Northern Ireland
Legal Quarterly
Summer Vol. 73 No. 2 (2022) 310–340
Article DOI: 10.53386/nilq.v73i2.962

On the compatibility of pandemic data-driven measures with the right to data protection: a review of 'under-the-radar' measures adopted in Ireland to contain COVID-19

Maria Grazia Porcedda

Trinity College Dublin*

Correspondence email: maria-grazia.porcedda@tcd.ie

ABSTRACT

This article reviews the compatibility of 'under-the-radar' data-driven measures adopted in Ireland to contain the COVID-19 pandemic with data protection law. Since data protection law implements and gives substance to the right to the protection of personal data enshrined in article 8 of the Charter of Fundamental Rights of the European Union, the article reviews the compatibility of data-driven measures with the applicable law in light of the Charter. The measures reviewed – thermal scanner guns, health self-check forms, Statutory Instruments for contact logging and the Vaccine Information System – appear well-meaning but partly incompatible with the right to data protection. The analysis points to the difficulty of reconciling public health and data protection without a systematic data-processing strategy and concludes with recommendations for right-proofing data-driven measures in the guise of a blueprint strategy for processing personal data for present and future pandemic purposes.

Keywords: fundamental right to protection of personal data; judicial review; legality; COVID-19 pandemic; data-driven measures; contact logging; vaccine information system; travel.

* Trinity College Dublin, School of Law, House 39, Trinity College Dublin, Dublin 2: Orcid 0000-0002-9271-3512. I wish to express my gratitude to Cian Henry and Ms Kate Heffernan for research assistance while drafting the public policy report from which this article was drawn, as well as Dr David Fennelly, the editors of the special issue and anonymous reviewers for the helpful comments on various drafts. All errors are mine. The law is correct as stated as of early July 2021. Research for this article was supported by Trinity College Dublin funding in the context of the COVID-19 Law and Human Rights Observatory and a public report appeared as Róisín A Costello, David Fennelly and Maria Grazia Porcedda, 'Data Protection and the Covid-19 Pandemic' (Covid-19 Law and Human Rights Observatory 2021).

INTRODUCTION

Since the beginning of the pandemic, policymakers in the European Union (EU) have adopted several data-driven measures to contain the spread of COVID-19. The 'comprehensive public health strategy to fight the pandemic'[1] was to include purpose-built technologies, off-the-shelf and even manual measures for locating infectious individuals in highly mobile societies, performing the necessary contact tracing to break the chain of infection and carrying out research to improve the response to the pandemic. Examples of purpose-built technologies include COVID-19 apps,[2] such as Ireland's COVID Tracker App,[3] Digital Green Certificates,[4] contact management systems and vaccine information systems (VISs). Off-the-shelf technologies are used, among others, in the context of return-to-work schemes, and manual measures include contact-logging by individuals and organisations.

Most data-driven measures rely on the processing of personal data and, therefore, trigger the question of how to reconcile the use of data for public health purposes with the right to the protection of personal data enshrined in article 8 of the Charter of Fundamental Rights (CFR) of the EU.[5] Yet, the question was publicly discussed primarily with respect to COVID-19 apps[6] on account of their potential for surveillance on a mass scale,[7] which creates the type of power imbalance that data protection legislation – and the multilevel system of human rights protection shared by EU member states – seeks to

1 European Data Protection Board (EDPB), 'Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak' (EDPB 21 April 2020).

2 European Commission, 'Communication from the Commission: guidance on apps supporting the fight against COVID 19 pandemic in relation to data protection' C 124 I/1 (European Commission 17 April 2020).

3 Health Safety Executive (HSE), 'HSE launch the COVID Tracker App' (HSE 7 July 2020). On the Irish app, see Fennelly (n ✳ above) ch 2.

4 EDPB-EDPS, Joint Opinion on the Digital Green Certificate (31 March 2021).

5 Charter of Fundamental Rights of the European Union [2010] OJ C 83/389.

6 Early responses in Ireland: Rónán Kennedy, 'Data protection and COVID-19: short-term priorities, long-term consequences' (*Bloomsbury Professional Ireland* 8 May 2020); Trinity College Dublin Covid-19 Law and Human Rights Observatory. Early responses in Europe, among many: Valsamis Mitsilegas, 'Responding to Covid-19: surveillance, trust and the rule of law' (*QMUL School of Law Blog*, 26 May 2020); Vincenzo Zeno-Zencovich, 'I limiti delle discussioni sulle "app" di tracciamento anti-Covid e il futuro della medicina digitale' (*Media Laws* 26 May 2020); Oskar J Gstrein and Andrej Zwitter, 'Using location data to control the coronavirus pandemic' (*VerfBlog* 20 March 2020).

7 Lily Kuo, '"The new normal": China's excessive coronavirus public monitoring could be here to stay' *The Guardian* (London, 9 March 2020); Patrick Wintour, 'Coronavirus: who will be winners and losers in new world order?' *The Guardian* (London, 11 April 2020).

prevent.[8] Public discussion was certainly beneficial,[9] though apps were unlikely to become mandatory in light of regulatory constraints (see below). Other commonplace, and often mandatory, data-driven measures have instead gone under the radar and, consequently, eluded public scrutiny. Examples of under-the-radar measures include low as well as high-tech solutions ranging from contact-logging to the VIS.

This article discusses the legality of such under-the-radar measures from a data protection law perspective. Health policy and the delivery of health services is a primary responsibility of member states (article 168 Treaty on the Functioning of the European Union), who retain the privilege to introduce more specific provisions to adapt the application of EU data protection law in this area. Therefore, this article discusses the results of an appraisal of levels of compliance with data protection law of select data-driven measures that were adopted in Ireland to contain the spread of COVID-19 from summer 2020 through to summer 2021.[10] Data protection law, including the General Data Protection Regulation (GDPR)[11] and other relevant instruments, is understood here not only as a source of regulatory compliance, but also as the implementation of the right to the protection of personal data enshrined in article 8 of the CFR.[12] I refer to such a blend of regulation and rights as the dual nature of data protection law and appraise compliance with the applicable law in light of the CFR.

Given the dual nature of data protection law, the perspective adopted in this article is one of reconciliation between equally important objectives. Mass surveillance is an undesirable goal, as

8 Eg Christopher Docksey and Christopher Kuner, 'The coronavirus crisis and EU adequacy decisions for data transfers' (*European Law Blog* 3 April 2020); Elif Mendos Kuskonmaz and Elspeth Guild, 'Covid-19: a new struggle over privacy, data protection and human rights?' (*European Law Blog* 4 May 2020). Interestingly, the public and academic debate has overlooked apps deployed by employers to locate workers attending the workplace during the pandemic.

9 Apps' data protection shortcomings were quickly redressed thanks to the swift intervention of expert and policy communities. In Ireland, see on the Irish Council for Civil Liberties, Eoin O'Dell, 'Principles for legislators on the implementation of new technologies' (*Cearta* 29 April 2020); HSE Ireland/covid-tracker-app (GitHub); European Commission (n 2 above).

10 For a review of measures adopted between March and August 2020, see Maria Grazia Porcedda, 'Data protection implications of data driven measures adopted in Ireland at the outset of the Covid-19 pandemic' (2021) 7(2) *European Data Protection Law* 260–269.

11 Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such data, and Repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

12 Eg Judgment of 15 June 2021, *Facebook Ireland and Others*, Case C-645/19, ECLI:EU:C:2021:483, para 45.

is a blanket prohibition against the processing of personal data to contain the pandemic. Ultimately, the challenge lies in designing a data-processing strategy that avoids the pitfalls of a zero-sum clash between public health and data protection.[13] As the Data Protection Commission (DPC) stated, data protection law 'does not stand in the way of the provision of healthcare and the management of public health issues'.[14] This is because the protection of personal data is a qualified right (alongside article 7 of the CFR protecting privacy),[15] whose enjoyment can be limited in line with article 52(1) of the CFR, provided the essence of the right is preserved. As the European Data Protection Board (EDPB) stated in a letter to Hungary in June 2020:

> Restrictions … to the extent that they void a fundamental right of its basic content cannot be justified. If the essence of the right is compromised, the restriction must be considered unlawful, without the need to further assess … the necessity and proportionality criteria.[16]

To begin with, I establish criteria to assess the compatibility of measures that collect personal data in light of the applicable data protection law by reading the rules enshrined in secondary law instruments in the context of the CFR, case law and authoritative guidance. I then discuss the extent to which sample data-driven measures, including measures that collect health data, comply with the applicable law and potentially interfere with article 8. In particular, I will demonstrate that thermal scanner guns may engender an overlooked interference with the right to data protection; self-check forms rest on weak legal bases; the quality of Statutory Instruments (SIs) for contact logging and locator

13 Department of Health, 'Ethical framework for decision-making in a pandemic' (17 April 2020); Andrea Mulligan, 'The ethics of lockdown: transparency, accountability and community involvement (COVID-19 Law and Human Rights Observatory 15 July 2020); European Union Agency for Fundamental Rights (EUFRA), 'Fundamental rights implications of Covid-19' (EUFRA 2020); Amedeo Santosuosso, 'La regola, l'eccezione e la tecnologia' (2020) 1 BioLaw Journal – Rivista di BioDiritto Special 609. The debate recalls in many ways the 'security v liberties' debate that dominated the post 9/11 legal order. My opinion on the need to avoid trade-offs understood as zero-sum games is illustrated in Maria Grazia Porcedda, 'Recrudescence of "security v privacy" after the 2015 terrorist attacks, and the value of "privacy rights" in the European Union' in Elisa Orrù, Maria Grazia Porcedda and Sebastian Weydner-Volkmann, *Rethinking Surveillance and Control: Beyond the 'Security versus Privacy' Debate* (Nomos 2017).

