Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

DATA PROTECTION AND THE COVID-19 PANDEMIC

Authors: Róisín Costello, David Fennelly and Maria Grazia Porcedda

A Public Policy Report of the

COVID-19 LEGAL OBSERVATORY

School of Law, Trinity College Dublin

https://www.tcd.ie/law/tricon/covidobservatory/

Harnessing Trinity's Collective Expertise for the Greater Good

ABOUT THE COVID-19 LEGAL OBSERVATORY

Harnessing Trinity's Collective Expertise for the Greater Good

COVID-19 presents an unprecedented public health crisis. New laws were introduced at a rapid pace on the basis of compelling public health and economic concerns. Universities play a vital role in ensuring that laws are effective but also that rights and fundamental freedoms are protected insofar as possible, even in emergency circumstances.

To address this, the COVID-19 Law and Human Rights Observatory[1] of Trinity College Dublin engages in research across the full range of Ireland's legal response to COVID-19. Academics in the Observatory the work with research assistants to identify, aggregate, contextualise, explain, and analyse the legal components of Ireland's COVID-19 response. We aim both to inform the public and to provoke public debate.

The Observatory's Blog[2] publishes academic commentary on Ireland's legal response to COVID-19 as it evolves. The Observatory also provides an unofficial consolidated version of Ireland's regulatory response to COVID-19, as well as a range of official guidance documents. This is the first public policy report of the Observatory. Other policy work of the Observatory is focused on data protection issues relating to the pandemic, and the public health response to the pandemic. The Observatory is also completing a report on behalf of the Irish Human Rights and Equality Commission that analyses how Ireland has deployed emergency powers in response to the pandemic.

The work of the Observatory is supported by the Trinity College Dublin COVID-19 Response Fund.

[1] https://www.tcd.ie/law/tricon/covidobservatory/index.php.

[2] https://tcdlaw.blogspot.com/.

Contributors to this Report

Maria Grazia Porcedda (Chapter 1)

Maria Grazia Porcedda is Assistant Professor in Information Technology Law at the School of Law, Trinity College Dublin. Her research focusses in particular on cybercrime, cybersecurity, data protection, privacy and surveillance in EU law.

David Fennelly (Chapter 2)

David Fennelly is an Assistant Professor at the School of Law, Trinity College Dublin and a barrister practising from the Law Library, Dublin.

Róisín Costello (Chapter 3)

Róisín Á Costello is an Assistant Professor of Law at the School of Law and Government at Dublin City University and a barrister. Her research focuses primarily on privacy law and policy, EU law and the interaction of law and linguistic identity.

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

INTRODUCTION

The aim of the Observatory's policy report series is to contribute actively to public debate and to shape public policy and law reform through analysing and evaluating Ireland's response to COVID-19.

In its statement of 19 March 2020 on the processing of personal data in the context of the COVID-19 outbreak, the European Data Protection Board stated that data protection rules, such as the GDPR, did not hinder measures taken in the fight against the coronavirus pandemic and that, even in these exceptional times, data controllers and data processors must ensure the protection of personal data of data subjects.

The COVID-19 pandemic has, however, presented significant challenges for data protection law: not only for data controllers and processors, whether in the public or private sector, but also for data subjects and indeed data protection authorities at national and EU level. By its nature, the management of a major public health emergency, such as COVID-19, has very significant implications for the protection of personal data, involving as it does very widespread and large-scale processing of personal data, including sensitive health data which is the subject of special protection under the GDPR.

Against this backdrop, it is not surprising that data protection has been a prominent feature of public debate around the response to COVID-19, from the early stages of the pandemic to the more recent relaxation of public health restrictions. In this Report, we examine a number of key aspects of the Irish response to the data protection challenges presented by COVID-19.

Chapter 1 provides an overview of mandatory and commonplace data-driven measures adopted in Ireland up until the beginning of July 2021 that have gone under the radar, and consequently eschewed public scrutiny. Sections include contact logging, locator forms for international passengers, the Covid-19 Contact Management Programme and the Vaccine Information System. The chapter appraises the compliance of such data-driven measures with data protection law.

Chapter 2 examines the COVID Tracker App, which was designed and deployed to assist with contact tracing in respect of COVID-19. While questions have been raised about the effectiveness of the App, the App has been heralded as a success on a number of fronts, both in terms of the process leading up to its launch and its relatively high uptake among the population.

Chapter 3 provides an overview of the laws governing data sharing between public bodies in Ireland during the period of Covid-19, with a particular focus on health data and how the Data Sharing and Governance Act 2019 will impact this sharing landscape.

In this dynamic field, where laws, regulations and practices are continually evolving both in response to the public health situation and other developments, the Report is intended to offer a snapshot of the Irish experience in dealing with the data protection challenges presented by COVID-19 as of July 2021.

RECOMMENDATIONS

This public policy report is focused on reflections on how public policy can provide support to underpin individuals, communities, businesses and the economy in Ireland against the contextual backdrop of COVID-19. The main conclusions and recommendations of the Report are as follows:

From chapter 1

- *Adopting an overarching instrument that contains the blueprint for data processing for pandemics*. 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 transfer of data to the HSE, in a clear, precise, and foreseeable manner. Such instrument should specify issues of controllership, purpose limitation and integrity and confidentiality of data, alongside other requirements found in the applicable law as discussed in these pages. The obligation to consult the DPC would help ensuring adherence to the law. The law should clarify when the processing of data concerning health is necessary and proportionate.
- *In the interim, and to the extent it is still relevant at the time this report is published, amending legislation* currently enabling the collection of passenger data, guests and members of the public attending hotels and premises serving food and drinks.
- *Issuing a facsimile data protection notice for all those entities that are processing 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 currently affixed to the walls (or shown on the website) of businesses.
- *Aggregating and publishing documentation concerning the digital components of the CMP*, to match the level of transparency achieved for the Covid-19 app and enable public scrutiny, including from a cybersecurity perspective.
- Clarifying to what country VIS data are being transferred to and under what arrangements set out in Chapter 5 of the GDPR, as well as *opening up the DPIA carried out for the VIS to public consultation.*
- *Discussing due diligence concerning the uptake of technologies for continued tele-working,* both from a health and safety and cybersecurity perspective.

From chapter 2

- Building on the experience with the COVID Tracker App, greater effort should be made to promote transparency, public consultation and engagement in the development of significant public sector and public-private projects that involve large scale processing of personal data, including through the timely publication of Data Protection Impact Assessments.
- Careful consideration must be given to the core data protection principles enshrined in Article 5 GDPR – including the principles of data minimisation, purpose limitation and storage limitation – at all stages of the design and development of significant public sector and public-private projects that involve large scale processing of personal data.
- In the context of the COVID Tracker App, caution is required in adding new and further functions, such as the feature allowing the uploading of the COVID Digital Certificate. Where it is desired to offer new functions and features which differ from those originally provided for, providing a separate application which data subjects may or may not choose to download and use is in principle the preferable approach.
- In order to assess the effectiveness of the COVID Tracker App in a holistic fashion with a view to informing future decision-making and data protection practices, the Health Service Executive and/or the Department of Health should support the carrying out of independent research and analysis of the experience with, and the utility of, the App in contributing to contact tracing efforts during the COVID-19 pandemic.

