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

School of Law, House 39, Trinity College Dublin, Dublin 2

maria-grazia.porcedda@tcd.ie

0000-0002-9271-3512

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, understood as both a source of regulatory compliance, and as the substantiation of a right. The article elaborates a test for permissible limitations on the right to data protection that incorporates requirements from the applicable law, followed by an analysis of how select data-driven measures comply with the various stages of the test. 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 for pandemic purposes. (147 words)

Keywords: fundamental right to the protection of personal data, judicial review, legality, Covid-19 pandemic, data-driven measures, contact logging, vaccine information system, travel

Introduction[1]

Since the beginning of the pandemic policymakers in the European Union (hereafter EU) have adopted several data-driven measures to contain the spread of Covid-19. The 'comprehensive public health strategy to fight the pandemic'[2] 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[3] such as Ireland's Covid Tracker App,[4] Digital Green Certificate,[5] contact management systems and vaccine information systems; manual measures include contact logging by individual and organisations; off-the-shelf technologies have been used, among others, in the context of return to work schemes.

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 Art. 8 of the Charter of Fundamental Rights of the European Union (hereafter CFREU).[6] Yet, the question has been publicly discussed only with

[1] 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 and the editors of the special issue for the helpful comments on a various drafts of this work. 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.

[2] 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' (21 April 2020).

[3] European Commission, 'Communication from the Commission. Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection*' (2020/C 124 I/01)*, C 124 I/1, 17.4.2020,

[4] Health Safety Executive (HSE), 'HSE launch the COVID Tracker App' (7 July 2020) <https://www.hse.ie/eng/services/news/media/pressrel/hse-hpsc-launch-the-covid-tracker-app.html>.

[5] EDPB-EDPS, Joint Opinion on the Digital Green Certificate (31 March 2021), <https://edps.europa.eu/data-protection/our-work/publications/opinions/edpb-edps-joint-opinion-digital-green-certificate_en>.

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

respect to Covid-19 apps[7] on account of their potential for surveillance on a mass scale,[8] which creates the type of power imbalance that data protection legislation, as well as the multilevel system of human rights protection shared by EU Member States, seeks to prevent.[9] Public discussion was certainly beneficial,[10] though Apps were unlikely to become mandatory in light of regulatory constraints (section 1.1.1.2). Other commonplace, and often mandatory, data-driven measures have instead gone under the radar, and consequently eluded public scrutiny. Examples include low-tech measures such as contact logging by hairstylists, as well as the specifics of high-tech solutions such as the vaccine information system.

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 TFEU), who retain the privilege to introduce more specific

[7] Early responses in Ireland: Rónán Kennedy, 'Data Protection and COVID-19: Short-Term Priorities, Long-Term Consequences' (*Bloomsbury Professional Ireland*, 8 May 2020) <https://ireland.bloomsburyprofessional.com/blog/data-protection-and-covid-19-short-term-priorities-long-term-consequences>; Trinity College Dublin Covid-19 Law and Human Rights Observatory, <https://www.tcd.ie/law/tricon/covidobservatory/index.php>. 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) <https://www.qmul.ac.uk/law/news/responding-to-covid-19/items/responding-to-covid-19-surveillance-trust-and-the-rule-of-law.html>; Vincenzo Zeno-Zencovich, 'I limiti delle discussioni sulle "app" di tracciamento anti-Covid e il futuro della medicina digitale' (*Media Laws*, 26 May 2020) http://www.medialaws.eu/i-limiti-delle-discussioni-sulle-app-di-tracciamento-anti-covid-e-il-futuro-della-medicina-digitale/; Oskar J. Gstrein and Andrej Zwitter, 'Using Location Data to Control the Coronavirus Pandemic' (*VerfBlog*, 20 March 2020) <https://verfassungsblog.de/using-location-data-to-control-the-coronavirus-pandemic/>.

[8] Lily Kuo, 'The New Normal': China's Excessive Coronavirus Public Monitoring Could Be Here To Stay', *The Guardian* (9 March 2020) <https://www.theguardian.com/world/2020/mar/09/the-new-normal-chinas-excessive-coronavirus-public-monitoring-could-be-here-to-stay>; Patrick Wintour, Coronavirus: who will be winners and losers in new world order? *The Guardian* (11 April 2020) <https://www.theguardian.com/world/2020/apr/11/coronavirus-who-will-be-winners-and-losers-in-new-world-order>.

[9] E.g. Christopher Docksey and Christopher Kuner, 'The Coronavirus Crisis and EU Adequacy Decisions for Data Transfers' (*European Law Blog*, 3 April, 2020) https://europeanlawblog.eu/2020/04/03/the-coronavirus-crisis-and-eu-adequacy-decisions-for-data-transfers/; Elif Mendos Kuskonmaz and Elspeth Guild, 'Covid-19: A New Struggle over Privacy, Data Protection and Human Rights?' (*European Law Blog*, 4 May 2020) <https://europeanlawblog.eu/2020/05/04/covid-19-a-new-struggle-over-privacy-data-protection-and-human-rights/>.Interestingly, the public and academic debate has overlooked apps deployed by employers to locate workers attending the workplace during the pandemic.

[10] Thanks to the swift intervention of the expertand policy community, apps' data protection shortcomings were quickly redressed. In Ireland, see Irish Council for Civil Liberties, 'Principles for legislators on the implementation of new technologies' (29 April 2020) <http://www.cearta.ie/2020/06/principles-for-legislators-on-the-implementation-of-new-technologies/>. HSE Ireland /covid-tracker-app (GitHub) <https://github.com/HSEIreland/covid-tracker-app>.European Commission, 'Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection' OJ 2020/C 124 I/01.

provisions to adapt the application of EU data protection law in this area. Thus, this contribution appraises the compliance with data protection law of select data-driven measures adopted in Ireland between summer 2020 and 2021[11] to contain Covid-19. Data protection law, including the GDPR and other relevant instruments (section 1.1.2.2), 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 CFREU.[12] I refer to such a blend of regulation and rights as the dual nature of data protection law.

Given the dual nature of data protection law, the perspective adopted in this article is one of reconciliation between equally important objectives. If mass surveillance is an undesirable goal, so is a blanket prohibition against the processing of personal data to contain the pandemic. Ultimately, the point is how to design 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 Art. 7 protecting privacy[15]), whose enjoyment can

[11] I reviewed measures adopted between March and August 2020 in Maria Grazia Porcedda, 'Data Protection Implications of Data Driven Measures Adopted in Ireland at the Outset of the Covid-19 Pandemic' (2021) *European Data Protection Law* 2/21.