14 DPC, 'Data protection and COVID-19' (*DPC Blogs* 6 March 2020).

15 This piece does not explicitly review the impact of measures on the right to private life enshrined in art 7 CFR. Among others reviewing private life implications is Elspeth Guild, 'Covid-19: European rules for using personal data' (*QMUL School of Law Blog* 4 June 2020).

16 'Statement on restrictions on data subject rights in connection to the state of emergency in Member States' (EDPB 2 June 2020).

forms is unsatisfactory; the VIS potentially has unnecessary elements; and many measures could potentially interfere with the essence of data protection. These results show that the response to the pandemic was well meaning but potentially unsound, and they stress how difficult it can be to reconcile public health and data protection without a systematic data-processing strategy.[17] On this account, I conclude with recommendations for right-proofing data-driven measures for present and future pandemics.

COMPATIBILITY OF DATA-DRIVEN MEASURES WITH THE FUNDAMENTAL RIGHT TO DATA PROTECTION: CRITERIA FOR ANALYSIS

The compliance of data-driven pandemic measures with data protection law must be assessed in light of the CFR,[18] which enjoys the same legal status as the treaties and is applicable by virtue of articles 29.4–29.6 of the Constitution of Ireland.[19] The CFR's scope of application is as broad as the scope of EU law,[20] so it must be respected even when member states need to derogate from EU law: namely, at times of emergency,[21] such as the COVID-19 pandemic. As a result, the processing of personal data for pandemic purposes can benefit from lawful limitations to the exercise of the rights of data subjects, as set out in article 52(1) of the CFR and the applicable law, for example article 23(1)(e) of the GDPR and section 60 of the Irish Data Protection Act 2018[22] (DPA 2018). In the following, I conceptualise the criteria for the analysis of the compatibility of data-driven measures with Irish data protection law.

17 Department of Health (n 13 above); Mulligan (n 13 above); EUFRA (n 13 above); Santosuosso (n 13 above).

18 Judgment in *Österreichischer Rundfunk*, C-465/00, C-138/01 and C-139/01, EU:C:2003:294, para 68.

19 Mr Justice John L Murray, 'Review of the Law on the Retention of and Access to Communications Data' (April 2017) 55.

20 Opinion of 10 January 2019 of AG Szpunar in *Google LLC v CNIL*, Case C-507/17, EU:C:2019:15, para 55.

21 Judgment of 17 December 2015 in *Åkerberg Fransson*, C-617/10, EU:C:2013:105, para 29.

22 Data Protection Act 2018; Maria Helen Murphy, 'The Irish adaptation of the GDPR: the Irish Data Protection Act 2018' in K Mc Cullagh, P Tambou and S Bourton (eds), *National Adaptations of the GDPR* (Collection Open Access Book/Blog droit européen 2019); Rónán Kennedy and Maria Helen Murphy, *Information and Communications Technology Law in Ireland* (Clarus Press 2017) 97–130.

Permissibility of data-driven measures: criteria for analysis of data-driven measures

The Court of Justice of the European Union (CJEU) has consistently said that the processing of personal data that falls within the scope of EU data protection law constitutes an interference with the right to the protection of personal data.[23] To review the compatibility of data-driven measures with the applicable law in light of the CFR means considering the permissibility of such an interference in light of the boundaries drawn by a variety of sources that affect the interpretation of the applicable law. These include, first and foremost, article 52(1) of the CFR, the case law of the CJEU in landmark cases such as *Digital Rights Ireland*[24] and of the European Court of Human Rights (ECtHR), as well as guidance by the European Data Protection Supervisor (EDPS) and the European Data Protection Board (EDPB) in light of CJEU and ECtHR case law. The analysis follows the approach of the EDPS in its Toolkit on necessity[25] and Guidelines on proportionality.[26] There, the EDPS outlines a 'methodology' developing the 'macro-criteria'[27] contained in article 52(1) 'to better equip EU policymakers and legislators responsible for preparing or scrutinising measures that involve the processing of personal data and limit the rights to protection of personal data and to privacy' and thus 'help with the assessment of compliance of proposed measures with EU law on data protection'.[28]

The assessment of compliance, which must follow 'the required order of the lawfulness assessment'[29] of an interference, begins with establishing the existence of an interference with the right, followed by the presence of a legal basis. If such a legal basis exists, according to article 52(1) the essence, that is the very substance, must not be infringed.[30] The interference must then be justified in light of objectives of general interest recognised by the EU, following which

23 Eg Judgment of 3 October 2018 in *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2018:788, para 51. A poignant criticism of this approach can be found in the work of Maria Tzanou, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-terrorism Surveillance* (Hart 2017).

24 Judgment of 8 April 2014 in *Digital Rights Ireland and Seitlinger and Others*, Joined Vases C-293/12 and C- 594/12, EU:C:2014:238, paras 35–46.

25 Assessing the Necessity of Measures that Limit the Fundamental Right to the Protection of Personal Data: A Toolkit (EDPS 2017).

26 EDPS, 'Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data' (25 February 2019).

27 Ibid 5.

28 Ibid 4.

29 Ibid 7.

30 *Digital Rights Ireland* (n 24 above) paras 39–40.

come the necessity and proportionality tests. Thus, in my analysis, I use the 'macro-criteria' contained in article 52(1) of the CFR to outline the relevant components of the applicable law. This process is then followed by an appraisal of compliance of data-driven measures with data protection law.

Interference with the right to personal data protection

As stated above, processing that involves personal data falling within the scope of data protection law constitutes an interference. The following section clarifies when data-driven measures use personal data and thus fall within the scope of the applicable law.

Are data-driven measures based on personal data?

The starting point is to ascertain whether measures process personal data, as otherwise the right is not at stake. Not all pandemic measures process personal data, meaning information relating to a natural living person that either identifies them, or makes them identifiable when combined with other pieces of information (article 4(1) GDPR). Here lies a catch in data protection law; the growing pool of data available, alongside improved data science and statistical techniques, keeps broadening the scope of 'identifiable' data[31] and narrowing the scope of the antonym, 'anonymous' data.

Data that are anonymous on their own, such as those captured by motion sensors,[32] may allow for the identification of a natural person in combination with data from other sources, thereby becoming personal. The same applies to anonymised data, namely information that no longer enables the identification of an individual. Anonymised data are outside the scope of the applicable law, provided data subjects are not re-identified. When information enabling the re-identification of individuals is kept separate but is still available to the controller, data are considered to be pseudonymised (article 4(5) GDPR) and subject to the applicable law.

Recital 26 GDPR conveys an understanding of 'anonymity' as dependent on 'objective factors' that determine 'all the means reasonably likely to be used' by the controller or any other person to identify the data subject, and thus relative in nature. This provision

31 Nadezhda Purtova, 'The law of everything: broad concept of personal data and future of EU data protection law' (2018) 10 Law, Innovation and Technology 40.

32 Examples include devices to monitor the maximum number of people who can fit in a room or beepers that emit signals to help individuals maintain the desired physical distance.

is very close to recital 26 of repealed Directive 95/46,[33] which was interpreted in *Patrick Breyer*.[34] There, the court followed the systematic interpretation by AG Campos Sanchez-Bordona,[35] whereby 'reasonable' means are those within the framework of the law, provided they are lawful, and include the transfer of data from third parties in possession of additional information enabling identification. Although the law applicable to *Patrick Breyer* was Directive 95/46, the continuity between recital 26 of Directive 95/46 and the GDPR[36] suggests the court's interpretation is still relevant. For instance, in its COVID-19 Guidelines, the EDPB refers to a 'reasonability test' based on objective and contextual aspects and suggests that the robustness of anonymisation can be measured using three criteria: singling-out, linkability and inference.[37]

The legal and practical limits of anonymisation cannot be overstated. Data processed for research purposes (explicitly mentioned in recital 26 GDPR) to block COVID-19,[38] as foreseen by the VIS, are likely to fall into the category of anonymised data and are therefore susceptible to re-identification. Another example of seemingly anonymous data, those collected by non-contact thermometers, can soon take on the nature of personal data (see below).