From chapter 3

- Provision should be made without delay by way of Ministerial Regulations for the sharing of special category data concerning health and the governance of same under ss.63-66 of the Data Sharing and Governance Act 2019.
- Particular concern should be afforded to ensuring that the sharing of health data between public bodies is mapped in order to facilitate clarity about who has access to, and control of data within organisations and Departments, when and where data is being duplicated and, based on this information, how the security of such data and its sharing can be facilitated and ensured most effectively.
- Serious consideration should be given to the introduction of similar governance and transparency requirements for the sharing of public data, and in particular public health data, with third parties i.e., non-State actors.

CHAPTER 1: DATA PROTECTION IMPLICATIONS OF 'UNDER THE RADAR' DATA-DRIVEN MEASURES FOR CONTACT LOGGING, CONTACT TRACING & HEALTH CHECKING

Maria Grazia Porcedda

Introduction[3]

Since the beginning of the pandemic policymakers have adopted several data-driven measures to contain the spread of Covid-19. With the exception of the Covid-19 App, which received great publicity,[4] other mandatory, and therefore commonplace data-driven measures have gone under the radar, and consequently eschewed public scrutiny. This chapter reviews the most common personal data-driven measures adopted[5] in Ireland *up until the beginning of July 2021* and appraises their compliance with data protection law.

The chapter is divided into two parts. Part 1 illustrates measures that collect personal data, including health-related data, and is organised thematically. Sections include contact logging, locator forms for international passengers, the Covid-19 Contact Management Programme and the Vaccine Information System. Part 2 reviews the compliance of such measure with data protection law, following an overview of the criteria used to assess compliance. The chapter offers recommendations before drawing conclusions.

[3] I wish to express my gratitude to Cian Henry for the excellent research assistance and the many helpful suggestions he gave while drafting this report. All errors are mine. The law is correct as stated as of June 2021.
[4] See chapter 2 by David Fennelly.
[5] A review of measures adopted between March and August 2020 is discussed 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.

Part 1: data-driven measures explained

A. Contact logging

Contact logging by individuals and organizations

Contact logging means recording the presence of a person in a given place at a given time and is the backbone of contact tracing. Contact logging was at the heart of the first guidance for reopening society issued by the Department of Health and the Department of the Taoiseach[6] (hereafter the Government Roadmap). The revised Government Roadmap no longer encourages individuals and recreational facilities to undertake contact logging, possibly in light of the limited success of such measures to contain the spread of the virus.[7] Guidance for the reopening of non-essential businesses mentions 'protective measures', which, for the hotel sector specifically, include 'customer details recorded for contact tracing process.'[8] Unlike the Government Roadmap, updated guidance by the National Standards Authority of Ireland (hereafter NSAI) retains the original advice[9] to log contacts by means of a two-part template created by NSAI. End-users include retailers,[10] and sectoral organizations such as the Hair and Beauty Industry Confederation of Ireland (hereafter HABIC).[11]

---

[6] Department of Health and Department of the Taoiseach, 'Face coverings and other public health measures in place right now' (13 August 2020) <https://www.gov.ie/en/publication/cf9b0d-new-public-health-measures-effective-now-to-prevent-further-spread-o/>.

[7] As described 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. 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. See also chapter 2 by David Fennelly.

[8] 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.

[9] "All organizations, and where possible individuals, should keep a contact log to facilitate HSE contact tracing in the event of a COVID-19 case in the workplace. This may be through the use of sign in sheets, clocking systems, visitor logbooks, delivery personnel details, third party service provider visitor information. This information should be stored securely, maintained centrally and readily available upon request."National Standards Authority of Ireland (NSAI), 'COVID-19 Workplace Protection and Improvement Guide', version 7 (2020), p. 16.

[10] 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.

[11] The original template's 'company' field now features the customer's address. 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. The guidance remains unchanged. 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>

Furthermore, two authorities issued guidance *mandating* keeping a log of contacts. The updated 'Work Safely Protocol'[12] requires ('must' and 'will') employers to keep a log of contacts to facilitate contact tracing and inform workers and others of the purpose of the log. Contact logging is recommended ('should') for 'recording visits to the site(s) by workers/others as well as visits by workers to other workplaces'.[13] The HSE Health Protection Surveillance Centre (hereafter HPSC) also *requires* food service businesses to log the contact details for the person making the booking.[14]

Contact logging by hotels and premises serving alcohol was given statutory footing by the Health Act 1947 (Section 31A - Temporary Restrictions) (Covid-19) (No. 2) Regulations 2021.[15] There,[16] a 'specified person' in relation to 'a relevant premise' or a 'relevant accommodation premises'[17] must ('shall') 'make a record of the time and date that each relevant guest, or each member of the public, is permitted, or otherwise granted, access to such premises, and the name and telephone number of each relevant guest and each member of the public'. By laying down that a specified person 'may request a relevant guest to provide the specified person with the relevant guest's name and telephone number', Regulation 13(4) seems to imply that the collection of name and number is not mandatory, yet a guest must ('shall') provide name and number if asked. Unlike paragraphs (2) and (3), paragraph (4) is not

[12] Department of Business, Enterprise and Innovation (DBEI), Work Safely Protocol. COVID-19 National Protocol for Employers and Workers (14 May 2021) <https://enterprise.gov.ie/en/Publications/Publication-files/Work-Safely-Protocol.pdf>, p. 5. This substitutes the previous Department of Business, Enterprise and Innovation (DBEI) and Department of Health, 'Return to Work Safely Protocol' (9 May 2020) <https://www.gov.ie/en/publication/22829a-return-to-work-safely-protocol/>.

[13] Department of Business, Enterprise and Innovation (DBEI), Work Safely Protocol. COVID-19 National Protocol for Employers and Workers (14 May 2021) <https://enterprise.gov.ie/en/Publications/Publication-files/Work-Safely-Protocol.pdf>, p. 20.

[14] HSE Health Protection Surveillance Centre (HSPC), 'COVID-19: Guidance for Food Service Businesses' v 1.3 (11 March 2021) <https://www.hpsc.ie/a-z/respiratory/coronavirus/novelcoronavirus/guidance/employersemployeesguidance/HPSC%20COVID-19%20guidance%20-%20food.pdf>. "Keep contact details for the person making the booking. Explain that the reason for keeping these records is to provide them to Public Health for contact tracing in the event that someone becomes ill with COVID-19.These records should be kept for 1 month." P. 13

[15] Health Act 1947 (Section 31A - Temporary Restrictions) (Covid-19) (No. 2) Regulations 2021.

[16] N.B.: Regulation 13 was amended on July 27th 2021, after this report was drafted. An informal consolidation of the Regulations and related amendments up to June 2021 is available at <https://www.gov.ie/en/publication/04388-informal-consolidation-of-covid-19-temporary-restrictions-regulations/>. The frequent changes to the legislation illustrate the difficulty of keeping abreast of developments.

[17] 'Relevant premises' and 'Relevant Accommodation Premises' are defined at Reg 13(8) and 'Specified premises' at Reg 13(5)(b).

a penal provision for the purposes of section 31A of the Act of 1947.[18] Relevant data include time and date, and possibly name and telephone number of each guest or member of the public, which a relevant person must ('shall') retain for a period of 28 days (Regulation 13(3)). Records can be accessed, within the 28-day period, by the Garda Síochána for inspection purposes falling within their duties as laid down in the Regulations, and by a person appointed by the Health Service Executive for the purposes of the Covid- 19 Contact Management Programme.