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

[13] Department of Health, 'Ethical Framework for Decision-making in a Pandemic' (17 April 2020) https://www.gov.ie/en/publication/dbf3fb-ethical-framework-for-decision-making-in-a-pandemic/; Andrea Mulligan, 'The Ethics of Lockdown: Transparency, Accountability and Community Involvement' (*COVID-19 Law and Human Rights Observatory, 15 July 2020*); Fundamental Rights Agency, 'Covid-19', <https://fra.europa.eu/en/themes/covid-19>; Amedeo Santosuosso, 'La regola, l'eccezione e la tecnologia' (2020) *BioLaw Journal – Rivista di BioDiritto Special Issue* 1/2020, 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), available at <https://eprints.whiterose.ac.uk/140945/1/Porcedda_Valu_Privacy_Data_Protection_Symplectic.pdf>.

[14] Data Protection Commission (DPC), 'Data Protection and COVID-19' (March 2020) <https://www.dataprotection.ie/en/news-media/blogs/data-protection-and-covid-19>.

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

be limited in line with Article 52(1) CFREU, provided the essence of the right is preserved. As the European Data Protection Board (hereafter 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]

In part 1 I elaborate a hypothetical test for permissible limitations on the right to data protection, thereby outlining criteria to assess measures that collect personal data. In part 2 I discuss how some sample data-driven measures, including measures that collect health data, comply with the various stages of the test. In particular, every measure is discussed with respect to the specific stage of the test for permissible limitations that it conflicts with. In particular: thermal scanner guns exemplify the presence of an overlooked interference; self-check forms defy the presence of a legal basis; S.I.s for contact logging and locator forms fail the quality of the law test; the Vaccine Information System 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 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 pandemic purposes, and adopt a blueprint strategy for processing for pandemic purposes.

<https://www.qmul.ac.uk/law/news/responding-to-covid-19/items/covid-19-european-rules-for-using-personal-data.html>.

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

[17] Department of Health, 'Ethical Framework for Decision-making in a Pandemic' (17 April 2020) https://www.gov.ie/en/publication/dbf3fb-ethical-framework-for-decision-making-in-a-pandemic/; Andrea Mulligan, 'The Ethics of Lockdown: Transparency, Accountability and Community Involvement' (*COVID-19 Law and Human Rights Observatory, 15 July 2020*); Fundamental Rights Agency, 'Covid-19', <https://fra.europa.eu/en/themes/covid-19>; Amedeo Santosuosso, 'La regola, l'eccezione e la tecnologia' (2020) *BioLaw Journal – Rivista di BioDiritto Special Issue* 1/2020, 609.

1. 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 CFREU,[18] which enjoys the same legal status as the Treaties and is applicable by virtue of Art. 29.4 - 29.6 of the Constitution of Ireland.[19] The CFREU'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, i.e. 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 Art 52(1) CFREU and the applicable law, e.g. Art. 23 (1) (e) GDPR[22] and Section 60 Data Protection Act 2018[23] (hereafter DPA 2018). In the following I conceptualise the steps of a test for permissible limitations, drawn from Art 52(1) CFREU in light of data protection law, which will form the basis of the analysis of select data-driven pandemic measures.

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

[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 Review of the Law on the Retention of and Access to Communications Data (April 2017), p. 55 <http://www.justice.ie/en/JELR/Review_of_the_Law_on_Retention_of_and_Access_to_Communications_Data.pdf/Files/Review_of_the_Law_on_Retention_of_and_Access_to_Communications_Data.pdf>.
[20] Opinion of 10 January 2019 of AG Szpunar *in Google LLC v CNIL*, Case C-507/17, ECLI, para 55.
[21] Judgment of 17 December 2015 in *Åkerberg Fransson*, C-617/10, EU:C:2013:105, para 29.
[22] 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), OJ L 119/1.
[23] 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 europeen 2019); Rónán Kennedy and Maria Helen Murphy, Information and Communications Technology Law in Ireland (Clarus Press 2017), pp. 97-130.

The steps of a test for permissible limitations forming the criteria for the analysis of data-driven measures are drawn from Art 52(1) CFREU, *Digital Rights Ireland,*[24] CJEU and European Court of Human Rights (hereafter ECtHR) case law, guidance by the EDPS and the EDPB in light of CJEU and ECtHR case law, and finally the applicable law. The assessment of permissibility 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, Art 52(1) CFREU requires to discount a potential infringement of the essence of the right,[25] that is the very substance of the right. The interference must then be justified in light of objectives of general interest recognised by the Union, following which come the necessity and proportionality tests. These various steps are discussed in greater detail below

1.1.1 Interference with the right to personal data protection

The CJEU has consistently said that the processing of personal data that fall within the scope of EU data protection law constitutes an interference with the right to the protection of personal data.[26] The following illustrates when data-driven measures use personal data and fall within the scope of the applicable law.

1.1.1.1 Are data-driven measures based on personal data?

[24] *Judgment of 8 April 2014 in Digital Rights Ireland and Seitlinger and Others, Joined cases C-293/12 and C-594/12, EU:C:2014:238*, paras 35-46.
[25] Ibid. § 39-40.
[26] E.g. Ministerio Fiscal, 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).

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 him or her, or makes him or her identifiable when combined with other pieces of information (Art 4(1) GDPR). Here lies a catch of data protection law; the growing pool of data available, and improved data science and statistical techniques, keep broadening the scope of 'identifiable' data[27] and narrowing the scope of the antonym, 'anonymous' data.

Data that are anonymous on their own, such as those captured by motion sensors,[28] 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, that is information that has undergone a process of erasure which no longer permits the identification of an individual. Anonymised data are outside the scope of the applicable law, provided data subjects are not re-identified. If, conversely, information enabling the re-identification of individuals is kept separate but is still available to the controller, then data are considered to be pseudonymised (Art. 4 (5) GDPR) and subject to the applicable law.