Does the processing fall within the scope of data protection law?

Personal data-driven measures are amenable to data protection law when they fall within its material and territorial scope (articles 2 and 3 GDPR). A departure from these rules is the household exception (article 2(1)(c) GDPR), whereby information collected 'by a natural

33 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data (Data Protection Directive) [1995] OJ L 281.

34 Judgment of 19 October 2016 in *Patrick Breyer*, Case C-582/14, ECLI:EU:C:2016:779.

35 Opinion of 12 May 2016 of AG Campos Sanchez-Bordona in *Patrick Breyer*, Case C-582/14, ECLI:EU:C:2016:339, paras 68–73.

36 But the GDPR may offer 'a more liberal conceptualisation of anonymised information'. See Triin Siil and Dan Bogdanov, 'Anonymisation 2.0: Sharemind as a tool for de-identifying personal data' (*Sharemind* 17 August 2018).

37 EDPB (n 1 above) 5.

38 Gianclaudio Malgieri, 'Data protection and research: a vital challenge in the era of COVID-19 pandemic' (2020) 37 Computer Law and Security Review 37; EDPB, 'Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak' (EDPB 21 April 2020). In Ireland: SI 314/2018 – Data Protection Act 2018 (Section 36(2)) (Health Research) (Amendment) Regulations 2019.

person in the course of a purely personal or household activity' is not subject to data protection law. However, when individuals make such information available publicly (for example online), the household exception no longer applies, turning individuals into data controllers within the scope of the GDPR.[39]

The GDPR and the DPA 2018, which contains provisions pursuant to articles of the GDPR that require legislative intervention by member states' law, will apply in most cases.[40] The GDPR and DPA 2018 are particularised and complemented[41] by two *leges speciales* transposed into Irish law. The first is the Law Enforcement Directive for processing for law enforcement purposes.[42] The second is the ePrivacy Directive (EPD),[43] which applies to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the EU and, insofar as article 5(3) is concerned, information society services (ISSs).[44]

EDP rules on the processing of traffic and location data[45] and of information stored in the terminal equipment of users[46] are the reason why COVID-19 apps could not be forced on people to automate contact

39 Judgment of 14 February 2019 in *Sergejs Buivids*, C-345/17, ECLI:EU:C:2019:122, para 43; Judgment of 11 December 2019 in *TK v Asociaţia de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, para 55.

40 A&L Goodbody, 'Contact tracing apps – a privacy primer', Focus on Covid-19 (2020).

41 *Ministerio Fiscal* (n 23 above) para 31.

42 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of such Data, and Repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/89; transposed into Irish law by the DPA 2018.

43 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector [2002] OJ L 201 (E-privacy Directive), as updated in 2009; transposed into Irish law by SI 336/2011.

44 EDPB (n 1 above). Commented by S Guida, 'The European Data Protection Board's position on the processing of personal data in the context of Covid-19' (2020) 6(2) European Data Protection Law Review 262–264.

45 Arts 2(b) and 2(c) EDP, the latter: 'Any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user' of such a service.

46 To the extent that Covid-19 apps are amenable to ISSs, app providers could only place data in the terminal equipment and access data located therein with user consent. A thorough discussion as to whether Covid-19 apps fall in the definition of an ISS is beyond this paper. See Judgments of 20 December 2017, *Asociación Profesional Elite Taxi* C-434/15, EU:C:2017:981 and of 3 December 2020, *Star Taxi App*, C-62/19, EU:C:2020:980.

tracing. Providers of electronic communication services, including but not limited to Telcos, can only collect traffic and location data for the purposes specified in articles 6 and 9, with location data only to 'be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service'.

Article 15 EPD enables the restriction of the scope of rights and obligations contained in articles 5, 6 and 9, but only for a strictly enumerated[47] list of objectives, a list which does not include public health. As a result, instruments adopted *qua* exception pursuant to article 15 EPD, including the now invalidated Directive 2006/24/EC, could not, on their own, help in the health response to COVID-19, but only its public security dimension.[48] Following *Ministerio Fiscal*, access to targeted and limited data is likely to be permissible for the fight against criminal offences that are not serious – an assessment that is for the referring court to make.[49] This could include the prosecution of violation of self-isolation measures by single individuals, insofar as they constitute an offence. It is unlikely, however, to include the monitoring of individuals for the sake of preventing the breaking of self-isolation measures.

In a development that deserves to be watched closely, the draft regulation set to repeal the EPD[50] makes provisions for processing traffic and location data to protect the vital interest of a natural person,[51] which 'may include for instance processing necessary for humanitarian purposes, including for monitoring epidemics'.[52] The GDPR and DPA 2018 are the relevant pieces of applicable law for data-driven measures reviewed in the second half of this article.

Whether the interference is in accordance with the law

The criterion to be 'in accordance with the law' refers to the need for (i) a legal basis (lawfulness) that (ii) meets parameters of quality (legality)

47 '... the list of objectives ... is exhaustive, as a result ... access must correspond, genuinely and strictly, to one of those objectives': *Ministerio Fiscal* (n 23 above) para 31.

48 Following judgment of 21 December 2016 in *Tele 2 Sverige*, Joined Cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, para 102, only serious crime justifies the retention of traffic and location data.

49 *Ministerio Fiscal* (n 23 above) paras 53–57.

50 Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Mandate for negotiations with EP, Brussels, 10 February 2021 (2017/0003(COD)).

51 Ibid art 6b(1)(d).

52 Ibid recital 17a.

developed by the court and often borrowed from the ECtHR, in recognition of the Council of Europe's leading role on the rule of law.[53] Data protection legislation contains rules on lawfulness of processing and legality drawn from the rule of law, starting with the principles enshrined in article 5 GDPR – lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, and integrity and confidentiality – which apply to the processing of any personal data.[54] For instance, the principles of lawfulness, fairness and transparency enshrined in article 5(1)(a) GDPR can be said to stem from the rule of law.[55] Many of these principles become actionable as rights of the data subjects and corresponding obligations of the data controller.

The GDPR also embodies a form of legality in that the data controller, the entity who decides the means and purposes of the processing, must have a lawful basis to act (articles 6 and 9 GDPR). The data controller has responsibility, *de facto* and *de jure*,[56] for fulfilling the data protection principles, in the form of technical and organisational measures commensurate with the risks entailed by the processing (article 24 GDPR). In other words, in order to benefit from the processing, the controller must safeguard the data so as to protect the data subjects concerned[57] – which turns the data controller into the *de facto* gatekeeper for data subjects' rights.

Legal basis for the processing of personal data within data-driven measures and determination of the controller

The Irish DPC notes that processing personal data for the sake of containing pandemics can take place under different legal bases.[58] For instance, 'where organisations are acting on the guidance or directions of public health authorities, or other relevant authorities' data concerning health can be processed based on article 9(2)(i) GDPR

53 Judgment of 6 October 2020 in *La Quadrature du Net and Others*, C-511/18, ECLI:EU:C:2020:791, para 103.

54 Combined reading of the Judgment of 29 June 2010 in *Bavarian Lager Ltd*, C-28/08 P, ECLI:EU:C:2010:378, para 61 and Judgment of 13 May 2014 in *Google Spain and Google*, C-131/12, EU:C:2014:317, para 96.

55 Lee A Bygrave, *Data Privacy Law: An International Perspective* (Oxford University Press 2014).

56 The responsibility of the controller is commensurate to their role in the processing, Judgment of 24 September 2019 in *GC, AF, BH, ED v Commission nationale de l'informatique et des libertés* (CNIL), Case C-136/18, ECLI:EU:C:2019:772, para 46.

57 Eg Judgment of 5 June 2018 in *Wirtschaftsakademie Schleswig-Holstein*, Case C-210/16, ECLI:EU:C:2018:388, para 28; *GC, AF, BH, ED* (n 56 above) para 43.

58 DPC (n 14 above).

and section 53 DPA 2018.[59] Employers must protect their employees under the Safety, Health and Welfare at Work Act 2005, which, together with article 9(2)(b) GDPR, provides a legal basis to process personal data concerning health.[60] Either way, suitable safeguards need to be implemented, for instance as laid down in section 36 DPA 2018. Furthermore, in case of emergency, protection of the vital interest of a data subject in line with articles 6(1)(d) and 9(2)(c) GDPR can act as a legal basis.