According to Regulation 14, data can be processed: (a) by a specified person for complying with the requirements laid down in Regulation 13; (b) by the Health Service Executive for the purposes of the identification, tracing and contacting of persons who have been in contact with potential persons who have been diagnosed, or suspected of having been infected, with Covid-19; and (c) a member of the Garda Síochána for monitoring compliance by a specified person with, or enforcing, these Regulations. Individuals or organisations under letters (a) to (c) are data controllers in relation to the purposes specified under each letter. Data processed for such purposes must also be retained for 28 days (Regulation 14(3)). However, where time, date, names and telephone numbers 'are required for the purposes of the prevention, investigation, detection or prosecution of *a criminal offence*'[19], the data 'may be processed for as long as they are required for such prevention, investigation, detection or prosecution' and only deleted after they are no longer required (Regulation 14 (4)). Regulation 14 mentions the General Data Protection Regulation (hereafter GDPR) but not the Data Protection Act 2018 (hereafter DPA 2018).

[18] The Regulations are silent as to liability in case guests or members of the public were to provide a fake name and telephone number. The situation is not academic. Contact tracing following a super-spreader event that took place in Sardinia, Italy in the summer of 2020 was hindered by the fact that attendees to an event gave fake personal information for contact logging purposes. Ollie A Williams, 3,000 Billionaire Clubbers Flee Quarantine on Italian Island, Forbes (28 August 2020) <https://www.forbes.com/sites/oliverwilliams1/2020/08/28/3000-billionaire-clubbers-flee-quarantine-on-italian-island/>.

[19] Emphasis added.

Locator form for international passengers (Covid-19 Passenger Locator Form)

The latest version of delegated legislation adopted by the Minister for Health[20] requires ('shall')[21] international passengers arriving in Ireland from outside the island to fill in and hand in to the 'relevant person' a locator form.[22] Legislation refers to the collection of passengers' "contact details", that is a telephone number and email address (Regulation 2), as well as the "place of residence", meaning "the place, or places, in the State or in Northern Ireland[23] at which he or she intends to reside during the relevant period" (Regulation 2). Pursuant to Regulation 7, those contact details may be used by a relevant person to contact an international passenger to provide public health information within 14 days from his or her arrival.

Unlike the Covid-19 Passenger Locator Form contained in the 2020 Regulations, the 2021 Regulations identify the Minister for Health as the sole data controller. [24] The Minister for Health is also a processor, alongside the Health Service Executive and 'one or more relevant persons', among others for 'recording and verifying information regarding the place of residence of an international passenger' and 'identifying, tracing and contacting [of] persons who have been in contact with persons who have been diagnosed, or are suspected of having been infected, with Covid-19' (Regulation 8(1)(a)). The Garda Síochána is an identified processor for 'the purposes of the prevention, detection, investigation or prosecution of a criminal offence arising from a contravention of a provision stated to be a penal provision under these Regulations or under S.I. No. 44 of 2021' (Regulation 8(1)(b)). Processed data must be erased 28 days after the date of arrival, with the exception of 'when they are required

[20] 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. The Regulations were revised to 14 June 2021. It is unclear how the introduction of vaccine passports (e.g. <https://www.dfa.ie/irish-embassy/usa/news-and-events/covid19-updates/>) will affect the Regulations.

[21] Pursuant to Regulation 4(5), the Regulations laying down the obligation to fill in and give the relevant Covd-19 form 'are penal provisions for the purpose of section 31A of the Health Act 1947 (No. 28 of 1947)'.

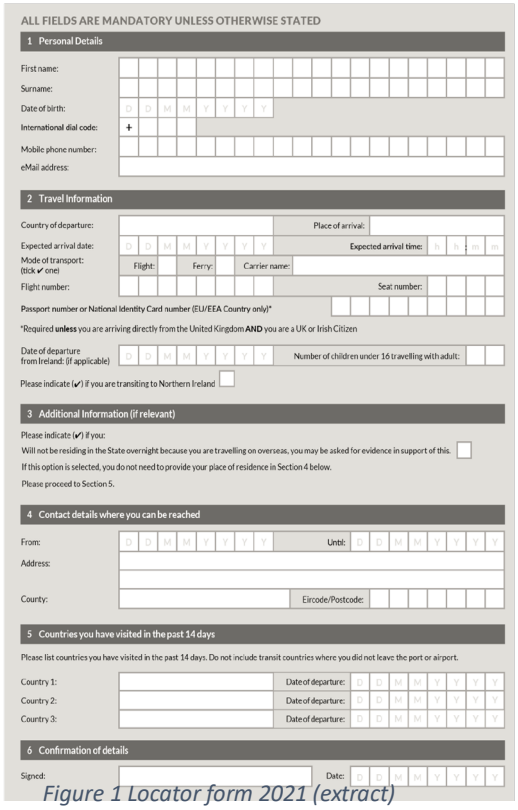
[22] Ibid., defined in Regulation 3. The form is available at <https://cvd19plf-prod1.powerappsportals.com/en-us/> and <https://www.gov.ie/en/publication/ab900-covid-19-passenger-locator-form/?referrer=http://www.gov.ie/locatorform/>. The previous version can be found at: <http://www.irishstatutebook.ie/eli/2020/si/181/made/en/print>.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

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

[24] Ibid., Regulation 8(2). Cf. 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.

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.

There are substantial differences between the Covid-19 Passenger Locator Form contained in the Regulations 2021 (figure 1) and that contained in the 2020 Regulations (figure 2). The 2021 digital version contains a section on 'travel information' that 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 citizen, who are exempted; it also collects information such as flight and seat numbers. The S.I. will elapse on August 31st 2021.


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

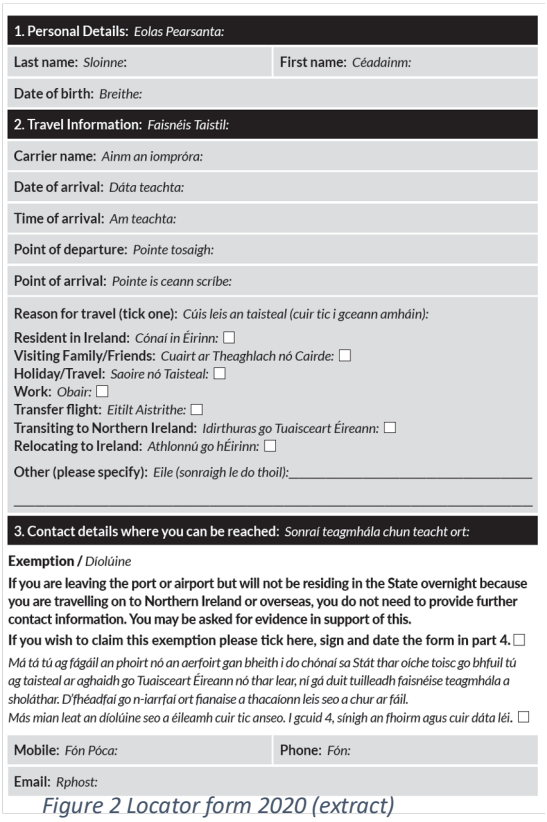
Please list countries you have visited in the past 14 days. Do not include transit countries where you did not leave the port or airport.

