data sets are used to organise and affect their access to resources and connections to a networked world.'[67] Indeed, as the authors have demonstrated elsewhere, some data controllers argue that they cannot accommodate data subject rights because they allegedly have no way of reidentifying the data subject, effectively disempowering individuals.[68]

68 Furthermore, the proportionality of anonymisation rather than erasure should be read in the context of the many hurdles to successful erasure in Article 17. If such hurdles are overcome (which in many cases are difficult and raise uncertainties about how to proceed, see section 4.2, this document), then a data subject should be entitled to erasure, and not less than that. **Erasure is possible when no valid processing purposes remain: these purposes include purposes where anonymisation and aggregation, which themselves are processing operations, are utilised.**

69 Thirdly, **the right to erasure does not explicitly mention anonymisation as constituting an equivalent measure**. This becomes clear when comparing the language of Article 17 – clearly dictating erasure *per se* – with other provisions that use the language of recital 26 on anonymisation – i.e. data no longer permitting identification – such as the storage limitation principle (Article 5(1)(e)) and its different mutations in Article 11 and 89.

II. Interpreting Erasure as Objection

70 The right to erasure tackles the underlying data involved in a processing operation. Because the same data can and is often processed in many different ways, often with a different lawful ground, erasure may fail if the data controller can retain a valid

Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10 Law, Innovation and Technology 40.

63 See eg the work of Stefano Rodotà, former chairman of the Article 29 Working Party, in particular Stefano Rodotà, *Elaboratori Elettronici E Controllo Sociale* [Computers and Social Control] (Societa Editrice Il Mulino 1973) and in Germany: Wilhelm Steinmüller and others, *Grundfragen des Datenschutzes Gutachten im Auftrag des Bundesmnisteriums des Innern* (BT-Drs. VI/3826 1971).

64 See generally Anton Vedder, 'KDD: The Challenge to Individualism' (1999) 1 Ethics and Information Technology 275; Linnet Taylor and others (eds), *Group Privacy: New Challenges of Data Technologies* (Philosophical Studies Series, Springer International Publishing 2017).

65 See further Edwards and Veale (n 35) 46–48.

66 It is worth noting that such anonymisation may also not be valid, as machine learning models can 'remember' data they have been trained on, or in some cases such as *support vector machines*, simply store it as part of their model. See generally Michael Veale and others, 'Algorithms that Remember: Model Inversion Attacks and Data Protection Law' (2018) 376 Phil Trans R Soc A 20180083.

67 Seda Gürses, 'The Spectre of Anonymity' in Renée Turner (ed), *Sniff, scrape, crawl . {on privacy, surveillance and our shadowy data-double}* (Mute Publishing Ltd 2012) 3; 5; Seda Gürses, 'Can You Engineer Privacy?' (2014) 57 Communications of the ACM 20.

68 Specifically, Apple denies access requests with regard to Siri voice data it collects and stores for up to two years, because they say they do not have the tools in place to re-connect such voice data to the user. Even if this argumentation can be contested significantly, it does raise a considerable hurdle to data subject empowerment. See particularly Michael Veale and others, 'When Data Protection by Design and Data Subject Rights Clash' (2018) 8 International Data Privacy Law 105.

lawful ground for data processing. Even if one of the grounds in Article 17(1) applies, this might not lead to effective erasure. It is therefore important that the guidance clarifies how to resolve situations in which erasure is requested, but the controller claims it can further process the respective personal data for different purposes.

71 Even where data controllers offer data subjects a right to erasure, it is often unclear *what* personal data it applies to exactly and *under what circumstances* the right can be invoked. As illustrated in Table 1 below, **the applicability of the right to erasure inherently depends on what lawful ground is relied on for which processing purpose(s) relating to what specific personal data** in particular. The vast majority of privacy notices/statements of information society services fails to clearly link these components (simply listing what personal data is processed separately from what purposes they process personal data for and/or the lawful grounds relied on), rendering it very hard to effectively exercise the right to erasure. This is made even more challenging by the practice of data controllers to 'switch' between, for example, consent and legitimate interests.[69] It is exacerbated by the 'list' approach to Article 13/14, whereby data controllers provide a list of lawful bases (often copied straight from the GDPR), a list of data categories, and a list of data processing operations, without cross-referencing them in any way.

72 **In order for the right to erasure to have any meaningful role, data controllers should make it very clear upfront (eg in their privacy notice/statement) what personal data it applies to and under what circumstances.** This obligation also follows from the transparency principle (Article 5(1)(a)), purpose limitation principle (Article 5(1)(b)) and transparency requirements in Articles 13–14. Table 1[70] (see next page) describes the complexity of the 'erasure triggers'. These illustrate the importance of making the functioning of the right to erasure clear to data subjects. It is also not clear that data controllers understand these distinctions.

73 Making it clear which data a data subject can, and cannot, erase is important because without this, the data subject cannot easily make an informed choice as to whether they should use a particular service, or engage with a particular data controller.

69 See eg Privacy International, 'Submission to the Information Commissioner: Request for an Assessment Notice/Complaint of AdTech Brokers Criteo, Quantcast and Tapad (the 'AdTech Data Brokers')' (8 November 2018).

70 Jef Ausloos, The Right to Erasure in EU Data Protection Law. From Individual Right to Effective Protection (Oxford University Press forthcoming).

74 In this context, it is also important to recall the Court's view that rights must be protected in an 'efficient and timely' manner.[71] An efficient manner is one which does not require the data subject to expend unnecessary energy in order to secure protection of their rights. An efficient, timely approach here would be to **require data controllers to interpret 'failed' erasure attempts, due to residual legal bases, as a clear signal to object.** The controller would then be required to re-substantiate its claim to have a continued lawful ground for further processing said personal data.

> An employee at work has their 'screen time' monitored by an employer who produces aggregate activity about the different tasks workers engage in. The employer utilises a piece of software to undertake such tracking, and claims that such monitoring falls within its legitimate interests. An employee requests the erasure of this data. However, recent data is also used for the purposes of security and access control, as the installed software has more than one purpose, and the data controller believes such security presents a compelling legitimate interest, meaning that not all the data can be erased. The data controller must interpret the erasure request as erasure insofar as possible and treat the remaining portions of the request as a request to object (or, if appropriate, withdraw consent) in relation to processing operations for which the data subject's prevail in a balancing test.
>
> **Proposed Example**

III. Availability of erasure does not absolve from other GDPR obligations

75 In principle, the right to erasure is only a last resort solution, empowering data subjects to request erasure in situations where their personal data ought to have been erased already in the first place. This clearly appears from the six situations listed in Article 17(1), which all im-/explicitly refer to other provisions in/outside the GDPR that already imply erasure (cf. Table 2 next page).