Consent (article 6(1)(a) GDPR) and the legitimate interests pursued by the controller (article 6(1)(f) GDPR) are unlikely to constitute valid bases for processing information other than data concerning health for pandemic purposes, a point shared by some, but not all, commentators.[61] Individuals are unlikely to agree to the required measures in a freely given, specific, informed and unambiguous manner; there is too much of a power imbalance between those requesting consent and data subjects. The legitimate interest basis is also unsuitable for its weakness vis-à-vis the interests or fundamental rights and freedoms of the data subject as per the interpretation of the court in *Rīgas satiksme*[62] and article 6(1)(f) GDPR.[63]

The most suitable bases for public authorities are article (6)(1)(e) GDPR and section 38 DPA 2018; these are necessary for either the exercise of official authority vested in the controller or the performance of a task carried out in the public interest. Private entities supporting the Health Service Executive (HSE) contact-tracing effort through contact logging could, in theory, be seen as performing a specific task carried out in the public interest, but the GDPR requires this legal basis to apply only when laid down in member state (or EU) law to which the controller is subject (articles 6(3) and 6(2), recitals 10 and 45). Although there is no need for 'a specific law for each individual processing' and 'a law as a basis for several processing operations … may be sufficient' (recital 45), such 'law' has to comply with the requirements of a legal measure (e.g. recital 41). This begs the question of what role private

59 See Costello in Costello et al (n ✳ above) ch 3.

60 For the UK, see Ruby Reed-Berendt and Edward Dove, 'Healthcare Workers' Data and Covid-19 Research' (UK-Reach Project 2020).

61 Kennedy (n 6 above).

62 According to the CJEU, there are 'three cumulative conditions so that the processing of personal data is lawful, namely, first, the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the fundamental rights and freedoms of the person concerned by the data protection do not take precedence': Judgment of 4 May 2017 in *Rīgas satiksme*, C-13/16, ECLI:EU:C:2017:336.

63 'Such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.'

individuals or entities have when logging contacts for the benefit of the HSE COVID-19 contact-tracing programme. The adoption of an officially published instrument mandating contact logging would open up the path for the application of article 6(1)(c) GDPR (and possibly section 38 DPA 2018), which authorises processing operations pursuant to a legal obligation to which the controller is subject. Article 6(1)(c) GDPR is subject to the same conditions laid down for article (6)(1)(e) GDPR.

Quality of the legal basis

It is important to stress that references to 'law' do not necessarily mean an official Act adopted by a national or European legislative body in all circumstances, without prejudice to requirements pursuant to the constitutional order of the member state concerned. However, in all circumstances the 'law' must respect the parameters of quality proper of a 'law'.[64] However, such a legal basis or legislative measure should be *clear* and *precise* and its application should be *foreseeable* to persons subject to it, in accordance with the case law of the CJEU and ECtHR. In *Bara and Others*, the CJEU found that a legislative measure that was not the object of official publication was not in compliance with article 13 of Directive 95/46, now article 23 GDPR.[65] Furthermore, case law has stressed that for the most serious interference, the guarantees must be strongest.[66] It is therefore difficult to imagine how a serious interference could be permissible in the absence of legislation scrutinised by parliament, which raises questions as to the legality of early COVID-19 measures stemming from regulation and even soft law. I will discuss the matter in greater detail when I review select data-driven measures and in the conclusions.

Article 6(3) and recital 45 outline criteria for the quality of the law with respect to the lawful bases laid down in article 6(1)(c) and (e). The law must specify the purpose of the processing, a purpose that must be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller when processing operations are based on article 6(1)(e). The law must

64 Recital 41 GDPR. European Data Protection Board, Guidelines 10/2020 on restrictions under article 23 GDPR (2020) 7, referring in particular to the ECtHR, 14 September 2010, *Sanoma Uitgevers BV v The Netherlands*, EC:ECHR:2010:0914JUD003822403, para 83. None of the measures reviewed in these pages explicitly aim at restricting the scope of the exercise of the right as in art 23 and recital 73 GDPR. Some processing operations need to be mandated by additional instruments (eg art 6(1)(c) and 6(1)(e), 9(2)(h) and (I) GDPR, ss 38, 51 and 53 DPA 2018).

65 Judgment of 1 October 2015 in *Bara and Others*, C-201/14, ECLI:EU:C:2015:638, para 40.

66 See, among others, *Tele 2 Sverige* (n 48 above).

also meet an objective of public interest and be proportionate to the legitimate aim pursued. Article 6 recommends the law contain specific provisions about:

- general conditions on lawfulness of personal data processing;
- types of personal data to be processed;
- the data subjects concerned;
- the purposes for, and entities to which, personal data may be disclosed;
- purpose limitation;
- storage period; and
- other measures for lawful and fair processing.

Given the language used ('should'), the inclusion of specific provisions in the law may appear to be desirable but optional from a regulatory perspective. However, when looking at data protection as a fundamental right, the provisions listed in article 6(3) appear necessary to respect, protect and fulfil the right, protect its essence[67] and comply with the substantive requirements of the rule of law: that is, the quality of the law and proportionality.

Unlike article 6(3), recital 45 recommends the law also contain the specifications for determining the controller. It is submitted that this addition is particularly important, not only because the identity of the data controller is not always self-evident,[68] but also because the controller is the gatekeeper for the exercise of the rights of data subjects. Uncertainty as to controllership can both generate confusion among those who process data following the guidance or directions of relevant authorities and curtail *de facto* the rights of data subjects who may not know whom to approach about enforcing their rights.[69] Clarifying matters of controllership is also relevant to understanding who should be the recipient of data collected according to guidance.[70]

In Irish law, section 36 DPA 2018 covers the introduction of suitable and specific measures for processing (and section 60 DPA 2018 covers restrictions). Importantly, the DPC is to be consulted before a minister makes regulations pursuant to sections 36, 38 and 51 (as well as section 60). The adoption of delegated legislation is not mandatory, though provisions such as section 53 DPA 2018 require that suitable

67 The essence includes limiting the purposes for which data can be processed and adopting rules to ensure the integrity and confidentiality of the data: Opinion 1/15 of the Court (Grand Chamber), ECLI:EU:C:2017:592, para 150.

68 To this effect, see EDPS, Concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 7 November 2019.

69 Judgment of 1 October 2015 in *Weltimmo*, C-230/14, EU:C:2015:639; *Wirtschaftsakademie Schleswig-Holstein* (n 57 above).

70 Müge Fazlioglu, 'Confusion as to how to share data with public authorities' (*International Association of Privacy Professionals* 21 April 2020).

and specific measures be taken to process data concerning health for purposes of public interest in the area of public health (following section 36 DPA 2018).

A systematic reading of the applicable law suggests that guidance requiring the processing of data without the necessary safeguards could amount to undue restrictions and could be challenged on rule of law grounds. Limitations to the rights of data subjects should stem from legislation derogating from the GDPR in line with article 23(1). Yet, the requirements for derogating legislation listed in article 23(2) are similar to those contained in article 6(3) and recital 45, as the list is formulated in an open-ended manner.

Whether the interference is compatible with the essence

The CJEU identified two elements that are the essence of article 8 of the CFR: the presence of a provision that 'limits ... the purposes for which ... data may be processed' and 'rules intended to ensure, inter alia, the security, confidentiality and integrity of that data, as well as to protect it against unlawful access and processing'.[71] These find correspondence in the principles of purpose limitation and integrity and confidentiality of data protection law. Therefore, any measure restricting the right without making provisions for purpose limitation, as well as integrity and confidentiality of data, is capable of crushing the essence and becomes automatically impermissible. It should be noted that the requirement of compatibility with the essence is a source of academic debate[72] as is the assessment of a breach of the essence.

Whether the interference is justified, necessary and proportionate

This article presumes that data-driven measures satisfy the condition that the interference is justified, as 'safeguarding public health' is 'an important objective of general public interest' justifying restrictions to data protection law pursuant to section 60(o) DPA 2018. However, a measure that intends to meet an important objective of public interest may still be discarded on grounds of necessity and proportionality.

---

71 Opinion 1/15 of the Court (Grand Chamber), ECLI:EU:C:2017:592, para 150.

72 See generally, Maja Brkan, 'The concept of essence of fundamental rights in the EU legal order: peeling the onion to its core' (2018) 2 European Constitutional Law *Review* 332–368; Maria Grazia Porcedda, 'On boundaries: finding the essence of the right to the protection of personal data in privacy and data protection' in Ronald Leenes et al (eds), *Data Protection and Privacy: The Internet of Bodies* (Hart 2018); Lorenzo Della Corte, 'A right to a rule: on the substance and essence of the fundamental right to personal data protection' in Dara Hallinan et al (eds), *Data Protection and Privacy: Data Protection and Democracy* (Hart 2020); Dara Hallinan, 'The essence of the right to the protection of personal data: essence as a normative pivot' (2021).

Whether the interference is necessary and proportionate

Earlier, I introduced the EDPS Toolkit on necessity[73] and the Guidelines on proportionality,[74] which primarily address decision-makers preparing legislation capable of interfering with article 8 CFR but are also useful for appraising the permissibility of interferences in light of existing legislation. The Toolkit and Guidelines are premised on the idea that the double requirements of necessity and proportionality[75] must be assessed on a case-by-case basis, and to this effect the EDPS develops a four-stepped methodology. The necessity test, which must be strictly met, requires first of all to factually describe the measure and secondly to identify whether the measure limits data protection (and other rights). Thirdly, one must define the measure's objectives against which to assess necessity and, lastly, choose the option that is effective and least intrusive.