Recital 26 GDPR establishes the relative nature of 'anonymity', which depends 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. This provision is virtually identical to Recital 26 of repealed Directive 95/46,[29] which was interpreted in *Patrick Breyer.*[30] There, the Court followed the systematic interpretation by AG Campos Sanchez-Bordona,[31] whereby

[27] 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.
[28] 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.
[29] 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) OJ L 281.
[30] Judgement of 19 October 2016 in *Patrick Breyer*, Case C-582/14, ECLI:EU:C:2016:779.
[31] 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.

'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 the Directive and the GDPR 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 with three criteria: singling-out, linkability and inference.[32] 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,[33] as foreseen by the Vaccine Information System, 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 section 2.1).

1.1.1.2 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 (Art. 2(1)(c) GDPR), whereby information collected "by a natural 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, e.g. online, the

[32] EDPB, 'Guidelines 04/2020', p. 5.
[33] Gianclaudio Malgieri, 'Data protection and research: A vital challenge in the era of COVID-19 pandemic' (2020) 37 *Computer Law & Security Review* 37 https://doi.org/10.1016/j.clsr.2020.105431; 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' (21 April 2020). In Ireland: S.I. No. 314/2018 - Data Protection Act 2018 (Section 36(2)) (Health Research) (Amendment) Regulations 2019.

household exception no longer applies, turning individuals into data controllers within the scope of the GDPR.[34]

The GDPR[35] 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.[36] The GDPR and DPA 2018 are particularised and complemented[37] by two *leges speciales* transposed into Irish law. The first is the Law Enforcement Directive for processing for law enforcement purposes.[38] The second is the e-privacy Directive (hereafter EPD),[39] 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 Art. 5 (3) is concerned, information society services.[40]

EDP rules on the processing of traffic and especially location data, defined in Artts. 2(b) and 2(c),[41] are the reason why Covid-19 apps could not be forced on people to automate contact tracing. Art. 15 EPD enables the restriction of the scope of rights and obligations contained in Article 9 (as well as 5 and 6), but only for a strictly enumerated[42] list of objectives, a list which does not include public health. As a result, instruments adopted *qua* exception pursuant to Art.

---

[34] 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 Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, para 55.
[35] 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), OJ L 119/1.
[36] A&L Goodbody, 'Contact Tracing Apps – A Privacy Primer', Focus on Covid-19 (2020), <https://www.algoodbody.com/files/uploads/news_insights_pub/COVID-19_-_Contact_Tracing_Apps_A_Privacy_Primer.pdf>.
[37] Judgement of 3 October 2018 in *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2018:788, para 31.
[38] 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, OJ L 119/89; transposed into Irish law by the DPA 2018.
[39] 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, OJ L 201 (E-privacy Directive); transposed into Irish law by S.I. 336/2011.
[40] EDPB, 'Guidelines 04/2020' (21 April 2020).
[41] '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.
[42] '…the list of objectives … is exhaustive, as a result … access must correspond, genuinely and strictly, to one of those objectives'. *Ministerio Fiscal*, para 31.

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.[43] 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 which is for the referring court to make.[44] 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.

It is worth noting that the draft Regulation set to repeal the EPD[45] makes provisions for processing traffic and location data to protect the vital interest of a natural person,[46] which "may include for instance processing necessary for humanitarian purposes, including for monitoring epidemics".[47] The GDPR and DPA 2018 are the relevant pieces of applicable law for data-driven measures reviewed in section 2.

1.1.2 Whether the interference is in accordance with the law

The requirement to be 'in accordance with the law' refers to the need for (i) a legal basis (lawfulness) that (ii) meets parameters of quality (legality) 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.[48] Data protection legislation contains rules on lawfulness of processing and legality drawn from the RoL, starting with the principles enshrined in Art. 5 GDPR – lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation

[43] Following judgment of 21 December 2016 in *Tele2 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.
[44] *Ministerio Fiscal*, paras 53-57.
[45] 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)).
[46] Ibid. Article 6b(1)(d).
[47] Ibid. Recital 17a
[48] Judgment of 6 October 2020 in La Quadrature du Net and Others, C-511/18, ECLI:EU:C:2020:791, para 103.

and integrity and confidentiality – which apply to the processing of any personal data.[49] For instance, the principles of lawfulness, fairness and transparency enshrined in Art. 5 (1)(a) GDPR can be said to stem from the rule of law.[50] 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*,[51] for fulfilling the data protection principles, in the form of technical and organisational measures commensurate with the risks entailed by the processing (Art. 24 GDPR). In other words, in order to benefit from the processing, the controller must safeguard the data so as to protect the concerned data subjects[52] – which turns the data controller into the *de facto* gatekeeper for data subjects' rights.

1.1.2.1 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 Covid-19 can take place under different legal bases.[53] 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 and Section 53 DPA 2018.[54]

[49] Combined reading of the judgment of 29 June 2010 in *Bavarian Lager Ltd*., C-28/08 P, ECLI:EU:C:2010:378, para 61 judgment of 13 May 2014 in *Google Spain and Google*, C-131/12, EU:C:2014:317, para 96.
[50] Lee A. Bygrave, *Data Privacy Law. An International Perspective* (Oxford University Press, 2014).
[51] The responsibility of the controller is commensurate to their role in the processing, Judgement 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.
[52] E.g. Judgment of 5 June 2018 in *Wirtschaftsakademie Schleswig-Holstein*, Case C-210/16, ECLI:EU:C:2018:388, para 28; *GC, AF, BH, ED v Commission nationale de l'informatique et des libertés (CNIL)*, Case C-136/18, ECLI:EU:C:2019:772, para 43.
[53] DPC, 'Data Protection and Covid-19'.
[54] See chapter 3 in Róisín A Costello, David Fennelly and Maria Grazia Porcedda, 'Data Protection and the Covid-19 Pandemic' (2021) Covid-19 Law and Human Rights Observatory, https://www.tcd.ie/law/2020.21/Data-Protection-and-COVID19%20Report.pdf.

Employers must protect their employees under the Safety, Health and Welfare at Work Act 2005, which, together with Article 9(2)(b) GDPR, provide a legal basis to process personal data concerning health.[55] 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 (Art 6(1)(a) GDPR) and the legitimate interests pursued by the controller (Art 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.[56] 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*[57] and Art. 6(1)(f) GDPR.[58]

The most suitable bases for public authorities are Article (6)(1)(e) GDPR and Section 38 DPA 2018; these are necessity 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 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 (Articles 6(3) and 6(2), Recitals 10 and 45) this legal basis to apply only when laid down in Member State (or EU) law to which

[55] For the UK, see Ruby Reed-Berendt and Edward Dove, Healthcare Workers' Data and Covid-19 Research, UK-Reach project (2020).
[56] Rónán Kennedy, 'Data Protection and COVID-19'.
[57] 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.
[58] "Such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data".

the controller is subject. 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 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 Art. 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.