76 In the authors' experience, data controllers often appear to use the availability of data subject rights as a red herring. Yet, offering data subjects a right to erasure does not absolve data controllers from having to comply with key data protection principles such as purpose limitation (Article 5(1)(b)), data minimisation (Article 5(1)(d)), or storage limitation (Article 5(1)(e)). Indeed, many privacy

71 *Fashion ID* (n 5) [102].

Legal Basis		Relation	Erasure Triggers
(a) Consent		When consent is relied on as lawful ground, the most relevant right to erasure trigger will be **b)**, i.e. withdrawing consent. When consent was given in the context of ISS while the data subject was a child, the last trigger **f)** could also be used. Theoretically, triggers **a)** (purpose expiration), **e)** (legal obligation), and **d)** (unlawful processing) will also be applicable. Given the difficulty of demonstrating expiration of purposes or unlawfulness in practice, it seems much more straightforward to simply rely on the less ambiguous withdrawal of consent to obtain erasure.	**a)** purpose expiration **b)** consent withdrawal **d)** unlawful processing **e)** legal obligation **f)** consent withdrawal in context of ISS offered to children
(b) Contract		When necessity for the performance of a contract is relied on as lawful ground for processing, the most relevant trigger to rely on will be **a** purpose expiration (which will generally occur at the latest upon rescinding the contract). Trigger **d)** may also be relevant when the lawful ground is not valid (anymore). To the extent this ground overlaps with the first lawful ground on consent, trigger **b)** might also be of some relevance. Finally, it cannot be excluded that an external legal obligation imposes erasure, even when processing is still necessary for performance of a contract (so trigger **e)** remains open).	**a** purpose expiration **b** consent withdrawal **d** unlawful processing **e** legal obligation
(c) Legal Obligation	*(d) Vital Interests*	These two lawful grounds are largely outside the control of any of the parties involved. The most relevant triggers therefore will be **a)** (purpose expiration) and **e** (legal obligation). As always, trigger **d)** remains available in those situations where the lawful ground is incorrectly relied upon in the first place.	**a)** purpose expiration **d)** unlawful processing **e)** legal obligation
(e) Task in Public Interest		Compared to the previous two, this lawful ground leaves more room for interpretation as to the scope of processing operations that it may cover. So, on top of triggers **a** (purpose expiration), **e** (legal obligation) and **d** (unlawful processing), data subjects will also be able to request erasure on the basis of trigger **c**, following a right to object.	**a)** purpose expiration **c)** right to object **d)** unlawful processing **e)** legal obligation
(f) Legitimate Interests		Contrary to the previous three, the last lawful ground leaves considerable freedom to controllers to define their interests and purposes. Particularly triggers **a)** (purpose expiration), **c** (right to object) and **d)** (unlawful processing) will be relevant, though **e)** (legal obligation) remains open as well.	**a)** purpose expiration **c)** right to object **d)** unlawful processing **e)** legal obligation

Table 1: Right to Erasure Trigger by Legal Basis

Right to erasure triggers	**Cross-references**	
Article 17(1)	**Articles**	**Recitals**
(a) Purpose expiration	5(1)b, c and e; 6(4); 13(2)a; 14(2)a	*39; 50*
(b) Consent withdrawal	*4(11); 6(1)a; 7; 8; 9(2)a*	*32; 42*
(c) Right to object	*21*	*69; 70*
(d) Unlawful processing	*4(11); 5(1)a; 6(1); 7; 8; 9*	*32; 65; 69*
(e) Legal obligation	*6(1)c*	*10; 45*
(f) Minors' withdrawal of consent in ISS context	*7; 8*	*38*

Table 2: Right to Erasure Triggers and relevant GDPR provisions

notices/statements appear to offer data subjects a right to erasure mainly pro forma only, while at the same time acknowledging a vast data processing apparatus.

77 Indeed, important research in behavioural sciences has demonstrated that the perceived control data subjects have over their personal data through tools such as the right to erasure, may paradoxically lead to lower concerns over data processing practices and a false sense of security, which in turn may lead to revealing even more (sensitive) information.[72]

E. The Right to Object (Article 21)

78 The right to object offers data subjects an opportunity to oppose the further processing of their personal data for specific purposes. It comprises a much stronger focus on the specific context in an individual situation than the ex-ante (and more generic) balancing as prescribed by Article 6(1)(f).[73] Even though processing may be 'lawful' under Article 6(1)(e–f) GDPR, the right to object offers a context-dependant and individualised re-assessment. This can be derived both from the use of the broader term 'grounds' (as opposed to interests as contained in Article 6(1)(e)-(f))74 and the words 'relating to his or her particular situation' (as opposed to a more generic situation in Article 6(1)(f)).75 In light of this, we recommend the EDPB to require data controllers to clearly demonstrate any argument against the right to object in relation to the specific situation of the data subject, rather than a generic statement.

I. Compelling Legitimate Interests Must be Detailed, Public and Foreseeable

79 The right to object is available to data subjects with regard to processing operations that rely on legitimate interests as a lawful ground (Article 6(1)(f)). As emphasised by the A29WP, legitimate interests are not an 'easy' alternative to consent, but require substantive and public justification.[76] The Information Commissioner's Office has expressed concern that particularly online, data controllers seeing legitimate interests as the 'easy option' lack a 'full understanding of what legitimate interests requires'.[77]

80 Because individuals are asked to formulate and provide 'grounds' specific to their situation, which will be weighed against any compelling legitimate grounds of the data controller, it should be the case that the legitimate interest of the data controller are laid out in advance in accordance with Article 13 and 14. Article 13(1)(d) states that data controllers must provide the data subject with 'the legitimate interests pursued by the controller or by a third party'.