Proportionality in a narrow sense must only be appraised for a measure that is strictly necessary, as evidenced by *Digital Rights Ireland* and *Schrems*.[76] The first step is to assess the legitimacy, or importance, of the objective and its effectiveness and efficacy, namely to what extent the proposed measure would meet this objective. The second step is to evaluate the scope, extent and intensity of the interference based on the effective impact of the measure on the rights. Third, comes the fair balance evaluation of the measure. The fourth and final step is to draw conclusions on the proportionality of the proposed measure, including the identification and safeguards which could make the measure proportionate. It is argued that none of the data-driven measures reviewed in this article reaches the proportionality stage of the test, as they all fail at previous stages, as I demonstrate next.

REVIEW OF SELECT 'UNDER-THE-RADAR' DATA-DRIVEN MEASURES

This section reviews several 'under the radar' pandemic data-driven measures, although not all measures deserving analysis are included. For instance, the Contact Management Programme (CMP), arguably a crucial component of the public health response to COVID-19 and any pandemic, is not reviewed here for want of technical documentation

73 EDPS (n 25 above).

74 EDPS (n 26 above).

75 On the necessity–proportionality nexus, see EDPS (n 25 above) 5.

76 Ibid 7; EDPS (n 26 above) 10, referencing *Digital Rights Ireland* (n 24 above) paras 46, 65 and 69, and Judgment of 16 July 2020 in *Facebook Ireland and Schrems*, C-311/18, ECLI:EU:C:2020:559, paras 92–93.

enabling ascertainment of its permissibility.[77] I review under-the-radar measures in light of the criteria just outlined: presence of an interference with the right to data protection; respect for the essence of the right; satisfaction of quality of the law requirements; meeting an objective of public interest, which is presumed here; necessity; and proportionality. To begin with, I show how thermal scanner guns can interfere with the right to data protection, meaning that they are not automatically permissible. I then show that self-check forms may not have an adequate legal basis and that instruments mandating contact logging do not fully satisfy 'quality of the law' requirements. I subsequently examine whether the VIS stands the test of necessity. I finally raise questions as to the compatibility of data-driven measures with the essence of article 8 of the CFR.

Thermal scanner guns may interfere with the right to data protection

Thermal scanner guns taking individuals' temperature have been widely used in a variety of settings. Models of thermal scanners capable of storing the temperature taken – and only the temperature taken with no logs of time and day – collect information which is not capable of identifying individuals; the ability of such data to become 'identifiers' is highly unlikely, as noted by DPAs across Europe.[78] However, the more information is stored, the higher the information's ability to identify an individual in conjunction with other data, based on the 'reasonably likely' test of *Patrick Breyer* and the EDPB, as discussed earlier. The finding changes dramatically for models of thermal screeners[79] connected to the internet that contain cameras and can support custom integrations such as third-party system software. These are akin to CCTV systems that collect data concerning health.

In its Guidance accompanying the 'return to Work Protocol', the DPC stressed the lack of HSE guidance concerning the use of thermo-scanners and advised against their use until such guidance is issued. Even if this mooted the need for further assessment, it would nonetheless be important to stress that the Health Information and Quality Authority found mass thermal screening (eg infrared thermal

77 Health Protection Surveillance Centre, 'Contact tracing guidance'. The CMP is analysed in Porcedda in Costello et al (n ✳ above) ch 1.

78 Christina Etteldorf, 'EU member state data protection authorities deal with COVID-19: an overview' (2020) 6(2) European Data Protection Law Review 265.

79 For purely illustrative purposes, see AXSIS Thermal Scanner Enabled Digital Hub.

scanners) at airports to be ineffective 'in identifying infectious individuals and limiting spread of disease'.[80]

The continued use of 'guns' that do not collect personal data could be no more than 'hygiene theatre'.[81] Other forms of thermal scanning capable of collecting personal data could constitute an interference requiring a legal basis, but in light of their manifest inadequacy such measures are unlikely to be deemed necessary and proportionate.

Self-check forms and measures for contact logging are unlikely to be 'in accordance with the law'

Self-check forms lack the requisite legal basis

In general, few data-driven measures are adopted pursuant to a clear and unambiguous legal basis.[82] At the beginning of the pandemic, many data-driven measures such as contact logging by individuals, businesses and entities of all kinds were based on guidance (hereafter the Government Roadmap) rather than statutory law, which raised rule of law challenges.[83] The 2021 Government Roadmap no longer encourages individuals and recreational facilities to undertake contact logging.[84] Non-essential businesses are instead encouraged to take 'protective measures' which, for the hotel sector specifically, include 'customer details recorded for contact tracing process'.[85] Eventually, the recording of customer details for contact-tracing purposes was given statutory footing (see further below). 'Protective measures' not specifically linked to statutory requirements include thermal scanner guns (reviewed earlier) and self-check forms for visitors to business premises, for example retailers,[86] universities and customers of hairstylists and beauticians[87] – forms that process data concerning health (article 4(15) GDPR).

80 Health Information and Quality Authority, 'Thermal screening' (6 August 2020).

81 Derek Thompson, 'Hygiene theater is a huge waste of time' (*The Atlantic* 27 July 2020).

82 See Porcedda in Costello et al (n ✳ above) ch 1.

83 Porcedda (n 10 above).

84 Department of the Taoiseach, 'COVID-19 resilience and recovery 2021 – the path ahead' (15 September 2020) 8 and 11.

85 Ibid 50.

86 NSAI, 'COVID-19 retail protection and improvement guide' version 21 (2020) 19.

87 'Re-opening guidelines for Irish hair salons and barber shops' (HABIC June 2020) 17. Paul Moore, 'Rules you have to follow in Ireland's hairdressers and barbers upon reopening' *Irish Mirror* (Dublin, 9 May 2021).

To ensure the Safety & Health of all people interacting with (insert Salon Name), clients and visitors must complete this declaration form prior to entering or on arrival our salon. If you indicate to us you have symptoms of COVID-19 OR you have been abroad in the last 14 days with exception to Northern Ireland you will be required to either restrict your movements or self-isolate.

Where this is the case, you are prohibited from entering the salon/barber shop and advised to seek professional medical help/ assistance in line with HSE Guidelines.

			Yes	No
1.	Have you visited any of the countries outside Ireland excluding Northern Ireland?		☐	☐
2.	Are you suffering any flu like symptoms?		☐	☐
3.	Are you experiencing any difficulty in breathing, shortness of breath?		☐	☐
4.	Are you experiencing any fever/temperature symptoms?		☐	☐
5.	Did you consult a Doctor or other medical practitioner?		☐	☐
6.	How are you feeling Health wise?	**Well**	☐	**Unwell** ☐
7.	Have you been in contact with someone who is confirmed to have COVID-19 has visited an affected region in the past 14 days?		☐	☐

Figure 1: Hair and Beauty Industry Confederation (HABIC) of Ireland visitor questionnaire.

The processing of data concerning health, as many COVID-19-related measures do, can be seen as a serious interference and deserves higher protection (recital 51 GDPR).[88] For such a reason, national DPAs disagree as to the permissibility of self-health screening questionnaires for employees,[89] let alone visitors. Data collected through self-check forms can be lawfully processed under the combined legal bases of articles 6(1)(c) and 9(2)(b), but only if, as the DPC notes, 'the processing is necessary[90] for the purpose of carrying out its obligations in the field of employment (such as the obligations arising under the 2005 Act)'.[91] If self-check forms emanated from the Safety, Health and Welfare at Work Act 2005, then they would have a legal basis. The compatibility of self-check forms with data protection law would then need to be assessed in light of their necessity, which remains to be demonstrated; self-check forms in their current form seem disproportionate and are

88 Judgment of 24 September 2019 in *GC, AF, BH, ED* (n 56 above) paras 44 and 67.

89 Etteldorf (n 78 above).

90 This links to the principles of fairness and purpose limitation.

91 DPC, 'Data protection implications of the return to work safely protocol' (June 2020) 3.

likely to amount to an impermissible interference with the right to data protection.[92]

If self-check forms did not emanate from the Safety, Health and Welfare at Work Act 2005, then a legal basis would need to be found. A facsimile of self-check forms for visitors was drawn up by the National Standards Authority of Ireland (NSAI)[93] and has remained unchanged throughout the pandemic. From a rule of law perspective, guidance can qualify as a legal basis if it fulfils the quality of law requirements illustrated earlier, including clarity and foreseeability,[94] which enable citizens to adjust their conduct. In spite of its publicity,[95] the Government Roadmap is unlikely to meet quality of law parameters: not only does it not meet the parameters required by articles 6(2) and (3) and *a fortiori* article 9 GDPR, but also, it never required visitors to produce self-check forms as one of the protective measures. Self-health check forms emanate from guidance, rather than standards,[96] which was not produced pursuant to a mandate issued by the legislature and is unlikely to constitute a legal basis. In sum, self-check forms suffer from many shortcomings that make them incompatible with data protection law.