1.1.2.2 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, but that in all circumstances the 'law' must respect the parameters of quality proper of a 'law'.[59] 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 the antecedent of Article 23 GDPR.[60] Furthermore, case law has stressed that, the most serious the interference, the strongest the

[59] Recital 41 of the GDPR. European Data Protection Board, Guidelines 10/2020 on restrictions under Article 23 GDPR (2020), p. 7, referring in particular to the European Court of Human Rights, 14 September 2010, Sanoma Uitgevers B.V. v. The Netherlands, EC:ECHR:2010:0914JUD003822403, paragraph 83. None of the measures reviewed in these pages explicitly aim at restricting the scope of the exercise of the right as in Article 23 and Recital 73 GDPR. Some processing operations need to be mandated by additional instruments (e.g. Articles 6(1)(c) and 6(1)(e), 9(2)(h) and (I) GDPR, Sections 38, 51 and 53 DPA 2018).
[60] Judgment of 1 October 2015 in *Bara and Others*,C-201/14, ECLI:EU:C:2015:638, para 40.

guarantees must be.[61] 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 in section 2 and the conclusions.

For the lawful bases laid down in Articles 6(1)(c) and (e), criteria for the quality of the law are contained in Article 6(3) and Recital 45. 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 Art.6(1)(e). The law must 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 Art. 6(3) appear necessary to respect, protect and fulfil the right, protect its essence[62] and comply with the substantive requirements of the rule of law, i.e. 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,[63] but also because the

[61] See, among others, *Tele 2 Sverige*.
[62] 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.
[63] To this effect, see European Data Protection Supervisor (EDPS), Concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 7 November 2019.

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 who to approach to enforce their rights.[64] Clarifying the nature of the controller is also relevant to understand who should be the recipient of data collected under guidance.[65]

In Irish law, Section 36 DPA 2018 addresses 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 60). The adoption of delegated legislation is not mandatory, though provisions such as Section 53 DPA 2018 require that suitable 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 Art. 23 (1). Yet, the requirements for derogating legislation listed in Art. 23(2) are similar to those contained in Article 6(3) and Recital 45, as the list is formulated in an open-ended manner.

1.1.3 Whether the interference is compatible with the essence

[64] Judgment of 1 October 2015 in *Weltimmo*, C-230/14, EU:C:2015:639; *Wirtschaftsakademie Schleswig-Holstein*.

[65] Müge Fazlioglu, Confusion as to how to share data with public authorities (*International Association of Privacy Professionals*, 21 April 2020) <https://iapp.org/news/a/sharing-covid-19-data-with-government-authorities-guidance-from-dpas/>.

The CJEU identified two elements that are the essence of Art. 8 CFREU: 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, and to protect it against unlawful access and processing."[66] 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, crushes the essence and becomes automatically impermissible. It should be noted that the requirement of compatibility with the essence is a source of academic debate[67] and that the assessment of a breach of the essence is therefore questionable.

1.1.4 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.

1.1.5 Whether the interference is necessary and proportionate

[66] Opinion 1/15 of the Court (Grand Chamber), ECLI:EU:C:2017:592, para 150.
[67] Among many, Maja Brkan, The concept of essence of fundamental rights in the EU legal order: Peeling the onion to its core, European Constitutional Law Review (2018) 2 pp. 332 – 368; Maria Grazia Porcedda, On boundaries. In search for the essence of the right to the protection of personal data, in Privacy and Data Protection: The Internet of Bodies, in Leenes et al. (eds) (Hart Publishing 2018); Lorenzo Della Corte, A right to a rule: On the substance and essence of the fundamental right to personal data protection. In Hallinanet al. (eds.), Data protection and privacy: Data protection and democracy (Hart Publishing 2020); Dara Hallinan, The Essence of the Right to the Protection of Personal Data: Essence as a Normative Pivot (2021 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3890861).

The EDPS published two toolkits, one for necessity,[68] the other for proportionality,[69] each based on a four-stepped methodology drawing from the ECtHR and CJEU case-law, as well as the work of the EDPS and EDPB, and premised on the idea that the double requirements of necessity and proportionality[70] must be assessed on a case-by-case basis. Although these methods are geared to decision-makers preparing legislation capable of infringing the right, they are nonetheless also useful for appraising the permissibility of interferences effected by existing legislation. Each test is made of four parts. 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*.[71] The first step is to assess the legitimacy, or importance, of the objective, and its effectiveness and efficacy, i.e. 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-

[68] EDPS, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit (2017) <https://edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf>.
[69] EDPS, Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (2019).
[70] For their connection, see EDPS, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit (2017), p. 5.
[71] Ibid. p. 7. EDPS (2019) FOOTNOTE, p. 10, referencing Digital Rights Ireland, paras 46, 65 and 69, and Schrems paras 92-93.

driven measures reviewed in this article reaches the proportionality stage of the test, as they all fail at previous stages, as I demonstrate next.

2. Review of select 'under the radar' data-driven measures

This section reviews several 'under the radar' pandemic data-driven measures in light of the test for permissible limitations just illustrated. Note that this section reviews a subset of measures deserving analysis. For instance, the Contact Management Programme, arguably a crucial component of the public health response to Covid-19, is not reviewed here for want of technical documentation enabling to ascertain its permissibility.[72] This section presumes that data-driven pandemic measures satisfy the requirement of meeting an objective of public interest. Each section reviews single measures against relevant steps of the test for permissible limitations. In section 2.1 I show how thermal scanner guns can interfere with the right to data protection, meaning that their use must be assessed against the test for permissible limitations. In section 2.2 I appraise self-check forms against the need for the 'presence of a legal basis', and instruments for contact logging against the requirement of 'quality of the law', which jointly make up the requirement of 'in accordance with the law'. In section 2.3 I apply the necessity test to the Vaccine information System. In section 2.4 I examine the compatibility of data-driven measures with the respect for the essence of the right.