81 This is an important component for the individual in determining whether and how to make the case for their right to object. It should be considered contrary to the fairness principle for a data controller, in balancing the right to object against potential compelling legitimate grounds, to rely on a legitimate interest which has not been clearly declared to the data subject in advance. This could put the data subject in a position where they chose a particular service provider and enabled them to process data about themselves under Article 6(1)(f), unaware of the interests of the controller and unable to foresee their own capacity to object in the face of these undeclared legitimate interests. This is particularly key because legitimate interests operate in the context of 'necessity', which is a concept that must be scrutinised in relation to determining whether or not processing is lawful.[78]

72 Laura Brandimarte and others, 'Misplaced Confidences: Privacy and the Control Paradox' (2012) 4 Social Psychological and Personality Science 1948550612455931.

73 See also Damian Clifford and Jef Ausloos, 'Data Protection and the Role of Fairness' (2018) 37 Yearbook of European Law 130.

74 The language used implies that the term 'grounds' here can be understood as broader than 'interests' (i.e. given the fact that the data subject grounds to object appear to include; context, interests rights and freedoms).

75 See in this regard also *Google Spain* (n 3) [75]–[76].

76 Article 29 Working Party, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' (Opinion, European Commission 9 April 2014).

77 Information Commissioner's Office, 'Update Report into Adtech and Real Time Bidding' (20 June 2019) 18.

78 See eg Case C-13/16 Valsts policijas Rīgas regiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme' EU:C:2017:336 [30] and the case-law cited.

A wayfinding transport application sequence, upon download, informs a data subject that they process location data on the basis of Article 6(1)(f) for the purposes of building an aggregated, anonymised dataset to help the company provide traffic data within the app. Later, the data controller receives an objection request from this data subject relating to the use of location data for this purpose. The data controller carries out a balancing test, and argues that while the data subject's objection request overrides the legitimate interest of in-app traffic data, the controller also provides this aggregated, non-personal data to local governments and planning agencies, and this represents a compelling legitimate ground. However, because the data controller had not already declared this specific, albeit genuine, legitimate interest, the right to object must be upheld.

Proposed Example

II. Objection and Processing 'Necessary for the Performance of a Contract'

82 The right to object only has a limited scope of application, as it only applies to situations where processing is based on either one of the last two lawful grounds in Article 6(1). It is therefore unsurprising that since the entry into force of the GDPR, many controllers whose business model relies heavily on personalisation (and advertisement) have shifted from relying on either consent[79] or legitimate interests,[80] to necessity for the performance of a contract.[81] Reliance on this ground effectively strips data subjects from the ability to withdraw their consent[82] or object[83] to said processing. In light of the recent EDPB guidance on the lawful basis of necessity for contract,[84] **many controllers may be illegitimately relying on this ground**.

83 With that in mind, it would be valuable if the guidance could specify that **data subjects also have the right – more broadly – to challenge controllers' compliance with any of the GDPR's requirements** (even if it does not qualify as a specific right in Chapter III). This is already reflected in the implied right in Article 18(1)(b) to object to 'unlawful' processing,[85] and Article 17(1)(d) to erase personal data processed without an adequate lawful ground.[86] As DPAs, such as the Information Commissioner's Office in the UK, are requesting that individuals 'raise a concern' with an organisation before they will take action, **clarification on the modalities for data subjects to challenge data controllers' compliance with key provisions (such as the data protection principles in Article 5 and the lawfulness requirement in Article 6) is particularly important**.[87] In particular, the guidance should specify what the obligation of a controller to respond to such claims of unlawful processing should be.

F. The Right to Restriction of Processing (Article 18)

84 Restriction of processing means 'the marking of stored personal data with the aim of limiting their processing in the future'.[88] The data subject has the right to restrict processing while they are waiting for an assessment of the accuracy or the efficacy of the right to object, as well as in situations where they claim the processing is unlawful (to ensure retention of evidence of unlawfulness) and where the data subject wishes to ensure the data still exist for the establishment, exercise or defence of legal claims.[89] Despite many such requests, **we have encountered not a single data controller that acknowledged, let alone accommodated, the right to restriction of processing**.

79 GDPR, art 6(1)(a).

80 GDPR, art 6(1)(f).

81 GDPR, art 6(1)(b).

82 GDPR, art 7(4).

83 GDPR, art 21.

84 European Data Protection Board, 'Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects (Version 2.0)' (8 October 2019).

85 Noting that the data subject shall have the right to obtain from the controller restriction of processing where 'the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead'.

86 Noting that 'the data subject shall have the right to obtain from the controller the erasure of personal data [...] the personal data have been unlawfully processed'

87 See Information Commissioner's Office, 'Raising a Concern with an Organisation' (24 September 2019) <https://ico.org.uk/your-data-matters/raising-concerns/> accessed 11 June 2019.

88 GDPR, art 4(3).

89 See generally, GDPR, art 18.

I. Restriction Timeframe for Information Society Services

85 Information society services encompass any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.[90] In many cases, data subjects will already be verified to use the service through having logged in.

86 The right to restrict processing is an interim measure. Particularly given the automated way information society services function, it is important to give effect to this interim measure. In *Fashion ID*, the Court was clear that provisions of data protection law must be interpreted as to give effect to the 'efficient and timely' protection of the data subject's rights.[91] As a consequence, the right to restrict processing must always be interpreted and enforced as to give effect to its nature as an interim measure.

The right to restrict must therefore be prioritised in time, and subject to a considerably tighter timeframe than, for example, the right to object it is linked to. Where it is feasible to automate restriction in this interim period, it may be incumbent on a data controller, on the basis of data protection by design and the risk-based approach throughout data protection, to do so.

II. In the context of continuous processing and profiling

87 The right to restrict processing is likely to impose different technological and organisational requirements on different data controllers. For example, for an organisation operating a customer relations management (CRM) system, a flagged, restricted profile can quite easily be separated from normal processing activities.

88 Many firms in the modern digital economy operate under conditions of *continual processing*, and do so under grounds including legitimate interests. This is the situation where the right to restrict is the most important, yet we are concerned that **data controllers are disregarding the right to restriction of processing.** The GDPR states:

> *In automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed.*[92]

89 For example, where an individual has objected to tracking or profiling, and has in the meantime restricted processing, this should mean that the **continual processing stops in the meantime, and that no more profiles are built, updated or applied.** In practice, this does not occur.