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 1 Locator form 2021 (extract)


1. Personal Details: *Eolas Pearsanta:*

Last name: *Sloinne:*
First name: *Céadainm:*
Date of birth: *Breithe:*

2. Travel Information: *Faisnéis Taistil:*

Carrier name: *Ainm an iompróra:*
Date of arrival: *Dáta teachta:*
Time of arrival: *Am teachta:*
Point of departure: *Pointe tosaigh:*
Point of arrival: *Pointe is ceann scribe:*

Reason for travel (tick one): *Cúis leis an taisteal (cuir tic i gceann amháin):*
Resident in Ireland: *Cónaí in Éirinn:* ☐
Visiting Family/Friends: *Cuairt ar Theaghlach nó Cairde:* ☐
Holiday/Travel: *Saoire nó Taisteal:* ☐
Work: *Obair:* ☐
Transfer flight: *Eitilt Aistrithe:* ☐
Transiting to Northern Ireland: *Idirthuras go Tuaisceart Éireann:* ☐
Relocating to Ireland: *Athlonnú go hÉirinn:* ☐
Other (please specify): *Eile (sonraigh le do thoil):*_____

3. Contact details where you can be reached: *Sonraí teagmhála chun teacht ort:*

Exemption / *Díolúine*

If you are leaving the port or airport but will not be residing in the State overnight because you are travelling on to Northern Ireland or overseas, you do not need to provide further contact information. You may be asked for evidence in support of this.

If you wish to claim this exemption please tick here, sign and date the form in part 4. ☐

Má tá tú ag fágáil an phoirt nó an aerfoirt gan bheith i do chónaí sa Stát thar oíche toisc go bhfuil tú ag taisteal ar aghaidh go Tuaisceart Éireann nó thar lear, ní gá duit tuilleadh faisnéise teagmhála a sholáthar. D'fhéadfaí go n-iarrfaí ort fianaise a thacaíonn leis seo a chur ar fáil.
Más mian leat an díolúine seo a éileamh cuir tic anseo. I gcuid 4, sínigh an fhoirm agus cuir dáta léi. ☐

Mobile: *Fón Póca:*
Phone: *Fón:*
Email: *Rphost:*

Figure 2 Locator form 2020 (extract)

A. *Collection of health-related data*

Health self-check surveys and questionnaires

'Self-check' surveys, "where data subjects answer questions related to their health (such as stating symptoms),"[25] are mandatory when returning to the workplace and the Irish Data

[25] European Data Protection Board (EDPB), 'Guidelines 03/2020' p. 5.

Protection Commission (hereafter DPC) has conceded that they can be legitimately used under specific circumstances;[26] in practice, their use extends beyond employees. In keeping with the 2020 Government Roadmap *obligation* ("must") for employers to adhere to the Return to Work/Work Safely Protocol[27] (based on the Health, Safety and Welfare at Work Act 2005), the 2021 Government Roadmap contains a section detailing inspections to assess compliance with the Protocol. The Protocol contains a data protection supplement, updated in November 2020,[28] which touches on contact logging, temperature testing and the pre-return to work form,[29] which has remained unchanged since its original adoption. The Health and Safety Authority prepared a template containing a disclaimer that clarifies the form is for educational purposes only and should not be considered exhaustive.[30] The form is still intended to be "disposed of or destructed securely as soon as the Worker has returned to the

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 3 HABIC visitor questionnaire

[26] DPC, 'Data Protection and Covid-19' <https://www.dataprotection.ie/en/dpc-guidance/blogs/data-protection-and-covid-19> (6 March 2020).

[27] DBEI and Department of Health, 'Return to Work Safely Protocol' (9 May 2020) <https://www.gov.ie/en/publication/22829a-return-to-work-safely-protocol/>.

[28] DBEI and Department of Health, 'Data Protection - Work Safely Protocol', v. 2 (20 November 2020) <https://www.gov.ie/en/publication/7a143-data-protection-work-safely-protocol/>. The first version was accompanied by guidance by the DPC, 'DPC Summary on Data Protection implications of the Return to Work Safely Protocol' (July 2020) <https://www.dataprotection.ie/sites/default/files/uploads/2020-07/Data%20Protection%20implications%20of%20the%20Return%20to%20Work%20Safely%20Protocol.pdf >.

[29] HSA, 'COVID-19 Templates, Checklists and Posters' <https://www.hsa.ie/eng/topics/covid-19_coronavirus_information_and_resources/covid-19_business_supports/business_supports/work_safely_templates_checklists_and_posters/rtw_form_1dec20.pdf>.

[30] Moreover, "The information contained in this guidance ... is not intended to provide legal advice to you, and you should not rely upon the information to provide any such advice. We do not provide any warranty, express or implied, of its accuracy or completeness…"etc.

Workplace".[31] The Work Safely Protocol also applies to retailers but, as seen, the 2021 Government Roadmap only refers to unspecified 'protective measures'.[32]

Part two of the questionnaire issued by the NSAI for the workplace and retailers[33] aims to screen the health of *visitors* in addition to employees. Figure 3 shows an adaptation of the NSAI self-check questionnaire incorporated in Guidance issued by HABIC to allow salons and barbers to safely reopen.[34]

The Covid-19 Contact Management Programme (CMP) and its digital components

The Health Service Executive Covid-19 Contact Management Programme (CMP)[35] notifies 'results to people tested (or their nominated person)' and identifies and manages 'contacts of people who have COVID-19'.[36] The CMP includes "decentralised physical and virtual call-centres"[37] called Contact Training Centres (CTCs) operated by a team of circa 1500 people[38] "working in virtual contact tracing groups remotely. This group links in with a coordinator who manages rotas and provides oversight and support."[39]

---

[31] DBEI and Department of Health, 'Data Protection - Work Safely Protocol', v. 2 (2 December 2020) < https://www.gov.ie/en/publication/7a143-data-protection-work-safely-protocol/>, p. 5

[32] This is unlike the 2020 Government roadmap, which explicitly recommended retailers and commercial services to put 'measures' in place.

[33] National Standards Authority of Ireland (NSAI), 'COVID-19 Workplace Protection and Improvement Guide', version 7 (2020), p. 16 <https://www.nsai.ie/images/uploads/general/NSAI-COVID-19-Workplace-Guide.pdf>; NSAI, 'COVID-19 Retail Protection and Improvement Guide' (2020), version 21, <https://www.nsai.ie/images/uploads/general/NSAI-COVID-19-Retail-Guide.pdf>

[34] HABIC, 'Re-Opening Guidelines', p. 17; RTE, 'Hair salons outline guidelines for reopening early' (8 June 2020) <https://www.rte.ie/news/business/2020/0608/1146056-hairdressers-on-reopening/>. As mentioned earlier, this guidance remains unchanged.

[35] Health Protection Surveillance Centre, Contact Tracing Guidance <https://www.hpsc.ie/a-z/respiratory/coronavirus/novelcoronavirus/guidance/contacttracingguidance/>.

[36] HSE, Introduction to COVID-19 Contact Tracing Centres(CTCs), (23 October 2020), <https://www.connectunion.ie/wp-content/uploads/2021/01/COVID-19-Contact-Management-Programme-CMP-Overview.pdf>.

[37] HSE, 'COVID-19 Contact Management Programme (CMP) Overview' (29 June 2020), no longer available online.

[38] To begin with, staff was made of public servants, then personnel was hired ad hoc. Department of Health, COVID-19 Contact Tracing Centres: Your questions answered (28 May 2020) <https://www.gov.ie/en/publication/6a6e32-covid-19-contact-tracing-centres/>. The Irish Times (sponsored article), Building technology solutions to meet the challenges of the Covid-19 pandemic in Ireland (7 December 2020) <https://www.irishtimes.com/sponsored/microsoft/building-technology-solutions-to-meet-the-challenges-of-the-covid-19-pandemic-in-ireland-1.4425648>.

[39] HSE, 'FAQs' (no longer online) <https://www.hpsc.ie/a-z/respiratory/coronavirus/novelcoronavirus/guidance/contacttracingguidance/3.%20COVID-19%20Contact%20Tracing%20Centres%20(CTCs).pdf>.