Instruments for contact logging and locator forms display 'quality of the law' shortcomings

Three Statutory Instruments (SIs) were adopted to support contact-tracing efforts. One such SI gives statutory basis to the recording of customer details by hotels, eateries and bars for contact-logging purposes.[97] Two SIs specifically required international passengers entering Ireland to 'retain', 'give or otherwise make available' to

92 Elsewhere I show that the lack of a 'generic data protection notice', which data controllers could easily affix in their premises to inform people of their rights, deprives data subjects of effective protection and is akin to restrictions to their rights, in defiance of art 23 GDPR and s 60 DPA 2018. See Porcedda in Costello et al (n ✳ above) ch 1. See also Maria Grazia Porcedda, 'Businesses need to be careful with personal data during pandemic' *Irish Times* (Dublin, 20 July 2020).

93 NSAI, 'COVID-19 workplace protection and improvement guide' version 7 (2020) 16.

94 Judgment of 25 May 2021, *Big Brother Watch and Others v UK*, App nos 58170/13, 62322/14 and 24960/15, CE:ECHR:2018:0913JUD005817013.

95 EDPS (n 25 above) 4.

96 The legal standing of standards adopted in the context of EU delegated legislation has changed since Judgment of 27 October 2016 in *James Elliot*, Case C-613/14, ECLI:EU:C:2016:821, para 40. However, the ability of standards, especially those adopted by national bodies, to act as a legal basis remains to be assessed.

97 Health Act 1947 (Section 31A – Temporary Restrictions) (Covid-19) (No 2) Regulations 2021. An informal consolidation of the regulations and related amendments is available at 'Informal consolidation of COVID-19 regulations'.

a relevant person or a member of the Garda Síochána a negative COVID-19 test result,[98] and to fill in and hand in to the 'relevant person' a locator form.[99]

The adoption of multiple instruments with similar aims creates a jigsaw puzzle of data collection requirements. One difference concerns controllership, which is determined by the identification of the means and purposes of the processing. Different SIs identify different controllers, and in one case (locator forms) controllership has changed from one version to the other. In particular, legislation affecting hotels, eateries and bars identifies three different controllers for three different purposes. For instance, hotels, restaurants and pubs are controllers when collecting data, thereby opening up the path for the application of article 6(1)(c) GDPR. Hotels, eateries and bars certainly decide the means of processing but not its purpose. The fact that data are ultimately collected for the benefit of contact tracing puts hotels, eateries and bars in a position closer to that of a processor than a controller. In all cases, the SIs presuppose a transfer of personal data currently lacking the requisite interinstitutional arrangements.[100]

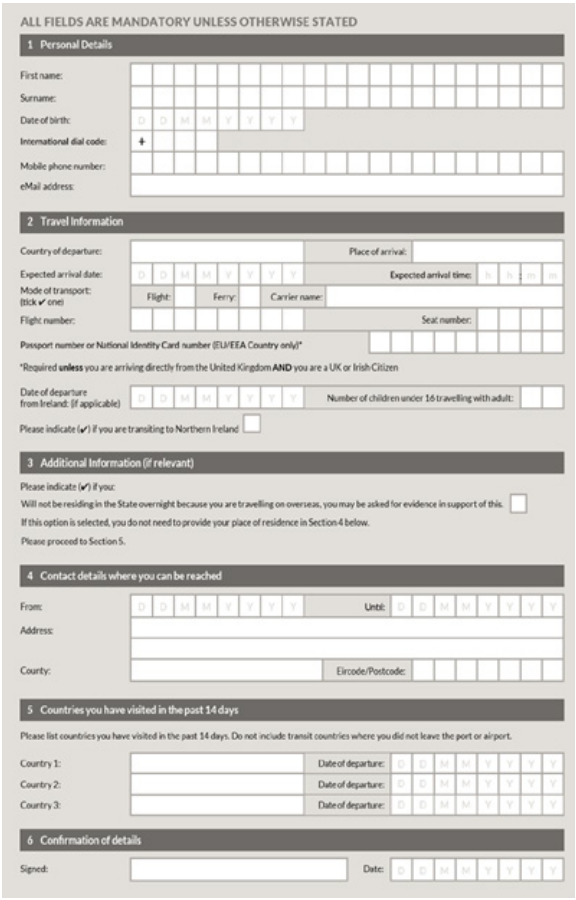
The jigsaw puzzle effect is worsened by the fact that all SIs have been amended multiple times in the space of a year, partly because measures were adopted on a trial-and-error basis and needed to be adjusted, partly to reflect initiatives coordinated at EU level, such as the adoption of Digital Green passes, and partly to lift restrictions. Frequent amendments of such fragmentary legislation undermine legal certainty, thereby impacting foreseeability, not to mention the operational costs to the addressees of legislation.

These instruments also show substantive similarities, begging the question of why the legislator privileged multiple instruments as opposed to an overarching law disciplining data processing for contact logging and tracing for pandemic purposes. First, all SIs lay down penal provisions and endow the Garda Síochána with enforcement powers with respect to preventing, detecting, investigating or prosecuting a criminal offence arising from a contravention of a provision stated to be a penal provision. Secondly, all SIs present exceptions to the term for data retention identified in legislation. Thirdly, none of the SIs

98 Reg 5(1) of SI 135/2021 Health Act 1947 (Section 31A – Temporary Restrictions) (COVID-19) (Restrictions upon travel to the State from Certain States) (No 5) Regulations 2021, revised to 14 June 2021. See also 'Statutory instruments relating to the COVID-19 pandemic'.

99 SI 45/2021: Health Act 1947 (Section 31A – Temporary Requirements) (Covid-19 Passenger Locator Form) Regulations 2021 revokes SI 181/2020: Health Act 1947 (Section 31A – Temporary Restrictions) (COVID-19 Passenger Locator Form) Regulations 2020. There, the HSE was also a data controller.

100 See Costello in Costello et al (n ✳ above) ch 3.



ALL FIELDS ARE MANDATORY UNLESS OTHERWISE STATED

1 Personal Details

First name:
Surname:
Date of birth: D D M M Y Y Y Y
International dial code: +
Mobile phone number:
eMail address:

2 Travel Information

Country of departure: Place of arrival:
Expected arrival date: D D M M Y Y Y Y Expected arrival time: h h : m m
Mode of transport: (tick ✔ one) Flight: Ferry: Carrier name:
Flight number: Seat number:
Passport number or National Identity Card number (EU/EEA Country only)*
*Required **unless** you are arriving directly from the United Kingdom **AND** you are a UK or Irish Citizen
Date of departure from Ireland: (if applicable) D D M M Y Y Y Y Number of children under 16 travelling with adult:
Please indicate (✔) if you are transiting to Northern Ireland

3 Additional Information (if relevant)

Please indicate (✔) if you:
Will not be residing in the State overnight because you are travelling on overseas, you may be asked for evidence in support of this.
If this option is selected, you do not need to provide your place of residence in Section 4 below.
Please proceed to Section 5.

4 Contact details where you can be reached

From: D D M M Y Y Y Y Until: D D M M Y Y Y Y
Address:
County: Eircode/Postcode:

5 Countries you have visited in the past 14 days

Please list countries you have visited in the past 14 days. Do not include transit countries where you did not leave the port or airport.

Country 1: Date of departure: D D M M Y Y Y Y
Country 2: Date of departure: D D M M Y Y Y Y
Country 3: Date of departure: D D M M Y Y Y Y

6 Confirmation of details

Signed: Date: D D M M Y Y Y Y

Figure 2: Example of passenger locator form.

satisfies in full the requirements of article 6(2) and (3). To exemplify the issue I focus on locator forms.

The degree of intrusiveness of locator forms[101] is arguably greater than simple contact logging because such forms collect more categories of personal data and are imposed on all international passengers. Moreover, the use of digital locator forms is riskier than the use of paper ones as per the revoked SI 181/2020 because the use of automated means of processing can facilitate further, unauthorised processing compared to manual processing. Legislation mandating the collection of travel forms constitutes a legal basis in line with article 6(1)(e) GDPR, but in its current form it arguably lacks the elements to ensure lawful and fair processing identified above.

101 Ibid, defined in reg 3. The previous version can be found at on the Irish Statute Book website. The regulations also cover passenger location form receipts, which are not reviewed here.

The revised locator form collects more categories of personal data than the revoked SI 181/2020. The updated section on 'travel information' gathers more information than the 2020 version and also features a new section titled 'countries you have visited in the past 14 days'. The form collects identity card data for EU citizens and passport data for all other citizens, with the exception of UK or Irish citizens, who are exempted; it also collects information such as flight and seat numbers. The principles of purpose specification and data minimisation require the text to adequately reflect the necessity of the data for the purposes of the processing. However, such categories are not adequately reflected in the regulations, which only explicitly refer to – and thus justify the need for – collecting passengers' 'contact details', namely a telephone number and email address, as well as the 'place of residence', meaning 'the place, or places, in the State or in Northern Ireland[102] at which he or she intends to reside' (regulation 2).