2.1 Interference with the right to data protection: thermal scanner guns

[72] Health Protection Surveillance Centre, Contact Tracing Guidance <https://www.hpsc.ie/a-z/respiratory/coronavirus/novelcoronavirus/guidance/contacttracingguidance/>.The CMP is analysed in Chapter 1 in Róisín A Costello, David Fennelly and Maria Grazia Porcedda, 'Data Protection and the Covid-19 Pandemic' (2021) *Covid-19 Law and Human Rights Observatory,* https://www.tcd.ie/law/2020.21/Data-Protection-and-COVID19%20Report.pdf.

Thermal scanner guns taking individuals' temperature are widely used in a variety of settings. Models of thermal scanners capable of storing the temperature taken, and only the temperature taken (e.g. 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.[73] 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[74] 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 (e.g. infrared thermal scanners) at airports to be ineffective 'in identifying infectious individuals and limiting spread of disease.'[75]

The continued use of 'guns' that do not collect personal data could be no more than 'hygiene theatre'.[76] 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 pass the test of necessity and proportionality.

[73] Christina Etteldorf, 'EU Member State Data Protection Authorities Deal with COVID-19: An Overview', (2020) *European Data Protection Law Review* 6(2) 265.
[74] For purely illustrative purposes, see <https://realityi.com/thermoscanner/>.
[75] Health Information and Quality Authority, 'Thermal Screening' (6 August 2020) <https://www.hiqa.ie/hiqa-news-updates/hiqa-review-finds-mass-thermal-screening-airports-covid-19-ineffective>.
[76] Derek Thompson, Hygiene Theater is a Huge Waste of Time, *The Atlantic* (27 July 2020), <https://www.theatlantic.com/ideas/archive/2020/07/scourge-hygiene-theater/614599/>.

2.2 'In accordance with the law': self-check forms and measures for contact logging

2.21 Presence of a legal basis: self-check forms

In general, few data-driven measures are adopted pursuant to a clear and unambiguous legal basis.[77] 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.[78] The 2021 Government Roadmap no longer encourages individuals and recreational facilities to undertake contact logging.[79] Non-essential businesses are instead encouraged to take 'protective measures' which, for the hotel sector specifically, include 'customer details recorded for contact tracing process'.[80] 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, as were reviewed earlier, and self-check forms for visitors to business premises, e.g. retailers[81] and even

[77] See Chapter 1 in Róisín A Costello, David Fennelly and Maria Grazia Porcedda, 'Data Protection and the Covid-19 Pandemic' (2021) *Covid-19 Law and Human Rights Observatory,* https://www.tcd.ie/law/2020.21/Data-Protection-and-COVID19%20Report.pdf.

[78] Maria Grazia Porcedda, 'Data Protection Implications of Data Driven Measures Adopted in Ireland at the Outset of the Covid-19 Pandemic' (2021) *European Data Protection Law* 2/21.

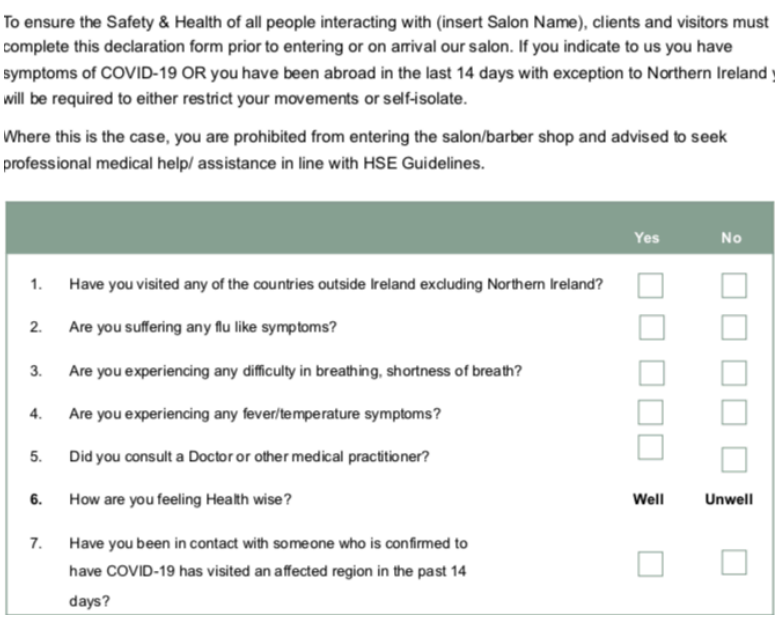
[79] Department of the Taoiseach, COVID-19 Resilience and Recovery 2021 - The Path Ahead (15 September 2020) <https://www.gov.ie/en/campaigns/resilience-recovery-2020-2021-plan-for-living-with-covid-19/?referrer=http://www.gov.ie/en/publication/cf9b0d-new-public-health-measures-effective-now-to-prevent-further-spread-o/>. See in particular pages 8 and 11.

[80] Department of the Taoiseach, COVID-19 Resilience and Recovery 2021 - The Path Ahead (15 September 2020)<https://www.gov.ie/en/campaigns/resilience-recovery-2020-2021-plan-for-living-with-covid-19/?referrer=http://www.gov.ie/en/publication/cf9b0d-new-public-health-measures-effective-now-to-prevent-further-spread-o/>, p. 50.

[81] NSAI, 'COVID-19 Retail Protection and Improvement Guide' (2020), version 21, <https://www.nsai.ie/images/uploads/general/NSAI-COVID-19-Retail-Guide.pdf> p. 19.

universities, and customers of hairstylists and beauticians[82]- forms that process data concerning health (Art. 4 (15) GDPR).

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).[83] For such a reason national DPAs disagree as to the permissibility of self-health screening questionnaires for employees,[84] let alone visitors. Data collected through self-check forms can be lawfully processed under the combined legal bases of Art. 6(1)(c) and Art. 9(2)(b), but only if, as the DPC notes, 'the processing is necessary[85] for the purpose of carrying out its obligations in the field of employment (such as the obligations arising under the 2005 Act)'.[86] If self-check forms emanated from the Safety, Health and Welfare at Work Act 2005, then they would have a legal basis and the measure should be reviewed against other steps of the test for permissible limitations. However, their necessity remains to be demonstrated and it is argued that self-



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 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 HABIC visitor questionnaire

[82] Hair and Beauty Industry Confederation of Ireland (HABIC), 'Re-Opening Guidelines for Irish Hair Salons and Barber Shops' (June 2020) <https://irishhairfed.com/wp-content/uploads/2020/06/Re-Opening-Guidelines-for-Irish-Hair-Salons-and-Barber-Shops-June-2020.pdf>, p. 17. Paul Moore, Rules you have to follow in Ireland's hairdressers and barbers upon reopening, *Irish Mirror* (9 May 2021) <https://www.irishmirror.ie/news/irish-news/rules-you-follow-irelands-hairdressers-24072385>

[83] Judgment of 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, paras 44 and 67.