III. Necessary processing, legitimate interests and the right to restrict

90 **Data controllers must be able to stop processing of data that is subject to the right to restriction in an interim period.** This must be technically and organisationally feasible within their systems, in light of the requirements in Articles 24-25 GDPR.

91 In this context, we note the recent 14m EUR fine levied by the DPA of Berlin in relation to a failure of data protection by design. In this case, a data controller operated an archiving system that was unable to erase data. Such a system was held to be in breach of Article 25.[93] Similarly, a processing system which is unable to implement an interim period of restricted data processing would quite clearly also fall foul of Article 25 in a similar manner.

92 We believe that the clearest way to deal with this issue is to state that **all data that has the potential to be restricted must be technically possible to restrict**, with the exception of data which the data controller can reliably continue to process for the reasons laid out in Article 18(2) without the authorisation of the data subject, namely (i) for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person; and (ii) for reasons of important public interest of the Union or of a Member State.

90 Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (Text with EEA relevance), art 1(1)(b).

91 *Fashion ID* (n 5) [102].

92 GDPR, recital 67.

93 Berliner Beauftragte für Datenschutz und Informationsfreiheit, 'Berliner Datenschutzbeauftragte verhängt Bußgeld gegen Immobiliengesellschaft' (711.412.1, 5 November 2019).

A data controller providing an app processes telemetry data, such as the data subject's behaviour inside the app, on the basis of legitimate interests. The data subject has logged into this app, and submits a request for restriction, and a request for objection in relation to the telemetry purposes. The data controller has no means to prioritise restriction in time over the objection request, and besides, has not installed functionality in the app to prevent all telemetry data processed under the legitimate interest ground to cease. Consequently, the data controller is in breach of the GDPR.

Proposed Example

G. The Right to Rectification (Article 16)

93 In this section, we look only at one element of the right to rectification: the right to rectify in the context of inferences and opinions.

I. Opinions and Inferences

94 Inferences and opinions are considered to be personal data by the CJEU.[94] As with all data rights, **the right to rectification should generally apply to inferences and opinions unless justified exceptions grounded in law exist**.

95 In some cases, the data controller may disagree with the attempt to rectify data by the data subject. This may be the case, for example, where a third party has provided an opinion to an employer about an individual's inappropriate behaviour in the workplace. In this case, balancing is clearly justified, as Charter rights could be implicated, such as Articles 11, 12, 15 and 21.

96 **The EDPB should avoid permitting either the data subject or the data controllers can act as the 'arbiter of truth' in contentious cases.** Where the data controller has good reasons to disagree with the data subject concerning a proposed rectification, the best solution is to **oblige both opinions to co-exist in the data processing system, and to oblige the data controller in line with the accuracy and fairness principles to consider both the rectified and the original data in downstream data processing**. In this sense, **rectification is an addendum rather than a replacement.**

97 **It should not, however, be considered a 'good reason' simply because the inference would be convenient to retain in its current form from a business perspective.** This is particularly the case for profiling in the digital economy, for example in the area of advertising 'interests'. In these cases, the right to data protection will be likely to prevail, particularly given the highly subjective nature of profiling and predictive inference techniques.[95] For example, in the context of the digital economy, an individual may be classified as 'male' by a predictive system: this should be open for an individual to rectify.

98 It should be recalled that the **data subject retains the right to erase the 'original', pre-rectified data that is retained by the data controller, or to object to its use**, and the procedures for each of these rights act as balances for the interests at stake in that situation.

H. Recognising Rights

99 Data rights can come in a variety of forms and manners, and the guidance must clearly address issues in practice that relate to the recognition of rights.

I. Requiring a Specific Request Form or Format Should Not Be Permitted

100 Both the data controller and processor have an explicit obligation to facilitate the exercise of data subject rights (Articles 12(1) and 28(3)(e)). In light of this obligation, it is certainly to be encouraged that tools be developed in order to make data subject rights more accessible to data subjects (eg privacy dashboards, forms, 'download my data' functions, etc). However, **data controllers or processors cannot force data subjects to exercise their rights in one way or another** as long as the requirements under the GDPR are complied with. Moreover, practice shows that when data subjects request access to additional information *not* included in 'download my data' functionalities (but mentioned in Article 15), they are often ignored.[96]

94 *Nowak* (n 4) [34].

95 See generally Solon Barocas and Andrew D Selbst, 'Big Data's Disparate Impact' (2016) 104 California Law Review 671.

96 See eg Jef Ausloos and Pierre Dewitte, 'Shattering One-Way Mirrors – Data Subject Access Rights in Practice' (2018) 8 International Data Privacy Law 4.

II. Accurately Recognising Data Subjects' Intent Without Legislative Wording

101 Following on from the previous point, it is important that data subjects cannot be expected to use the exact wording of the GDPR in order for their rights to be effectively accommodated. Indeed, the Commission's first objective when officially announcing its plans for a data protection reform concerns the strengthening of data subject rights.[97] In light of the Court's emphasis on ensuring an 'effective and complete protection', it is therefore necessary that data controllers act on the apparent intent of data subject requests, and cannot require them to use the exact phrasing (or article references) of the GDPR. **The guidance should be clear about what a data controller should do upon receiving a request which is vague, but could be interpreted as a right to restrict, object, erase, port or access.**

III. Joint Controllers and Processors Must Pass on and Deal with Data Rights

102 Article 26 of the GDPR clarifies the concept of *joint controllers*: '[w]here two or more controllers jointly determine the purposes and means of the processing of personal data, they are joint controllers [...]'.[98] The article further requires such joint controllers to delineate, in a transparent manner, their respective responsibilities in light of complying with the GDPR. Importantly, **data subjects can exercise their rights (to erasure) vis-à-vis any of the joint controllers, regardless of the arrangement (of respective roles and responsibilities) between these controllers (Article 26(2))**. In other words, even though 'joint controllership' might have considerable ramifications as to GDPR compliance and allocation of responsibilities,[99] from the perspective of a data subject exercising his/her rights it is less relevant.