Furthermore, in common with all SIs, processed data must be erased 28 days after the date of arrival, with the exception of 'when they are required for the purposes of the prevention, investigation, detection or prosecution of *a criminal offence*' (regulation 8(4), emphasis added), an exception that was first laid down in the 2020 Regulations. This exception is common to all SIs seen in this section and is highly problematic. Firstly, it *de facto* broadens the purposes for which data can be used, which sits uncomfortably with the 'quality of the law' tenet.[103] Secondly, the purpose '*a criminal offence*' is unspecified and is broader than the penal provisions identified in the SI thus providing insufficient clarity and foreseeability (on purpose limitation, see below). Finally, by stating that the data will be deleted when no longer required, the regulation fulfils the storage limitation principle only formally: without clearly specifying which 'criminal offence' the data could be processed for, the regulation opens up the possibility of endless retention, which would undermine the substance of the principle. As a result of these shortcomings, the SIs could excessively interfere with data protection law and therefore be partly invalid.

Are guidance and SIs in accordance with data protection law?

On balance, all data-driven measures drawing from guidance or SIs state the main purpose of the processing. Yet, measures do not consistently include the safeguards for data processing to ensure the lawful and fair processing listed in article 6(3) GDPR. SIs generally include provisions stating:

102 This was added in SI 45/2021 (n 99 above).

103 See also Oran Doyle, 'Quarantine after international travel: legal obligations, public health advice, pervasive confusion' (*COVID-19 Law and Human Rights Observatory Blog* 27 July 2020).

- the types of personal data to be processed;
- the data subjects concerned;
- the purposes for and entities to which personal data may be disclosed; and
- the identification of the data controller, though not always with clarity for all categories.

Some SIs fail to indicate clear storage periods and are silent on the conditions on lawfulness of personal data processing. Guidance rarely goes beyond the identification of the types of data to be processed and data subjects concerned. The mandatory language used by guidance sits uncomfortably with the requirements of article 6(3) GDPR and the criteria of 'clarity', 'precision' and 'foreseeability' found in recital 41 GDPR, constitutional law and international human rights instruments. Furthermore, the more intrusive the processing, the less likely it is to pass the legality test in case of judicial review.[104] All documents specify purposes, but none of those reviewed thus far clearly limit them. Thus, most measures would hardly be 'in accordance with the law'.

Necessity: the Vaccine Information System

The VIS is 'an end-to-end comprehensive digital solution to support the delivery and rollout of the nationwide COVID-19 vaccination programme'.[105] It is based on several frameworks, such as the Health Identifiers Act 2014, section 31 of the Health Act 1947, the Infectious Diseases Regulations 1981 (SI 390/1981)[106] and policies (ie the European Commission eHealth Network).[107] The VIS is justified by an objective of public interest and therefore the present analysis focuses on necessity.

In accordance with the methodology developed by the EDPS, to ascertain necessity one must first describe the measure. This can be easily accomplished thanks to the data protection impact assessment (DPIA) first published in December 2020. Although the publication of the DPIA was a very welcome move for transparency and public scrutiny, it should be noted that, first, the DPIA was edited 23 times between its publication and September 2021, and, second, the 'table of versions' does not enable the reader to track and identify changes to

104 See Ibid; Oran Doyle, 'Leaving home: reasonable excuses, vagueness, and the rule of law' (*COVID-19 Law and Human Rights Observatory Blog* 5 June 2020); Oran Doyle, 'On legal obligations and golf-gate' (*COVID-19 Law and Human Rights Observatory Blog* 28 August 2020).

105 HSE, Vaccine Information System for COVID-19 Vaccination Programme Data Protection Impact Assessment, version 1.8 (22 April 2021) 6.

106 Ibid 32–33.

107 Ibid 20.

the text.[108] It is even questionable whether a DPIA should be edited at all, as it is not a data management plan. Version 0.6 incorporates comments from the DPC, possibly in relation to prior consultation.[109] The present analysis is based on version 18.

The development, testing, security, operation and maintenance of the system is the joint responsibility of the HSE and IBM. The latter oversees the configuration of the VIS, which is hosted on Salesforce's HealthCloud platform[110] 'within Salesforce data centres within the European Economic Area (EEA)'.[111] The overall data controllers are the HSE and general practitioners (GPs) (with respect to their patients' data), as well as the Central Statistics Office (CSO), whereas IBM is identified as a processor, alongside pharmacists, healthcare facilities (acting under section 38 of the Health Acts 2004), private hospitals and Department of Public Expenditure and Reform. Salesforce is a subprocessor.

All these entities receive patient data, which include several categories of personal information: first name, middle name (optional), surname, mother's maiden name, date of birth, personal public service number (PPSN), sex, nationality, ethnicity, the individual health identifier (IHI),[112] home address, county, country, area code/Eircode, GP name, occupation, prioritisation category, vaccination status, contraindication to vaccination, health state, pregnancy, COVID history and vaccination history.[113] The Health Products Regulatory Authority and Department of Health are the recipients of anonymised data. Patient data are to be retained in perpetuity, though it is not clear on what system and therefore whether processors will also retain data in perpetuity.[114] The DPIA discusses risks and mitigation strategies, including generic technical and organisational measures and a description of data security measures.

Analysis of the Vaccine Information System

A reading of version 18 of the DPIA shows that the VIS limits the right to data protection. The VIS pursues a number of objectives, including vaccination, archival purposes for the HSE and GPs and statistical purposes for the CSO. Such objectives appear *prima facie* necessary, but based solely on the DPIA it appears difficult to carry out the last

108 Ibid.

109 Ailbhe Daly, 'Private information of thousands who received Covid vaccine exposed in HSE blunder' *Irish Mirror* (Dublin, 25 February 2021).

110 HSE (n 105 above) 13.

111 Ibid 35.

112 'Generated for each person registered for a vaccination': ibid 27.

113 Ibid 26–28

114 Ibid 23.

step of the necessity test, namely to choose the measure that combines effectiveness and minimal intrusion. First, the DPIA identifies three lawful bases, articles 6(1)(e), 9(2)(h) and (i) GDPR,[115] for the 'purposes of processing personal data for the vaccination programme', rather than for each specific purpose pursued by the different data controllers (eg vaccination and archival purposes for the HSE and GPs, statistical purposes for the CSO etc). This prevents an analysis of effectiveness.

Secondly, although the importance of the principle of data minimisation is stressed several times across the document, justification as to the need to collect data is only given for data enabling to uniquely identify a patient (IHI).[116] As for the remaining, long and broad, list of personal data to be collected, the DPIA only describes when the data are collected, not why they are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.[117] This hinders an analysis of effectiveness and minimal intrusion.

A third cause for concern is that both IBM and Salesforce 'are providing support of the Vaccine Information System from outside the EEA';[118] it is unclear why these companies, who have European and particularly Irish offices,[119] are operating from outside the EEA and where from exactly. The DPIA mentions 'appropriate arrangements as set out in Chapter 5 of the GDPR in order to facilitate the transfer and/or processing of vaccine data outside the EEA' but does not provide any further details as to such arrangements, for example whether they rely on binding corporate rules or standard contractual clauses. The transfer of VIS data to the United States (US), following the CJEU's decision in *Facebook Ireland and Schrems*,[120] which invalidated Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 on the adequacy of the protection provided by the EU–US Privacy Shield, would be highly problematic. Equally problematic would be the use of standard contractual clauses, as they do not automatically afford a level of protection essentially equivalent to that guaranteed within the EU, read in the light of the CFR.[121] Once more, an analysis of effectiveness and minimal intrusion is not possible.

Fourthly, all data collected are to be retained in perpetuity; this decision appears to be a serious breach to the principle of storage limitation, as it is unrelated to specific purposes and specific

115 Ibid 31.
116 Ibid 18.
117 Ibid 26.
118 Ibid 34.
119 Ibid. See also Salesforce, 'Europe, Middle East and Africa'; IBM Research Europe.
120 *Schrems* (n 76 above).
121 Ibid para 105.

controllers/processors. It is also unclear whether the processors and sub-processors would retain such data in perpetuity as well.[122] This point effects maximal intrusion and therefore challenges necessity.

Fifthly and relatedly, such an endless retention period necessarily invalidates the risk assessment: if data are to be held in perpetuity, by all parties involved, the risks of breaches of data protection legislation (which apply so long as the data subject is alive) are vastly multiplied, which the risk assessment does not adequately take into account.[123] Such a state of affairs has a knock-on effect on security. In February 2021, an individual who was erroneously given access to the IT system used by the HSE contacted the *Irish Mirror* to blow the whistle. The human error enabled the whistleblower to access confidential data such as PPSNs, addresses, names and contact details about thousands of vaccine recipients 'despite earlier warnings by data chiefs'.[124] Moreover, the list of technical and organisational security measures provided, which on paper appear adequate,[125] will need to be updated in years to come, for instance with the development of quantum computing. In sum, the VIS is implemented in such a manner that challenges the requirement to choose the most effective and least intrusive measures, thereby appearing unnecessary and therefore limiting the right to data protection by a greater extent than required.