[84] Christina Etteldorf, 'EU Member State Data Protection Authorities Deal with COVID-19: An Overview', (2020) *European Data Protection Law Review* 6(2) 265.

[85] This links to the principles of fairness and purpose limitation.

[86] DPC, Data Protection implications of the Return to Work Safely Protocol (June 2020), p. 3.

check forms in their current form are disproportionate and amount to an impermissible interference with the right to data protection.[87]

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 (hereafter NSAI)[88] 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 the law requirements illustrated earlier (section 1.1.2.2), including clarity and foreseeability,[89] which enable citizens to adjust their conduct. In spite of its publicity,[90] the Government Roadmap is unlikely to meet quality of the law parameters: not only does the it not meet the parameters required by Article 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,[91] 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.

2.2.2 Quality of the law: instruments for contact logging, including locator forms

[87] Elsewhere I show that the lack of a 'generic data protection notice' that 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 Chapter 1 in Róisín A Costello, David Fennelly and Maria Grazia Porcedda, 'Data Protection and the Covid-19 Pandemic' (2021) *Covid-19 Law and Human Rights Observatory,* https://www.tcd.ie/law/2020.21/Data-Protection-and-COVID19%20Report.pdf. See also Maria Grazia Porcedda, Businesses need to be careful with personal data during pandemic, The Irish Times (20 July 2020) <https://www.irishtimes.com/opinion/businesses-need-to-be-careful-with-personal-data-during-pandemic-1.4308278>.

[88] National Standards Authority of Ireland (NSAI), 'COVID-19 Workplace Protection and Improvement Guide', version 7 (2020), p. 16.

[89] Judgment of 25 May 2021, Big Brother Watch and Others v UK, n. 58170/13, 62322/14 and 24960/15,ECLI:CE:ECHR:2018:0913JUD005817013.

[90] EDPS (2017), p. 4

[91] 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.

Three Statutory Instruments (S.I.s) were adopted to support contact tracing efforts. One such S.I. gives statutory basis to the recording of customer details by hotels, eateries and bars for contact logging purposes.[92] Two S.I.s specifically require international passengers entering Ireland to 'retain', 'give or otherwise make available' to a relevant person or a member of the Garda Síochána a negative COVID-19 test result,[93] and to fill in and hand in to the 'relevant person' a locator form. [94]

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 S.I.s identify different controllers, and in one case (locator forms) controllership has changed from one versions 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 their 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 S.I.s presuppose a transfer of personal data currently lacking the requisite interinstitutional arrangements. [95]

---

[92] 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 <https://www.gov.ie/en/publication/04388-informal-consolidation-of-covid-19-temporary-restrictions-regulations/>.

[93] Regulation 5(1) of S.I. No. 135 of 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 June 14th 2021, <http://www.irishstatutebook.ie/eli/2021/si/135/made/en/print>, expiring on July 19th. <https://www.gov.ie/en/collection/1f150-view-statutory-instruments-related-to-the-covid-19-pandemic/>.

[94] S.I. No 45 of 2021: Health Act 1947 (Section 31A - Temporary Requirements) (Covid-19 Passenger Locator Form) Regulations 2021 <http://www.irishstatutebook.ie/eli/2021/si/45/made/en/print>. S.I. 45 of 2021 revokes S.I. No. 181 of 2020: Health Act 1947 (Section 31A - Temporary Restrictions) (COVID-19 Passenger Locator Form) Regulations 2020. There, the Health Service Executive was also a data controller.

[95] See Chapter 3 in Róisín A Costello, David Fennelly and Maria Grazia Porcedda, 'Data Protection and the Covid-19 Pandemic' (2021) *Covid-19 Law and Human Rights Observatory,* https://www.tcd.ie/law/2020.21/Data-Protection-and-COVID19%20Report.pdf.

The jigsaw puzzle effect is worsened by the fact that all S.I.s 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 S.I.s 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 S.I.s present exceptions to the term for data retention identified in legislation. Thirdly, none of the S.I.s satisfies in full the requirements of Article 6(2) and (3). To exemplify the issue, the next section focusses in particular on locator forms.

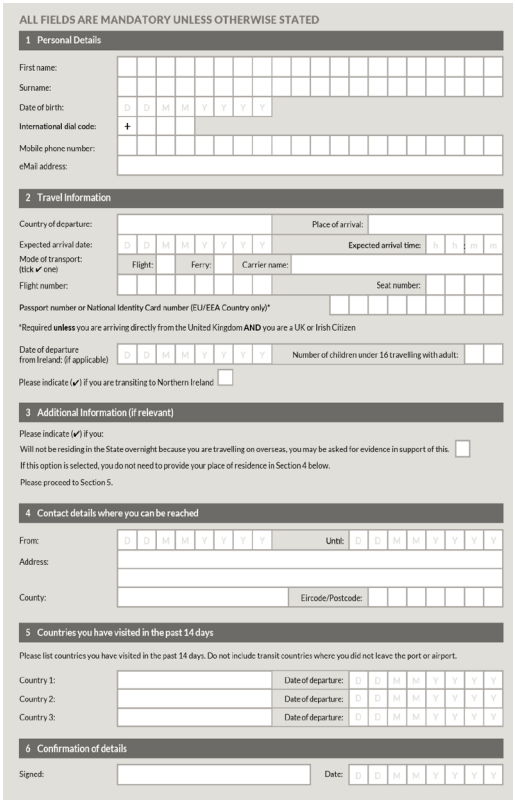
2.2.2.1 Example of passenger locator forms

The degree of intrusiveness of locator forms[96] 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 S.I. 181/2020, because the use of automated means of processing

[96] Ibid., defined in Regulation 3. The form is available at <https://cvd19plf-prod1.powerappsportals.com/en-us/> and <https://www.gov.ie/en/publication/ab900-covid-19-passenger-locator-form/?referrer=http://www.gov.ie/locatorform/>. The previous version can be found at: <http://www.irishstatutebook.ie/eli/2020/si/181/made/en/print>. The Regulations also cover PLF receipts, which are not reviewed here.

can facilitate further, unauthorised processing compared to manual processing. Legislation mandating the collection of travel forms constitutes a legal basis in line with Art. 6(1)(e)GDPR, but in its current form it arguably lacks the elements to ensure lawful and fair processing identified in section 1.1.2.2.