In a Daíl debate held in May 2020, deputy Leddin enquired about the HSE contact tracing back office, particularly whether and how computer systems could be used "to complement the Covid tracker app" and help automate and accelerate that process. Then Minister for Health Simon Harris responded the government would look into computerised solutions and referred to the Health Tech Assessment.[40]

A dataset specification dating to April 2020 shows a number of computerised solutions are in place.[41] One is Healthlink, which is a 'web-based messaging service which enables the secure transmission of clinical patient information between Hospitals, Health Care Agencies and General Practitioners'; [42] GPs are registered as facilities in Healthlink.[43] Another -possibly novel- solution is Swiftqueue, which provides a platform to support booking and communications in the context of "Covid Swabbing, Covid Testing and Covid Vaccination Appointments to Staff and Patients."[44]

The dataset specification also mentions the development of Individual Health Identifiers (IHI)[45] and the CovidCare Tracker (CCT) system, a cloud-based solution deployed to track care given to COVID-19 patients and perform contact tracing, including tracking and managing calls through a password-protected[46] module.[47] As documented, it is "based on a web platform

[40] Dáil Deb 14 May October 2020, vol 993, col 2, p. 138 <https://data.oireachtas.ie/ie/oireachtas/debateRecord/dail/2020-05-14/debate/mul@/main.pdf>.
[41] HSE, COVID-19 Dataset Specification (16 April 2020), p. 5.
[42] At the time of writing, the website <www.healthlink.ie> was down. The eHealth Ireland website states "Operational since 1995 it has evolved over time and is now the national health messaging broker. The Healthlink team work in partnership with many stakeholders, professional organisations, practitioners and software vendors, to enhance electronic communication for healthcare. Healthlink has a proven track record in delivering IT solutions to GPs and hospitals and continues to be the cornerstone for many HSE eHealth initiatives." <https://www.ehealthireland.ie/a2i-hids-programme/healthlink/>.
[43] HSE, COVID-19 Dataset Specification (16 April 2020), p. 5.
[44] As advertised on the Swiftqueue website. The service is used by the HSE in Ireland and some NHS Trusts in the UK <https://www.swiftqueue.com/services.php>. See also HSE, 'COVID-19 Testing and Tracing. Roadmap to enhance capacity and turnaround' (14 May 2020), <https://www.hse.ie/eng/services/news/newsfeatures/covid19-updates/covid-19-testing-and-tracing-roadmap.pdf> .
[45] HSE, COVID-19 Dataset Specification (16 April 2020), p. 5. See section on the vaccine information system.
[46] HSE, 'FAQs' (no longer online) <https://www.hpsc.ie/a-z/respiratory/coronavirus/novelcoronavirus/guidance/contacttracingguidance/3.%20COVID-19%20Contact%20Tracing%20Centres%20(CTCs).pdf>. See also HPSC <https://www.hpsc.ie/a-z/respiratory/coronavirus/novelcoronavirus/guidance/contacttracingguidance/Leaflet%202.%20COVID-19%20Contact%20Tracing%20Centres%20(CTCs).pdf>.
[47] HSE, 'COVID-19 Contact Management Programme (CMP) Overview' (29 June 2020), no longer available online. Updated guidance (28 January 2021) is available at <https://www.hpsc.ie/a-z/respiratory/coronavirus/novelcoronavirus/guidance/contacttracingguidance/Leaflet%201%20CMP%20Overview.pdf>.

that allows a rapid, large scale system approach to address the documentation and management of Covid 19 in citizens on a national scale […] to streamline the suboptimal paper based system,… notify the results to people tested and to identify and manage contacts of known COVID-19 positive people."[48] The contact tracing component "has been developed in partnership with public health and the Chief Information Officer's team",[49] though it has since become known that companies Microsoft (Microsoft Dynamics 365 tool), Sysco Software Solutions and Tekenable collaborated with the HSE on the development of the CCT.[50] The CCT "incorporates collection of surveillance data, demographic data on cases and their contacts, and it enables automatic notification of negative results, referral for testing and active follow up communication. It also allows for reporting on CMP."[51] Patient's confidentiality is maintained by using pseudonymization, whereby each person is allocated a CovidCare Tracker ID. [52] The dataset specification lists mandatory and optional data that contact tracers need to collect.[53] Finally, the dataset specification also refers to the National/HSE Data Lake, which is the dataset resulting from data collected within the CTT,[54] hosted in the cloud, on Microsoft Azure, [55] and a real-time Dashboard. A Data Protection policy for contact tracing and testing purposes is published on the HSE website.[56] Unlike the Covid tracker App, the digital components of the Health Service Executive Covid-19 CMP, and similar initiatives abroad, have received relatively little attention by commentators. A list of digital services

[48] HSE, COVID-19 Dataset Specification (16 April 2020), p. 35, Appendix I.
[49] Ibid.
[50] The Irish Times (sponsored article), Building technology solutions to meet the challenges of the Covid-19 pandemic in Ireland (7 December 2020) <https://www.irishtimes.com/sponsored/microsoft/building-technology-solutions-to-meet-the-challenges-of-the-covid-19-pandemic-in-ireland-1.4425648>.
[51] HSE, 'COVID-19 Contact Management Programme (CMP) Overview' (29 June 2020), no longer available online.
[52] Ibid. See also 'Introduction to COVID-19 Contact Tracing Centres'(CTCs) (28 January 2021) https://www.hpsc.ie/a-z/respiratory/coronavirus/novelcoronavirus/guidance/contacttracingguidance/Leaflet%202.%20COVID-19%20Contact%20Tracing%20Centres%20(CTCs).pdf, p 2.
[53] HSE, COVID-19 Dataset Specification (16 April 2020).
[54] Question by Deputy Cullinane to the Minister for Health, 24967/20, 15 October 2020, <https://www.hse.ie/eng/about/personalpq/pq/2020-pq-responses/september-2020/pq-24967-20-pearse-doherty.pdf>.
[55] The Irish Times (sponsored article), Building technology solutions to meet the challenges of the Covid-19 pandemic in Ireland (7 December 2020) <https://www.irishtimes.com/sponsored/microsoft/building-technology-solutions-to-meet-the-challenges-of-the-covid-19-pandemic-in-ireland-1.4425648>.
[56] HSE, Data Protection – Covid 19 <https://www.hse.ie/eng/gdpr/data-protection-covid-19/data-protection-covid-19.html>.

developed to manage the pandemic can also be found in Appendix 4(a) of the HSE National Service Plan 2021 on eHealth and ICT Capital, together with the related rollout stage and the capital allocation, for a total of €115 million (figure 8).[57]

Programme	Primary HSE Service Area	Key 2021 Deliverables	Roll-out in 2021
COVID Case Tracker (CCT)	Test and Trace	– Maintenance and further development of CCT for COVID-19 patient triage and registration, assessment, testing and result notification, contact tracing and surveillance	Y
COVID Tracker App	OoCIO	– Maintenance and further development of public COVID Tracker App	Y
COVID Test Appointment Scheduling (SwiftQueue)	Community	– COVID-19 appointment scheduling platform	N
HealthLink (COVID)	OoCIO	– Maintain streamlined processes for COVID-19 e-referral and priority Service Plan initiatives	Y
BI Data Lake	OoCIO	– Data ingestion engine, data lake, targeted dashboards	Y
Enterprise Collaboration	OoCIO	– Microsoft Teams deployed across the organisation	Y
Death Registration Solution	Acute	– Death notification and registration service (phase 1) in place, enabling digital notification within 24 hours of death	Y
Enterprise Scheduler	Community	– Pilot roll-outs (and Proofs of Concept currently) implemented and evaluated – Agreed Strategy for Enterprise Scheduler across health services	Y

Figure 8 eHealth and ICT capital, p. 146

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."[58] This section draws on the data protection impact assessment (DPIA) first released in December 2020, as revised in April 2021. The processing to take place within the VIS, and parts thereof, is justified by an objective of public interest drawing from multiple frameworks, such as the Health Identifiers Act 2014, Section 31 of the Health Act 1947, the Infectious Diseases Regulations 1981 (SI 390/1981),[59] and with prospective integration within the European Commission eHealth Network.[60]

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[61] 'within Salesforce data centres within the European Economic Area (EEA)'.[62] 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

[57] HSE, National Service Plan 2021 <https://www.hse.ie/eng/services/publications/serviceplans/national-service-plan-2021.pdf>.
[58] 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>.
[59] Ibid., p. 32-33
[60] Ibid., p. 20.
[61] Ibid. p. 13.
[62] Ibid. p. 35.