103 Article 28(3)(e) dictates that processors need to assist the controller in accommodating data subject rights, notably by adopting 'appropriate technical and organisational measures, insofar as this is possible'. This should be interpreted as allowing a data subject to invoke his/her right to erasure vis-à-vis processors as well. **Whereas they are not the ones responsible to effectively accommodate the data subject's rights, processors are liable to *assist* controllers in doing so**.

104 In sum, the plurality of actors processing personal data should not hinder the effective exercise of data subject rights. Data subjects can approach processors and/or (joint) controller(s) with their rights, even though that entity might not be the one who is ultimately responsible to accommodate such claims *in casu*. Even when the complexity of a processing chain causes the data subject to invoke their right vis-à-vis the 'wrong' controller, the latter should still be required to forward the request (Article 19). This process can be made easier with a single point for request to be made by data subjects, or forwarded to by joint controllers. Notwithstanding the possibility for data subjects to direct their requests to each joint controller, the EDPS recommends to establish a single contact point to which data subjects may forward their requests in exercising their rights.'[100] The burden of enabling effective use of data subject rights, especially in complex networks of processing, should be on the various controllers and processors.[101]

97 European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Comprehensive Approach on Personal Data Protection in the European Union' (4 November 2010).

98 The concept of 'joint controllership' only first made an appearance during the legislative process of Directive 95/46 (inserted by the European Parliament) Article 29 Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (Article 29 Working Party 16 February 2010) 17–18.

99 Brendan Van Alsenoy, 'Allocating Responsibility among Controllers, Processors, and "Everything in between": The Definition of Actors and Roles in Directive 95/46/EC' (2012) 28 Computer Law & Security Review 25; Korff (n 58) 61. The latter author highlighting issues arising from joint controllership between entities located in different jurisdictions.

100 European Data Protection Supervisor, 'Guidelines on the Concepts of Controller, Processor and Joint Controllership under Regulation (EU) 2018/1725' (7 November 2019) 30–31.

101 Rene Mahieu and others, 'Responsibility for Data Protection in a Networked World: On the Question of the Controller, Effective and Complete Protection and Its Application to Data Access Rights in Europe' (2019) 10 J Intell Prop Info Tech & Elec Com L 84.

A news website uses an installed third-party tracker which gathers data about website visits against persistent identifiers. A data subject contacts the news website to ask for access to data collected by these trackers. As the website is a joint controller with the organisations who maintain the code for the trackers, it is the websites responsibility to pass the access request on to every tracking organisation they have a joint controllership arrangement with.

Proposed Example

I. Illegitimate Refusal of Rights

105 The principle of effective and complete protection and the status of data protection as a fundamental right both point to a strong consideration of necessity where rights are being refused or restricted. In practice, we believe the scope of refusing rights is narrower than many data controllers currently understand and practice.

I. Prima Facie Limits of the 'Rights and Freedoms of Others'

106 The right to access a copy of personal data and the right to portability are both limited by paragraphs stating that the stated aspects of these rights 'shall not adversely affect the rights and freedoms of others.'[102] This requires some considerations of, among other issues, the privacy and data protection interests of third parties (see further, section 3.4 this paper).

107 However, it should be clarified in the guidance that this consideration **is not present for other rights, such as the right to object or restrict processing**. A different and more specific balancing arrangement is in place for the right to erasure. As a consequence, **the guidance should indicate that the right to object or restrict processing should not be unduly hindered by the privacy interests of others**.

A 'smart speaker' analyses voice recordings on the basis of legitimate interests to improve the quality of speech recognition in certain languages. A data subject who uses the device in a communal area requests the right to object to this processing purpose. The data controller does not need to seek the approval of the other members of the household, whose voices are also picked up by this speaker in an indiscriminate manner, in order to process this right.

Proposed Example

102 GDPR, arts 15(4), 20(4).

II. Excessiveness Exemptions Relate to Requests' Nature, Not Burden or Intent

108 Article 12(5) allows data controllers to refuse to act upon a right where 'requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character'. Where they do this, the 'controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.'

109 The A29WP have noted, in guidance endorsed by the EDPB and in relation to another right (i.e. to data portability), that for the cases of information society services which specialise in automated data processing, 'there should be very few cases where the data controller would be able to justify a refusal to deliver the requested information, even regarding multiple data portability requests.'[103]

110 They also note that the cost of building the infrastructure to comply with these requests is irrelevant to the notion of 'excessive' requests. In particular, they state that 'the overall system implementation costs should neither be charged to the data subjects, nor be used to justify a refusal to answer portability requests.'[104]

111 An argument that a 'manifestly unfounded or excessive' request might be construed as one which relates to any sufficiently large or complex processing operation sets a dangerous precedent that some data processing activities are 'too big to regulate'. This logic would mean to say that some processing activities are at such a global scale, and so complex, and producing and capturing so much data about individuals, that they escape the reach of fundamental rights such as the right to access. This seems perverse: **the more impactful and the more sizeable the activity, surely the higher the acceptable cost of compliance on the data controller, and the more urgent and pressing the need to provide data subjects with oversight and control rights**.

112 Where such processing implicates a high number of users, this would likely count as 'large scale' processing posing a high risk under the GDPR, and thus has little ground to be manifestly 'unfounded'. According to the GDPR compliance should scale *up* in relation to high risk processing, not down.[105]

103 Article 29 Working Party, 'Guidelines on the right to data portability (WP 242)' (n 9) 9–10.

104 ibid 15.

105 GDPR, art 24.

III. Repetitive Requests May Be Justified in Situations of Continuous Processing

113 In the case of information society services in particular, personal data is constantly being collected, amended, transformed and applied. As a result, any provisions which assume static, long term, unchanging datasets must, in order to preserve the fairness principle and the technology-neutral nature of the GDPR, be read in light of modern data processing practices.

114 As a result of this situation of 'continuous processing', the rights of access, rectification and/or erasure may be of permanent relevance as well. The guidance should therefore be mindful to **clearly constrain the scope of Article 12(5) GDPR**, allowing controllers to refuse to act or charge fees for accommodating data subject rights when they are 'excessive, in particular because of their repetitive character'. **When personal data, and how it is processed, constantly changes, repeatedly exercising data subject rights should not be considered excessive. Instead, it may be upon controllers to ensure an automated and easy manner to facilitate the accommodation of those rights.** This is also relevant for the right to data portability (not within the scope of the planned guidance), which may actually require controllers such as social networks to implement protocols for enabling interoperability (essentially allowing for a constant stream of 'access rights' in a machine-readable format).