The revised locator form collects more categories of personal data than the revoked S.I. 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', i.e. 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[97] at which he or she intends to reside' (Regulation 2).


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 Locator form 2021 (extract)

[97] This was added in SI 45/2021.

Furthermore, in common with all S.I.s, 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 S.I.s seen in this section (2.2.2) and is highly problematic. First, it *de facto* broadens the purposes for which data can be used, which sits uncomfortably with the 'quality of the law' tenet,[98] in that the purpose '*a criminal offence*' is unspecified, specifically it is broader than the penal provisions identified in the S.I., and thus does not provide sufficient clarity and foreseeability (on purpose limitation, see section 2.5). Secondly, 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 interference with data protection could be deemed impermissible and lead to a partial invalidation of the S.I.s.

2.2.3 Compatibility of data-driven measures with 'in accordance with the law': an overview

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

[98] 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) https://tcdlaw.blogspot.com/2020/07/quarantine-after-international-travel.html.

identification of the data controller, though not always with clarity for all categories. Some S.I.s 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 Art. 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.[99] 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'.

2.3 Necessity: the Vaccine Information System (VIS)

The 'vaccine information system' (hereafter VIS) is 'an end-to-end comprehensive digital solution to support the delivery and rollout of the nationwide COVID-19 vaccination programme.'[100] 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),[101] and policies, i.e. the European Commission eHealth Network.[102] The VIS is justified by an objective of public interest and therefore the present analysis focusses on necessity.

[99] Oran Doyle, 'Quarantine after international travel'; Oran Doyle, 'Leaving Home: Reasonable Excuses, Vagueness, and the Rule of Law' (*COVID-19 Law and Human Rights Observatory Blog*, 5 June 2020) <http://tcdlaw.blogspot.com/2020/06/leaving-home-reasonable-excuses.html>; Oran Doyle, 'On Legal Obligations and Golf-Gate' (*Ibid.*, 28 August 2020) <available at https://tcdlaw.blogspot.com/2020/08/on-legal-obligations-and-golf-gate.html>.

[100] HSE, Vaccine Information System for COVID-19 Vaccination Programme Data Protection Impact Assessment, Version 1.8 (22 April 2021), p. 6, <https://www.hse.ie/eng/gdpr/data-protection-covid-19/data-protection-impact-assessment.pdf>.

[101] Ibid., p. 32-33

[102] Ibid., p. 20.

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 (hereafter 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 secondly, the 'table of version' does not enable the reader to track and identify changes to the text.[103] 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.[104] 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[105] 'within Salesforce data centres within the European Economic Area (EEA)'.[106] The overall data controllers are the HSE and GPs (with respect to their patients' data), as well as the Central Statistics Office, whereas IBM is identified as a processor, alongside pharmacists, Healthcare Facilities (acting under Section 38 of the Health Acts 2004), private hospitals, and DPER. Salesforce is a subprocessor.

All these entities receive patient data, which include the following personal information: first name, middle name (optional), surname, mother's maiden name, date of birth, PPSN, sex, nationality, ethnicity, the Individual Health Identifier (IHI),[107] home address, county, country, Area code/Eircode, GP name, occupation, prioritisation category, vaccination status, contraindication to vaccination, health state, pregnancy, Covid history, and vaccination

[103] Ibid.
[104] Ailbhe Daly, Private information of thousands who received Covid vaccine exposed in HSE blunder, 25 February 2021, Irish Mirror <https://www.irishmirror.ie/news/irish-news/health-news/private-information-thousands-who-received-23566568>.
[105] Ibid. p. 13.
[106] Ibid. p. 35.
[107] 'Generated for each person registered for a vaccination', ibid. p. 27.

history.[108] The HPRA and Department of Health are the recipients of anonymised data. Patient data is to be retained in perpetuity, though it is not clear on what system and therefore whether processors will also retain data in perpetuity.[109] The DPIA discusses risks and mitigation strategies, including generic technical and organisational measures and a description of data security measures.

2.3.1 Analysis of VIS

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 Central Statistics Office. Such objectives appear *prima facie* necessary, but based solely on the DPIA it appears difficult to carry out the last 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,[110] for the 'purposes of processing personal data for the vaccination programme', rather than for each specific purpose pursued by the different data controllers (e.g. 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).[111] As for the remaining, long and broad, list of personal data to be collected, the DPIA only describes when the data is collected, not why they

[108] Ibid. pp. 26-28
[109] Ibid. p. 23
[110] HSE, Vaccine Information System for COVID-19 Vaccination Programme Data Protection Impact Assessment, Version 1.8 (22 April 2021), p. 31.
[111] Ibid. p 18.

are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.[112] 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';[113] it is unclear why these companies, who have European and particularly Irish offices,[114] 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 vaccine data outside the EEA' but does not provide any further details as to such arrangements, e.g. whether they rely on binding corporate rules or standard contractual clauses. The transfer of VIS data to the US, following the CJEU's decision in *Facebook Ireland and Schrems,*[115] 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 CFREU.[116] Once more, an analysis of effectiveness and minimal intrusion is not possible.

Fourthly, all data collected are to be retained in perpetuity; this decision is a serious breach to the principle of storage limitation, as it is unrelated to specific purposes and specific controllers/processors. It is also unclear whether the processors and sub-processors would retain such data in perpetuity as well.[117] This point effects maximal intrusion, and therefore challenges necessity.

---

[112] Ibid. p. 26.
[113] Ibid. p.34
[114] Ibid. P. 34. https://www.salesforce.com/eu/company/locations/; https://www.research.ibm.com/labs/europe/#ireland .
[115] Judgment of 16 July 2020 in Facebook Ireland and Schrems, C-311/18, ECLI:EU:C:2020:559.
[116] Judgment of 16 July 2020 in Facebook Ireland and Schrems, C-311/18, ECLI:EU:C:2020:559, para 105.
[117] HSE, Vaccine Information System for COVID-19 Vaccination Programme Data Protection Impact Assessment, Version 1.8 (22 April 2021), p. 23.