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),[63] 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.[64] 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.[65] The DPIA discusses risks and mitigation strategies, including generic technical and organisational measures and a description of data security measures. Version 0.6 incorporates comments from the DPC, possibly in relation to prior consultation.[66] 16 amendments of the document, which was not made available for public consultation, were recorded as of the beginning of July 2021.[67]

Part 2. Evaluation of data-driven measures from a data protection law perspective

Do the data-driven measures illustrated in this chapter comply with data protection law? Given the dual nature of data protection law, whereby legislation not only lays down obligations, but also gives substance and specifies the right to the protection of personal data enshrined in Article 8 of the Charter, assessing compliance is not straightforward. Section A explains the criteria used to assess compliance of the measures reviewed in Part 1 with data protection law. Section B reviews the compliance of single measures, followed by a discussion of issues transversal to all measures (Section C).

[63] 'Generated for each person registered for a vaccination', ibid. p. 27.
[64] Ibid. pp. 26-28
[65] Ibid. p. 23
[66] A news report points to the DPC being consulted about risks. The DPIA does not clarify the matter. 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>.
[67] N.B. The document was edited 5 times during the summer of 2021, so as to include, among other things, feedback by the DPC. Unfortunately the table of versions thus far does not specify which sections were edited.

A. Criteria for assessing compliance of data-driven measures with data protection law

All data-driven measures reviewed here process personal data and fall within data protection law's material and territorial scope (Articles 2 and 3 GDPR). The GDPR[68] and DPA 2018 will apply in most cases,[69] and their provisions are particularised and complemented,[70] among others, by the Law Enforcement Directive transposed by means of the DPA 2018.[71]

Data protection law must be interpreted in light of the Charter,[72] which enjoys the same legal status as the Treaties and applies by virtue of Articles 29.4 - 29.6 of the Constitution of Ireland.[73] This is because the secondary – EU and national – legislation gives substance and specifies[74] the right to data protection enshrined in Article 8 of the Charter, and must be interpreted in light of the right. The Charter's scope of application is as broad as the scope of EU law,[75] and must be respected even when Member States derogate from EU law, i.e. at times of emergency such as the Covid-19 pandemic.[76] In other words, where such measures entail the processing of personal data and fall within the remit of the applicable law, then they must do so in compliance with the right, even when the measures lawfully restrict the right.

[68] 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.
[69] 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>.
[70] Judgement of 3 October 2018 in *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2018:788, para 31.
[71] 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.
[72] Judgment in *Österreichischer Rundfunk*, C-465/00, C-138/01 and C-139/01, EU:C:2003:294, para 68.
[73] 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>.
[74] Judgment of 13 May 2014 in Google Spain and Google, C-131/12, ECLI:EU:C:2014:317, para 69.
[75] Opinion of 10 January 2019 of AG Szpunar *in Google LLC v CNIL*, Case C-507/17, ECLI, para 55.
[76] Judgment of 17 December 2015 in *Åkerberg Fransson*, C-617/10, EU:C:2013:105, para 29.

The dual nature of data protection law – imposing regulatory compliance and implementing a fundamental right – means that data-driven measures must respect the rule of law, which includes legality, respect for fundamental rights and proportionality. Thus, one way to assess data-driven measures' compliance to data protection law is to review them in light of a test for permissible limitations. It will be for a different publication to review the measures in light of such a test, but for the purposes of this chapter it suffices to state that: (i) regulatory obligations and human rights requirements are intertwined in data protection law; (ii) most data-driven measures covered in this chapter would struggle to pass the legality test, either formally or substantively; (iii) substantive shortcomings are arguably due to an incomplete or unsound implementation of data protection requirements.

The dual nature of data protection law is embodied, among others, by the principles enshrined in Art. 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.[77] For instance, the principle of lawfulness, fairness and transparency enshrined in Art. 5 (1)(a) GDPR can be said to stem from the rule of law.[78] 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*,[79] for fulfilling the data protection principles, in the form of technical and organizational 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.[80] The data controller is the *de facto* gatekeeper for data subjects' rights.

[77] 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.
[78] Lee A. Bygrave, *Data Privacy Law. An International Perspective* (Oxford University Press, 2014).
[79] 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.
[80] 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.

More specifically on legality, the Irish DPC notes that processing personal data for the sake of containing Covid-19 can take place under different legal bases.[81] 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 of DPA 2018.[82] 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.[83] 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.[84]

As acknowledged by commentators,[85] 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. 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.

The most suitable bases for public authorities are Article (6)(1)(e) and Section 38 DPA 2018; these are necessity for either the exercise of official authority vested in the controller (e.g. the Covid-19 CMP) or the performance of a task carried out in the public interest (e.g. Covid-19 passenger locator forms). 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 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

[81] DPC, 'Data Protection and Covid-19'.
[82] See chapter 3 by Róisín Á Costello.
[83] Ibid.
[84] Ibid.
[85] Rónán Kennedy, 'Data Protection and COVID-19'.

question of what role private individuals or organisations have when collecting personal data in the context of the HSE Covid-19 CMP. Ideally, such doubts should be removed by means of the adoption of an officially published instrument mandating contact logging, opening 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.

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, but that in all circumstances the 'law' must respect the parameters of quality proper of a 'law'.[86] 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, 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 ('should') to 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[87] and comply with the substantive requirements of the rule of law, i.e. the quality of the law and proportionality.

[86] 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.

[87] 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.

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,[88] but also because the controller is the gatekeeper for the exercising 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.[89] Clarifying the nature of the controller is also relevant to understand who should be the recipient of data collected under guidance.[90]

In Irish law, Section 36 DPA 2018 addresses the introduction of suitable and specific measures for processing (and Section 60 DPA 2018 covers restrictions). An important feature is that 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).

In the following each measure is assessed against a combination of data protection principles and the criteria contained in Article 6(3) and Recital 45. The analysis highlights main areas of concern and does not intend to be exhaustive, as a fully-fledged data protection legal assessment is beyond the scope of this chapter.

B. Compliance of data-driven measures with data protection law

Compliance of contact logging with data protection law

Simple contact logging is of limited intrusiveness, but still needs to comply with the applicable law. The extent to which data protection law applies when individuals share their contact logs

[88] To this effect, see European Data Protection Supervisor (EDPS), Concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 7 November 2019.