> A gaming platform runs a dynamic data collection and scoring system which determines an individual's visibility to other players. This data is updated every day, and the score is updated accordingly. A data subject makes two requests within a month for this changing data. The data controller is not permitted to refuse the request on the basis that it is 'excessive, in particular because of [its] repetitive character', because the data processing operation is of a similar character. Instead of refusal, the data controller must either honour the requests or justify refusal under some other basis. This is proportionate as, in line with the obligation of data protection by design (Article 25), the data controller should be implementing technical and organisational measures to ensure data rights keep pace with data processing, such as providing more regular access to the personal data through, for example, an API or automated data download.
>
> **Proposed Example**

IV. Data Rights are Intent-Agnostic/ Motive-Blind

115 Access rights have commonly been used in relation to highly specific pieces of information, often as part of disputes that might be related to issues of criminal,[106] employment,[107] immigration,[108] trust[109] or defamation proceedings.[110] These types of cases can create, in the words of Advocate General Bobek, 'certain intellectual unease as to the reasonable use and function of data protection rules'.[111]

116 National courts have also held specifically that data rights are purpose-blind. Courts in England and Wales have long supported the 'purpose-blind' nature of data rights.[112] The Court of Appeal of England and Wales held that there is no 'no other purpose' [than privacy or data protection] rule that requires data subjects to specify a reason for a subject access request or refrain, for example, using it for litigation.[113] Courts 'should not enquire into or permit investigation of the purpose for which a SAR has been made'.[114] The ICO has further stated that there is nothing in data protection legislation 'that limits the purposes for which a SAR may be made, or which requires the requester to tell you what they want the information for'.[115]

106 *Kololo v Commissioner of Police for the Metropolis* [2015] EWHC 600 (QB). *Lin & Anor v Commissioner of Police for the Metropolis* [2015] EWHC 2484 (QB).

107 *Ittihadieh v 5-11 Cheyne Gardens RTM Company Ltd & Ors* [2017] EWCA Civ 121.

108 Joined Cases C141/12 and C372/12 *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S* EU:C:2014:2081.

109 *Dawson-Damer & Ors v Taylor Wessing LLP* [2017] EWCA Civ 74.

110 *Rudd v Bridle & Anor* [2019] EWHC 893 (QB).

111 Case C-13/16 *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme'* EU:C:2017:43, Opinion of AG Bobek, para 93.

112 See eg *Durham County Council v D* [2012] EWCA Civ 1654 [16]; *Guriev v Community Safety Development (UK) Ltd* [2016] EWHC 643 (QB) [67]–[72]; *Dawson-Damer & Ors v Taylor Wessing LLP* [2017] EWCA Civ 74 [105]–[113]; *Ittihadieh v 5-11 Cheyne Gardens RTM Company Ltd & Ors* [2017] EWCA Civ 121 [104]–[110]; *DB v General Medical Council* (n 47) [79].

113 *Dawson-Damer & Ors v Taylor Wessing LLP* (n 112) [104]–[114].

114 *Guriev v Community Safety Development (UK) Ltd* (n 112) [70].

115 Information Commissioner's Office, 'Subject access code of

> *Arden LJ, in Dawson-Damer, stated an important general reason why access rights should not be subject to an analysis of intent noting that 'a "no other purpose" rule would have undesirable secondary consequences, such as non-compliance by data controllers with SARs on the grounds that the data subject had an ulterior purpose."*[116]

The CJEU, in *YS and Others*, did not comment on the fact that the individual was seeking to use the documents they sought in litigation as a factor which would disqualify the access right from succeeding.[117]

V. Freedom to Conduct a Business is Unlikely to Override Data Subject Rights

117 Data subject rights may effectively pit data subjects' rights, freedoms and interests against the economic freedoms of the data controller. The right of access may challenge trade secrecy, and the rights to object and erasure may conflict with various economic and property interests. From a data protection perspective, the ensuing balancing act shifts in favour of the data subject by default upon invoking said right.[118] As emphasised repeatedly by the Court,[119] at least in delisting cases the economic interests of the search engine operator are trumped by the rights, freedoms and interests of data subjects by default. This also appears from the general drafting of the GDPR, which took a rigorous 'fundamental human rights' approach, implying that 'data protection automatically trumped other interests and could not be traded-off for economic benefits.'[120]

118 The only situations where commercial interests (alone) may effectively block data subject rights, will be when accommodating these rights would affect the *essence* of a fundamental right in the Charter or at the very least not be proportionate *stricto sensu*.[121] The two most relevant fundamental rights in the present context are the freedom to conduct a business (Article 16 Charter) and the right to (intellectual) property (Article 17 Charter). Both of these have repeatedly been declared not to be absolute rights, to be considered in relation to their social function.[122] All evidence suggests that, as a general rule, they are not self-sufficient to override individual freedoms in the Charter,[123] such as the rights to privacy (Article 7), data protection (Article 8), or freedom of expression (Article 11).[124] Indeed, pursuant to Article 52(3) – which aligns Charter provisions with those in the ECHR – it would be difficult to claim economic objectives alone can constrain fundamental rights/freedoms representing essential values in a democratic society.[125] Only when, in light

practice' (n 48) 55.

116 *Dawson-Damer & Ors v Taylor Wessing LLP* (n 112) [108].

117 See generally Joined Cases C141/12 and C372/12 *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S* EU:C:2014:208.

118 After all, it is a direct expression of their informational autonomy, implicating the fundamental right to data protection in Article 8 Charter.

119 *Google Spain* (n 3); Case C507/17 *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* EU:C:2019:772.

120 Federico Ferretti, 'Data Protection and the Legitimate Interest of Data Controllers: Much Ado about Nothing or the Winter of Rights?' (2014) 51 CML Rev 843, 852. This work refers to Joined Cases C-465/00, C-138/01 and C-139/01 *Rechnungshof v* Österreichischer *Rundfunk and Others* EU:C:2003:294. See also Dorothee Heisenberg, *Negotiating Privacy* (Lynne Rienner, 2005) chapters 1–3; Viktor Mayer-Schonberger, 'Generational development of data protection in Europe', in Philip Agre and Marc Rotenberg (eds), *Technology and Privacy: The New Landscape* (MIT Press, 1997) 219–241; Spiros Simitis, 'From the market to the polis: The EU Directive on the protection of personal data' 80 Iowa Law Review (1995) 445–469.