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 (i.e. risk #10 and mitigation #10) does not adequately take into account.[118] 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 PPS numbers, addresses, names and contact details about thousands of vaccine recipients 'despite earlier warnings by data chiefs'.[119] Moreover, the list of technical and organisational security measures provided, which on paper appear adequate,[120] will need to be updated in years to come, e.g. 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.

2.4 Respect for the essence: a transversal shortcoming?

Following Art 52(1) CFREU, the assessment of whether the essence is infringed, i.e. whether is the right is emptied of its core elements,[121] must be done immediately after the analysis of lawfulness. However, as mentioned earlier (section 1.1.3), a methodology to ascertain respect

[118] Ibid., p. 26.
[119] Ailbhe Daly, Private information of thousands who received Covid vaccine exposed in HSE blunder, 25 February 2021, Irish Mirror <https://www.irishmirror.ie/news/irish-news/health-news/private-information-thousands-who-received-23566568>.
[120] An assessment is impossible without reference to detailed technical measures and specific standards.
[121] EDPS, Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (2019).

of the essence is hitherto missing, and the operationalisation of the concept is debated by scholarship. The following analysis is, therefore, exploratory.

A purposive reading of the law would suggest that 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,'[122] 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'.

Moreover, all S.I.s and most data-driven measures, except the VIS DPIA, lack provisions addressing the integrity and confidentiality of the data collected. As before, a purposive interpretation of the law in light of the essence would invalidate most measures. Irrespective of this finding, 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.[123] 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% in 2020[124] and by 50% in 2021.[125] The use of cloud computing solutions, which the VIS relies on, can increase the costs of a data breach by exfiltrated/lost unit.[126]

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

[122] Opinion 1/15 of the Court (Grand Chamber), ECLI:EU:C:2017:592, para 150.
[123] DPC, Protecting Personal Data When Working Remotely (12 March 2020), <https://www.dataprotection.ie/en/protecting-personal-data-when-working-remotely-0>.
[124] The Journal.ie, Garda stats: Domestic violence, drug possession and fraud on the rise during lockdown (12 June 2020) <https://www.thejournal.ie/pandemic-garda-crime-stats-5121435-Jun2020/>.
[125] Conor Lally, Online crime jumps by half last year as cyber fraud increases, The Irish Times (12 March 2021) <https://www.irishtimes.com/news/crime-and-law/online-crime-jumps-by-half-last-year-as-cyber-fraud-increases-1.4508513>
[126] Larry Ponemon, 2017 Cost of Data Breach Study <https://www.ibm.com/account/reg/us-en/signup?formid=urx-15763>. The CMP also relies on cloud computing.

arrangements between the controller and the processor.[127] Importantly, the security incident did not seem to affect the VIS.[128] 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.'[129]

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 the right to data protection. The analysis was conducted on the basis of a hypothetical test for permissible limitations that incorporates elements of the applicable law. 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 statutory instruments for contact logging is insufficient, elements of the Vaccine Information System 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

[127] As elaborated in Maria Grazia Porcedda, 'Patching the Patchwork: appraising the regulatory framework on cyber security breaches (2018) Computer Law and Security Review 35(2).
[128] Eoin Butler, Life as a Covid Vaccine Volunteer, *The Irish Times* (13 June 2021).
[129] Health Information and Quality Authority, Review of information management practices for the National Incident Management System (NIMS) within the HSE (May 2021) <https://www.hiqa.ie/sites/default/files/2021-05/Review-of-information-management-practices-for-the-National-Incident-Management-System-(NIMS)-within-the-HSE.pdf>.

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[130] and the consequences this carries for legality.[131] 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.[132] However, better use could have been made 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,[133] and the related judicial saga has traced the boundaries of pandemic 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 statutory instruments for contact logging and the publication of the VIS DPIA but, as seen, such measures could benefit from correction.[134]

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

[130] Alan Greene, 'Ireland's Response to the COVID-19 Pandemic' (*VerfBlog*, 11 April 2020) https://verfassungsblog.de/irelands-response-to-the-covid-19-pandemic/; Conor White, 'The Oireachtas and Mandatory Face Coverings' (*COVID-19 Law and Human Rights Observatory Blog*, 13 July 2020) http://tcdlaw.blogspot.com/2020/07/the-oireachtas-and-mandatory-face.html; 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.
[131] 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).
[132] 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.
[133] Rónán Kennedy, 'Data Protection and COVID-19'.
[134] Porcedda (2021), fn 11.

the HSE, and undermine trust in the provision of public services. On this account, I formulate three recommendations.

The first recommendation is to publish *a facsimile data protection notice for all those entities that process personal data for Covid-19 purposes*, to step up the effectiveness of data subject rights. Such notice could be in the guise of Covid-19 posters affixed to the walls (or shown on the website) of businesses and public institutions.

Secondly, I recommend to a*ggregate and publish documentation concerning the digital components of the Contact Management Programme*, to match the level of transparency achieved for the Covid-19 app and enable public scrutiny, including from a cybersecurity perspective. This includes *opening up the DPIA carried out for the VIS to public consultation* and clarifying where patient data are being transferred to and under what arrangements set out in Chapter 5 of the GDPR.

Thirdly and most importantly, I recommend *to adopt an overarching instrument that contains the blueprint for data processing for pandemic purposes*. In the Irish adaptation of data protection law, this would be ideally a measure of the rank of a statutory instrument or higher, laying down the legal basis for the most common forms of processing operations, such as contact logging and transfers of data to the HSE, in a clear, precise, and foreseeable manner. Accordingly, such instrument should specify issues of controllership, purpose limitation and integrity and confidentiality of data, alongside other requirements stemming from Art 6(2) and (3) GDPR, the DPA 2018 and the test for permissible limitations I elaborate in this article. Indeed, the steps of the test for permissible limitations illustrated in these pages could be repurposed as a list of criteria that the blueprint must follow. The obligation to consult the DPC would help to ensure adherence to the law. The law should clarify when the processing of data concerning health is necessary and proportionate. 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.