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

[90] 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/>.

with the HSE is unclear. When, as it has happened, they act on its behalf, arguably individuals become processors.[91]

Two frameworks mandating contact logging can be said to have clear lawful bases. Processing under the Return to Work/Work Safely Protocol can be said to be based on Art. 6(1)(c) (compliance with a legal obligation to which the controller is subject). Contact logging by a relevant premise or a relevant accommodation premise under Regulation 13 of the Health Act 1947 (Section 31A - Temporary Restrictions) (Covid-19) (No. 2) Regulations 2021 can be said to be based on Article 6(1)(e) GDPR. The latter instrument is a welcome addition to what was originally unsuitable guidance, though in its current form the Regulations raise issues insofar as they enable further processing of personal data for law enforcement purposes, issues addressed in Part 2C.

The suitability of 'guidance' by the HSE, NSAI, DBEI and the Department of Health, addressing entities other than those covered by the Protocol and Regulations, to constitute a legal basis pursuant to Art. 6(1)(c) GDPR was[92] and remains questionable. The guidance issued is neither clear nor consistent; it lacks many of the provisions covered by Art 6(3) GDPR/Recital 45 (see Part2C) and does not adequately fulfil data protection principles. Guidance also does not clearly identify data controllers for contact logging purposes, which is problematic insofar as entities unaccustomed to processing personal data are concerned.[93]

Compliance of Covid-19 passenger locator forms with data protection law

The degree of intrusiveness of locator forms is arguably greater than simple contact logging, because such forms collect more categories of personal data and are imposed on all

[91] E.g. as Henry and Nuding noted, close contacts contacted their own close contacts when the HSE contact tracing capabilities became unable to process contacts. Cian Henry and Matthew Nuding, Ireland, Privacy and Covid19 Country Reports, Institute for Internet and the Just Society (2021), p. 67 https://irp-cdn.multiscreensite.com/34a95d4d/files/uploaded/Privacy%20%26%20Covid19%20Country%20Reports%202021.pdf.

[92] The rationale can be found 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.

[93] In more detail, Maria Grazia Porcedda, Under the radar: lessons from ordinary data processing in easing pandemic lockdown (2020) <https://tcdlaw.blogspot.com/2020/07/under-radar-lessons-from-ordinary-data.html>. Along similar lines, see Cian Henry and Matthew Nuding, Ireland, Privacy and Covid19 Country Reports, Institute for Internet and the Just Society (2021), p. 67 <https://irp-cdn.multiscreensite.com/34a95d4d/files/uploaded/Privacy%20%26%20Covid19%20Country%20Reports%202021.pdf>.

international passengers. Moreover, the use of digital locator forms is riskier than paper ones, 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 Art. 6(1)(e)GDPR, but in its current form it arguably lacks the elements to ensure lawful and fair processing identified earlier (Part 2A). The revised locator form collects more categories of personal data than the revoked S.I. 181/2020; however, such categories are not adequately reflected in the Regulations, which only explicitly refer to, and thus justify the need for, contact details and place of residence. Arguably the text should be amended to adequately reflect the necessity of the data for the purposes of the processing, in line with the principles of purpose specification and data minimisation.

Moreover, the S.I. lacks explicit provisions to ensure the confidentiality and integrity of the data collected. The instrument also raises issues insofar as it enables further processing of personal data for law enforcement purposes, issues addressed in Part 2C.

Compliance of health self-check forms with data protection law

Operations processing data concerning health (Art. 4 (15) GDPR), as many Covid-19 related measures do, deserve higher protection "as the context of their processing could create significant risks to the fundamental rights and freedoms" (Recital 51 GDPR) which can be seen as a serious interference.[94] Etteldorf[95] notes that DPAs disagree as to the permissibility of questionnaires screening the health of employees, which can be explained as processing in the context of employment being subject to national legislation (Art. 88 and Recital 155 GDPR).

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 for the purpose of carrying out its obligations in the field of employment (such as the obligations arising under the 2005 Act)".[96] Note the emphasis placed by the DPC on necessity,

[94] 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.
[95] Christina Etteldorf, 'EU Member State Data Protection Authorities Deal with COVID-19: An Overview', (2020) *European Data Protection Law Review* 6(2) 265.
[96] DPC, Data Protection implications of the Return to Work Safely Protocol (June 2020), p. 3.

which links to the principles of fairness and purpose limitation. Clear guidance on what constitutes 'strict necessity' and 'proportionality' for forms used under legal bases other than Art. 6(1)(c) and Art. 9(2)(b) remains sorely needed, especially to avoid purpose creep and the normalising of intrusive data collection practices.[97]

Part 1B of this chapter covered three forms, all of which have remained unchanged since they were first drawn up in 2020. As a result, previous findings as to their compliance still apply.[98] The Return to Work/Work Safely self-check facsimile can be compliant when supplemented by information pursuant to Art. 12 and 13 GDPR. In its current form, the NSAI and HABIC self-check forms fail to meet most principles laid down in Art. 5 GDPR, such as lawfulness, minimisation, storage limitation, integrity and confidentiality. The absence of information notices defies the principle of transparency (Art. 5, 12 and 13 GDPR), thereby depriving data subjects of information about their entitlements, chiefly their right of access - an essential component of the right, as it features in the definition of the right[99] – which is preliminary to the effective exercise of rights conferred by data protection law.[100] This is all the more worrying as the questionnaire collects data concerning health, which are special categories of personal data deserving reinforced protection (Art. 9 GDPR), and has been adopted by sectorial organizations like HABIC.

Compliance of Covid-19 CMP and its digital components with data protection law

The CMP and the VIS are arguably the most important part of the data-driven response to the pandemic and the most relevant from a data protection perspective, in light of the spread and variety of personal data collected. In his response to the question relating to computerised systems for contact tracing in the Daíl, Minister Simon Harris mentioned he would avail of Health Technology Assessment, which falls within the remit of the Health Information and Quality Authority. Besides the loose collection of documents going under the

[97] 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>.
[98] 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.
[99] By analogy, Judgment of 6 October 2015 in *Schrems*, C-362/14, EU:C:2015:650, para 41.
[100] Judgment of 20 December 2017 in *Nowak*, C-434/16, ECLI:EU:C:2017:994, para 57.

heading 'Contact Tracing Guidance',[101] there was no other publicly available information about either a specific legal basis or the (legally required) data protection impact assessment. A DPIA 'prior to the processing' (Art. 35 GDPR), and potentially prior consultation of the supervisory authority, are needed in light of the risky nature to the rights and freedoms of data subjects inherent in large-scale processing operations, operations by means of a new technology, and operations processing health data (Recital 91 GDPR). Such processing operations amount to a serious interference with the right and, to be permissible, they must be proportionate, adequate and necessary.

The digital components of the CMP arguably require a DPIA, particularly as laid down in Article 35(3)(b). Given the generic nature of the data protection notice referred to in Part 1B, and given the absence of a DPIA, it becomes difficult to assess this intervention from a data protection perspective; there is a strong case for making the relevant documentation available for the sake of transparency, as was for instance done in the case of the Covid Tracker App.[102]

Compliance of the VIS with data protection law

A DPIA was performed and made available in the context of the 'vaccine information system' (VIS). The publication of the DPIA is a welcome step as it increases transparency and enables public scrutiny. The document identifies three lawful bases: Articles 6(1)(e), 9(2)(h) and (i) GDPR.[103] It needs to be noted that these legal bases are identified 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.). Version 0.6 incorporates comments from the DPC, possibly in relation to prior consultation.[104] There appear to be a few

[101] Health Protection Surveillance Centre (HSPC), 'Contact Tracing Guidance' <https://www.hpsc.ie/a-z/respiratory/coronavirus/novelcoronavirus/guidance/contacttracingguidance/>. A search on the HIQA website returned no results. Health Information and Quality Authority <https://www.hiqa.ie/>.