121 Ausloos (n 70) ch 6.

122 See for example, the following cases, and the case-law cited: Case C-554/10 *Deutsches Weintor eG v Land Rheinland-Pfalz* EU:C:2012:526 [54]; Case C-101/12 Herbert Schaible v Land Baden-Württemberg EU:C:2013:661 [28]; Case C-283/11 Sky *Österreich GmbH v Österreichischer Rundfunk* EU:C:2013:28 [45].

123 See similarly: Peter Oliver, 'The Protection of Privacy in the Economic Sphere before the European Court of Justice' (2009) 46 Common Market Law Review 1443, 1481.

124 Serge Gutwirth, 'De Toepassing van Het Finaliteitsbeginsel van de Privacywet van 8 December 1992 Tot Bescherming van de Persoonlijke Levenssfeer Ten Opzichte van de Verwerking van Persoonsgegevens' [The Application of the Purpose Specification Principle in the Belgian Data Protection Act of 8 December 1992]' (1993) 1993 Tijdschrift voor Privaatrecht 1409, 1431.1431."","plainCitation":"Serge Gutwirth, 'De Toepassing van Het Finaliteitsbeginsel van de Privacywet van 8 December 1992 Tot Bescherming van de Persoonlijke Levenssfeer Ten Opzichte van de Verwerking van Persoonsgegevens' [The Application of the Purpose Specification Principle in the Belgian Data Protection Act of 8 December 1992]' (1993 Some call the rights in Article 16–17 of the Charter 'peripheral rights' that are always overridden by data protection rights. See eg Hielke Hijmans, 'The European Union as a Constitutional Guardian of Internet Privacy and Data Protection' (PhD Thesis, University of Amsterdam 2016) 196, 216–17, 258.

125 Paul P Craig and Gráinne De Búrca, EU law: text, cases,

of Article 52(1), a specific legal provision ordains processing for commercial purposes and/or raises obstacles to invoke certain data subject rights, does it seem realistic that a controller can legitimately *not* accommodate data subject rights purely on the basis of commercial interests.[126]

119 In relation to this, attention should be given to a decision by the Supreme Court of the Netherlands, which did not accept exemptions based on a claim by a company that received requests based on alleged harm to their freedoms or rights. In *Dexia*[127] it did not accept three instances of this argument. First the high cost associated with responding to a single access is not (in itself) a reason to exempt access. Second, the fact that an organisation may receive a high number of requests is not accepted as a reason to restrict access. Third, the fact that data subjects have been incited to use their rights by a consumer protection programme and have made use of a request template provided by that programme cannot be invoked.

VI. Rights a Controller Expects to Refuse Must be Flagged as per Arts 13/14/25

120 An important, but underappreciated, aspect of the GDPR is found in the parts of Articles 13–15 which require data controllers to declare the existence of certain GDPR rights.[128] These parts have usually been interpreted as copy-pasting the GDPR into, say, a privacy policy. It is quite clear however, that in some cases, in respect to some data, these rights exist, and in other cases, they do not exist. As a result, this can only be interpreted as a contextual provision which requires consideration of the ability for these rights to be exercised in a data subject's specific situation.

121 While the data controller should be flagging these rights to facilitate the data subject's awareness and use of them — a common EU law trope found in areas such as airline and rail delay rights[129] — this is not the only role of this provision. Given that the data subject often (although not always) has a choice as to whether to engage with a data controller, such as putting themselves to actively consent to processing or contract with the controller, or to move within a zone where processing on the basis of, for example, legitimate interests is likely to occur, the purpose of the GDPR's information rights is to provide information to help the data subject decide whether they wish to enable such data processing. **A core piece of that information is whether that specific processing can be objected to, erased, ported or accessed.**[130]

122 The data controller should have pre-empted how to deal with rights in relation to all data they process, and the principles of fairness and transparency require that this information be provided ahead, read in line with the specific requirements of Article 13-14 not subsequent to processing. Furthermore, as there will be times where individuals have not been informed of their rights under either Article 13 or 14,[131] the data controller should be prepared to reveal this information upon request under Article 15.[132]

and materials (Oxford Univ Press 2011) n 221. Gutwirth (n 124) 1430–31; Orla Lynskey, 'Regulating "Platform Power"' (Working Paper, LSE Legal Studies Working Paper, LSE 21 February 2017) 25–26; Hijmans (n 124) 258. The last author refers to Craig and De Búrca who explain that permitting economic objectives to limit the scope of fundamental rights, would go against ECHR jurisprudence. See: Paul P Craig and Gráinne De Búrca, EU law: text, cases, and materials (Oxford Univ Press 2011) n 221.

126 This can be the case, for example, when the controller can invoke a legal obligation to process the personal data as a lawful ground (GDPR, art 6(1)(c)) and/or as an exemption to the right to erasure (GDPR, art 17(3)(b)). Regardless, further processing in this context will be constrained to what the legal obligation requires only (again reiterating the importance of the need for a granular approach).

127 *Hoge Raad* (29 June 2007) NL:HR:2007:AZ4663; *Hoge Raad* (29 June 2007) NL:HR:2007:AZ4664.

128 GDPR arts 13(2)(b), 14(2)(c), 15(1)(e).

129 Regulation (EC) No 261/2004 of the European Parliament and of the Council of 11 February 2004 establishing common rules on compensation and assistance to passengers in the event of denied boarding and of cancellation or long delay of flights, and repealing Regulation (EEC) No 295/91 (Text with EEA relevance) OJ L 46/1, art 14; Regulation (EC) No 1371/2007 of the European Parliament and of the Council of 23 October 2007 on rail passengers' rights and obligations OJ L 315/14, art 29.

130 See generally Veale and others (n 68) 118.

131 Such as in the situations envisaged in GDPR, art 14(5)(b) ('the provision of such information proves impossible or would involve a disproportionate effort').