Respect for the essence: a transversal shortcoming?

Following article 52(1) CFR, the assessment of whether the essence is infringed (ie whether the right is emptied of its core elements)[126] must be done immediately after the analysis of lawfulness. However, as mentioned earlier, a methodology to ascertain respect of the essence is hitherto missing and the operationalisation of the concept is debated by scholarship. The following analysis is, therefore, exploratory.

A purposive interpretation of the law in light of the essence would invalidate most measures. First, derogations from strict data retention periods for as vague a purpose as 'a criminal offence' would fail to constitute a provision that 'limits ... the purposes for which ... data may be processed,'[127] thereby crushing the essence and invalidating the relevant measure (or part thereof). The same could potentially apply to data stored by the VIS 'in perpetuity'. Secondly, all SIs and most data-

122 HSE (n 105 above) 23.
123 Ibid 26, risk #10 and mitigation #10.
124 Daly (n 109 above).
125 An assessment is impossible without reference to detailed technical measures and specific standards.
126 EDPS (n 26 above).
127 Opinion 1/15 of the Court (Grand Chamber), EU:C:2017:592, para 150.

driven measures, except the VIS DPIA, lack provisions addressing the integrity and confidentiality of the data collected. Whether or not the essence is compromised, the importance of securing personal data cannot be overstated due to the increased risk of data breaches tied to an unaware, overwhelmed or home-bound workforce.[128] Unsafely discarded logged contacts, even manual ones from hotels, eateries and bars could be a treasure trove for fraudsters, adding to the tally of phishing (email), vishing (voicemail) and smishing (text messaging) frauds, which were up by 45 per cent in 2020[129] and by 50 per cent in 2021.[130] The use of cloud-computing solutions, which the VIS relies on, can increase the costs of a data breach by exfiltrated/lost unit.[131]

The ransomware attack suffered by the HSE in May 2021 demonstrates how data security requirements need to become a regulatory priority and cannot be left to contractual arrangements between the controller and the processor.[132] Importantly, the security incident did not seem to affect the VIS.[133] The incident provides a cautionary tale for any data collection system put into place. A report published in May 2021 on the National Incident Management System within the HSE found 'lack of clear governance, leadership and management … The HSE owns this data and should be taking responsibility for leading a long-term strategic approach to ensure the effective collection and use of this data.'[134]

128 DPC, 'Protecting personal data when working remotely' (12 March 2020).

129 'Garda stats: domestic violence, drug possession and fraud on the rise during lockdown' (*The Journal.ie* 12 June 2020).

130 Conor Lally, 'Online crime jumps by half last year as cyber fraud increases' *Irish Times* (Dublin, 12 March 2021).

131 Larry Ponemon, '2017 cost of data breach study'. The CMP also relies on cloud computing.

132 See Maria Grazia Porcedda, 'Patching the patchwork: appraising the regulatory framework on cyber security breaches' (2018) 35(5) Computer Law and Security Review 1077–1098.

133 Eoin Butler, 'Life as a Covid vaccine volunteer' *Irish Times* (Dublin, 13 June 2021).

134 Health Information and Quality Authority, 'Review of information management practices for the National Incident Management System (NIMS) within the HSE' (May 2021).

CONCLUSIONS: LEGISLATORS OUGHT TO DEVELOP A BLUEPRINT FOR PROCESSING PERSONAL DATA FOR PANDEMIC PURPOSES

This article has reviewed the compliance of data-driven measures adopted in Ireland some months into the COVID-19 pandemic with regard to the right to data protection. The analysis was conducted on the basis of criteria drawn from the applicable law read in light of the CFR. The analysis shows that thermal scanner guns can potentially interfere with the right to data protection; self-check forms rest on shaky legal bases; the quality of SIs for contact logging is insufficient; elements of the VIS seem unnecessary; and a rigorous interpretation of the essence of the right to data protection could invalidate many data-driven measures. Crucially, while the rationale of such interventions can be justifiable, the delivery does not fully comply with data protection law.

A systematic review of the applicable law in light of the right to data protection suggests that digital and manual data-driven measures that process data without the necessary safeguards could amount to undue restrictions and could be challenged on rule of law grounds. Such an outcome is in keeping with the findings of other commentators who stressed the potential inadequacy of national rules overseeing the state of emergency[135] and the consequences this carries for legality.[136] The outcome points to the difficulty of reconciling public health and data protection without a systematic data-processing strategy.

The lack of coordination was fully understandable at the beginning of the COVID-19 epidemic, as EU member states were relatively inexperienced in pandemics and consequently have been learning as they went along.[137] However, EU member states could have made better use of lessons learnt from other situations of emergency, such as terrorism and the related data retention debate. Indeed, the relevance of data retention debates has not escaped commentators:[138] the related judicial saga has traced the boundaries of pandemic

135 Alan Greene, 'Ireland's response to the COVID-19 pandemic' (*VerfBlog*, 11 April 2020); Conor White, 'The Oireachtas and mandatory face coverings' (*COVID-19 Law and Human Rights Observatory Blog* 13 July 2020); Gianluca Sardi, 'L'emergenza sanitaria da Covid-19 nella Repubblica d'Irlanda. Strumenti giuridici per contrastare la pandemia e conseguenze problematiche sulla protezione dei diritti fondamentali' (2020) DPCE Online 2.

136 Conor Casey, Oran Doyle, David Kenny and Donna Lyons, 'Ireland's emergency powers during the Covid-19 pandemic' (Irish Human Rights and Equality Commission 2020).

137 Martina Cardone and Marco Cecili, 'Osservazioni sulla disciplina in materia di tutela dei dati personali in tempi di Covid-19. L'Italia e i modelli sudcoreano, israeliano e cinese: opzioni a confronto' (2020) Nomos 1.

138 Kennedy (n 6 above).

interventions. Furthermore, successive waves of lockdown have offered the opportunity to review and, where necessary, correct the responses given in the heat of the moment. To an extent, this has happened with the adoption of SIs for contact logging and the publication of the VIS DPIA, but, as seen, such measures could benefit from additional correction.[139]

The applicable law provides the necessary elements for an intervention that reconciles the objectives of protecting personal data and public health. A half-hearted application can come at great cost – as evidenced for instance by the ransomware attack and data breach suffered by the HSE – and undermine trust in the provision of public services. On this account, I formulate three recommendations towards a blueprint for data processing for pandemic purposes.

First, I recommend *the adoption of an overarching instrument that contains the blueprint for data processing for pandemic purposes*. The criteria for compliance with the applicable law discussed above can be repurposed as a blueprint for such processing, in combination with the EDPS Toolkit on necessity and the Guidelines on proportionality. In the Irish transposition of data protection law, the blueprint would ideally be a measure of the rank of an SI or higher, laying down the legal basis for contact logging and transfers of data to the HSE for contact-tracing purposes, in a clear, precise and foreseeable manner, following the criteria stemming from article 6(2) and (3) GDPR and the DPA 2018 outlined above. The obligation to consult the DPC would help to ensure adherence to the law.

Accordingly, the law should at a minimum identify the department retaining overall controllership (eg Department of Health), list co-controllers and refer to inter-institutional data-sharing arrangements. The law should outline the data subjects concerned within different contexts, such as travel, entertainment, employment, healthcare and so on and clarify the categories of data to be collected in abidance with the principles of purpose limitation and data minimisation. The law should clarify when the processing of data concerning health is necessary and proportionate. The blueprint should identify thresholds to protect the integrity and confidentiality of data and deadlines for the erasure of data commensurate with the risks engendered by the settings of data-processing operations.

Secondly, to fulfil transparency requirements the blueprint should include *a facsimile data protection notice for all entities asked to process personal data for pandemic purposes*, to step up the effectiveness of data subject's rights. Such notice could be in the guise of COVID-19-related posters affixed to the walls (or shown on websites) of businesses and public institutions.

139 Porcedda (n 10 above).

Thirdly, the blueprint should be complemented by a commitment to *aggregate and publish documentation concerning the digital components of the response to COVID-19 as well as future CMPs*, to match the level of transparency achieved for measures such as the COVID-19 app and enable public scrutiny, including from a cybersecurity perspective. This includes *opening up the DPIA carried out for the VIS and future similar systems to public consultation* and clarifying where patient data are being transferred to and under what arrangements, as set out in chapter 5 of the GDPR.

The adoption of a blueprint for data processing would remove the need for constantly updating guidance and legislation, with the extant impact on legal certainty for all members of society. It would also represent a concrete step towards the reconciliation between the rights to data protection and to public health worthy of democracies committed to the rule of law.