132 GDPR, art 15(1)(e).

A data controller in response to an Article 15 request informs the data subject, by data category and processing purpose, where the right to request rectification, erasure, restriction or objection exists. Where no possibility for a request exists — such as the lack of right to object to data necessary for a contract, such as credit card data processed for the purposes of fulfilling a future payment, the data controller makes this clear in their response.

Proposed Example

J. Verifying Data Subjects

123 Verification of data subjects is an important part of exercising data rights, however academic research and the authors' experience show that verification approaches taken by many data controllers today are not compliant with the principles of the GDPR.[133]

I. Authentication should not be an unnecessary obstacle to data subject rights

124 Many controllers engage in singling-out of the data subject for the purpose of service delivery or analysis but have not built a system with which to identify data subjects for the purposes of exercising their rights. In some cases, they simply refuse to build a system that can be accessed by the user, despitehaving access *to* the specific user and device from their server.[134] Examples of this are documented by two of the authors in a recent academic paper.[135]

125 In other cases, such as in the case of wireless analytics or targeting advertising, data controllers have established a system where their business model can operate with imprecise targeting or singling out of individuals (which nonetheless is highly individualised over time). The impact of this imprecise, but personalised targeting is that the data controller can claim that providing data rights would be imprecise too, but the consequences of doing so would be in breach of the security principle, and therefore not something they are willing to countenance.[136]

126 In cases where, by design or not, verification is imperfect, **data controllers must take a realistic risk-based approach to release, which does not disempower data subjects**. In many cases, the impact of accidental release of data to someone other than the data subject, *particularly where the data subjects are inherently difficult to identify*, will be low, and possible to monitor on an aggregate level.

II. Rights-Dependent Verification Burden

127 Different rights have different levels of consequence for data subjects if they are applied by mistake or fraudulently. For example, the rights of access and portability can lead to sensitive data disclosure, and it is important that verification is an effective and secure process.[137]

128 Other rights, such as erasure, restriction and objection are more contextual in nature. Misapplied erasure might, for certain kinds of data, result in an inability for the genuine data subject to establish or substantiate legal claims, or affect the availability of services, or cause the loss of important personal data. Yet for many kinds of data which already have limited storage retention, erasure will merely hasten deletion which should have occurred anyway. For example, the impact on an individual's rights and freedoms of the incorrect erasure of web-tracking data, or app telemetry data, is significantly lower than the impact of accidental disclosure of this data.

129 The lack of negative consequences for the data subject is perhaps most stark where the data is being processed on the basis of legitimate interests of the data controller, as the individual did not explicitly request this processing be carried out, and therefore in many cases their interest in the processing will be minimal.

130 Where the right to object is being applied, as the data are still being stored but simply not processed for the objected-to purposes, the process is generally reversible in the case that verification was incorrect. **As a result, the right to object or to restrict processing should, in general, require a lower burden of verification than access and erasure. The Guidance should also lay out the**

133 Coline Boniface and others, 'Security Analysis of Subject Access Request Procedures How to Authenticate Data Subjects Safely When They Request for Their Data' [2019] Annual Privacy Forum, Jun 2019, Rome, Italy.

134 See eg Veale and others (n 68); Chris Norval and others, 'RECLAIMING Data: Overcoming App Identification Barriers for Exercising Data Protection Rights' in *Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers* (UbiComp '18, New York, NY, USA, ACM 2018).

135 See Veale and others (n 68).

136 See eg the example of Transport for London in ibid.

137 See generally Andrew Cormack, 'Is the Subject Access Right Now Too Great a Threat to Privacy?' (2016) 2 European Data Protection Law Review 15.

circumstances in which the right to erasure should require less of a burden of verification than the right of access. In particular, the controller should need to demonstrate, in accordance with the principles of accountability and fairness, compelling reasons as to why they are requesting detailed verification from a data subject for the right to object.

III. Verifiability, Fairness and Data Protection by Design

131 The GDPR's risk-based approach, and its by-design approach, are not currently widely recognised and followed in relation to verification systems for data rights. The method used for authentication should be proportionate to avoid abusive identity checks.[138] For example, controllers such as information society services, which due to users explicitly requesting the service often have login credentials or an existing verification system, should not, in general, require a higher level of verification. **If controllers request a higher level of verification than required to access the service, they must justify this in relation to the accountability and fairness principles, and minimise both the burden on the user (in line with 'efficient and timely protection') and personal data processed (in line with data minimisation) in the process.**

132 Furthermore, **data controllers often ask for a government issued identification document in situations where it is clearly disproportionate**. In many cases, for example when an individual is seeking data connected to an identifier (eg a cookie ID) and the controller has no knowledge of the real identity of the data subject, it is unclear what purpose the government ID serves. Moreover, asking for a government ID entails unnecessary risk as data controllers may not have secure systems set up to receive such data, and often in the authors' experience request it through email. Furthermore, in many cases, a data subject will be requesting data on the basis that they do not trust the data controller, and wish to consider their options in terms of eg objection, erasure or the withdrawal of consent. In these cases, the need to provide sensitive data to the data controller may be unfairly dissuading data subjects from exercising their rights. Some recommendations of national DPAs recommend controllers to request a government ID. **The Guidance should make clear that a government-issued ID should only be required when this is proportionate.** This would also provide reassurance to data controllers who may feel obliged to ask for such information.

138 Boniface and others (n 133).

K. Concluding Remarks

133 In this document we have laid out our understanding – considering case-law, the provisions and the regulatory guidance thus provided – of the extent of data rights and the context in which they must operate. There are strongly held views on the matter, not least from industry, but these must be very carefully considered in light of the fundamental rights framework underpinning data protection. The system of data rights is both intrinsically important and key as an enabler of the entire data protection regime. They are going to be more important than ever in the years to come in mitigating the power asymmetries that have emerged, and in many cases appear to be worsening, between individuals and their representations in data. The Guidance therefore should ensure data rights are the strong tools the text and case-law intend them to be, in order to uphold fundamental rights in the information age.

Coordinating Academics:

***Jef Ausloos**, Postdoctoral Researcher*

Institute for Information Law, University of Amsterdam

***René Mahieu**, PhD Candidate*

Law, Science, Technology & Society (LSTS), Vrije Universiteit Brussel

***Michael Veale**, Lecturer in Digital Rights & Regulation*

Faculty of Laws, University College London and the Alan Turing Institute