[102] See chapter 2 by David Fennelly. I'm grateful to Cian Henry for contrasting the transparency of the App with the lack of transparency of the CovidCare Tracker.

[103] HSE, Vaccine Information System for COVID-19 Vaccination Programme Data Protection Impact Assessment, Version 1.8 (22 April 2021), p. 31.

[104] A news report points to the DPC being consulted about risks. The DPIA does not clarify the matter. 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>.

shortcomings arising from the current version of the DPIA, the most relevant of which are discussed in the following.

Firstly, 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).[105] 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 are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.[106]

A second cause for concern is that both IBM and Salesforce 'are providing support of the Vaccine Information System from outside the EEA';[107] it is unclear why these companies, who have European and particularly Irish offices,[108] 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. In general, identifying the recipient country of VIS data is fundamental to appraise the adequacy of such a transfer. The transfer of VIS data to the US, following the CJEU's decision in *Facebook Ireland and Schrems,*[109] 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 Charter.[110]

Thirdly, all data collected is to be retained in perpetuity. This decision is a serious breach of the principle of storage limitation, as it is unrelated to specific purposes and specific

[105] Ibid. p 18.
[106] Ibid. p. 26.
[107] Ibid. p.34
[108] Ibid. P. 34. https://www.salesforce.com/eu/company/locations/; https://www.research.ibm.com/labs/europe/#ireland .
[109] Judgment of 16 July 2020 in Facebook Ireland and Schrems, C-311/18, ECLI:EU:C:2020:559.
[110] Judgment of 16 July 2020 in Facebook Ireland and Schrems, C-311/18, ECLI:EU:C:2020:559, para 105.

controllers/processors. Thus, in light of the DPIA, it is unclear whether the processors and sub-processors would retain such data in perpetuity as well.[111]

Fourthly and relatedly, such endless retention period necessarily affects 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.[112] 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".[113] Moreover, the list of technical and organisational security measures provided, which on paper appear adequate,[114] will need to be updated in years to come, e.g. with the development of quantum computing. In light of the shortcomings identified, it is submitted that the VIS may be in breach of data protection principles, and that current mitigation measures are not adequate to redress the risks.

C. Issues transversal to data-driven measures: legality, purpose limitation and data security

Data-driven measures reviewed in this chapter satisfy the requirements identified in Part 2A[115] to varying degrees. All data-driven measures state the main purpose of the processing and meet an objective of public interest. Only processing within the VIS is explicitly based on Art.6(1)(e) though, as stated above, not all categories of data processed within the VIS are explicitly justified.[116] It is difficult to assess the proportionality of data-driven measures in

[111] HSE, Vaccine Information System for COVID-19 Vaccination Programme Data Protection Impact Assessment, Version 1.8 (22 April 2021), p. 23.
[112] Ibid., p. 26.
[113] 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>.
[114] An assessment is impossible without reference to detailed technical measures and specific standards.
[115] As enshrined in Articles 6(2) and (3) read in conjunction with Recitals 41, 45 and 73, the notion of essence, Sections 36, 38, 51 and 53 DPA 2018 and the rule of law.
[116] See chapter 3 by Róisín Á Costello.

light of the scarcity of details provided; the *de facto* disrespect of data protection principles and requirements is likely to amount to a disproportionate interference.

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 identification of the data controller, though not always with clarity for all categories. Some Regulations 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 terminology used by some documents 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.[117] Data-driven measures suffer from transversal issues concerning the principles of 'lawfulness, fairness and transparency', 'purpose limitation' and 'integrity and confidentiality' enshrined in Article 5 GDPR.

Lawfulness, fairness and transparency. Measures adopted do not consistently include the safeguards for data processing to ensure lawful and fair processing listed in Art. 6(3) GDPR. All documents specify purposes, but few documents clearly limit them. In particular, guidance documents lack a 'generic data protection notice' that data controllers could easily affix in their premises to inform people of their rights. It is unclear how data subjects are notified of their rights when they hand in a PCR test at a border crossing. Such a state of affairs 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. The DPC has consistently sanctioned data controllers who failed to enable data subjects to avail of their protections.[118] The circumstances would warrant the adoption of an instrument of the rank of a Statutory Instrument pursuant to S. 36, 38 and 51 DPA 2018 (and, where necessary, S. 60 DPA 2018) to provide consistent

[117] 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>.

[118] DPC, Case Studies <https://www.dataprotection.ie/en/pre-gdpr/case-studies>.

guidance benefitting from the consultation of the DPC, as well as the drafting of Covid-19 specific data protection notices.

Purpose specification and storage limitation. The two statutory instruments reviewed here[119] lay down rules enabling the further processing of data collected for pandemic purposes for generic law enforcement purposes. The problem can be explained for all instruments by reference to Regulation 8(4) of the passenger locator forms (reproducing Regulation 7(4) of the now revoked S.I. 181/2020). According to Regulation 8(4), personal 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)).

First, such a Regulation *de facto* broadens the purposes for which data can be used, which sits uncomfortably with: (i) the purpose limitation principle; (ii) the essence of the right, in that it fails to constitute a provision that "limits (…) the purposes for which (…) data may be processed";[120] and (iii) the 'quality of the law' tenet of the rule of law,[121] in that the purpose "*a criminal offence*" is not specified, specifically it is broader than the penal provisions identified in Regulation 8(1)(b), and thus does not provide sufficient clarity and foreseeability. This could invalidate the specific Regulation without the need to perform a proportionality assessment.

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. These shortcomings should be remedied in all instruments: amendments should include necessary safeguards and clarify the scope of data retention and transfers for 'criminal offences'.

[119] The same issue applied to Part 4 of 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>, which was set to expire on July 19th. <https://www.gov.ie/en/collection/1f150-view-statutory-instruments-related-to-the-covid-19-pandemic/>.

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

[121] 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.

Finally, it is unclear who would be the data controller for law enforcement purposes. In addition, processing for law enforcement purposes would require a transfer of personal data.[122]

Integrity and confidentiality. The existence of provisions concerning the integrity and confidentiality of the data is one of the elements fulfilling the essence of data protection. Only the Return to Work/Work Safely Data Protection Supplement mentions the secure storage of data; the DPIA of the VIS clarifies the categories of technical and organisational measures adopted to this effect. All other measures are silent in this respect. The importance of securing such data cannot be overstated because of the increased risk of data breaches tied to a home-bound or overwhelmed workforce.[123] Lost logged contacts, including manual ones, would be a treasure trove for potential offenders and worsen the tally recorded by the Central Office of Statistics for Q1 2020, whereby phishing (email), vishing (voicemail) and smishing (text messaging) frauds were up by 45%,[124] and further increased by 50% in 2021.[125] The use of cloud computing solutions can increase the costs of a data breach by exfiltrated/lost unit.[126]

The recent ransomware attack suffered by the HSE demonstrates how data security requirements need to become a regulatory priority and cannot be left to contractual arrangements between the controller and the processor.[127] Importantly, the security incident did not seem to affect the VIS, but seemed to affect the CTT.[128] The incident provides a cautionary tale for any data collection system put into place. A report published in May 2021

[122] See chapter 3 by Róisín Á Costello.

[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/>. Maria Grazia Porcedda, 'Covid-19 and cyber security: averting cybercrime, safeguarding data and protecting people' (COVID-19 Law and Human Rights Observatory, 31 July 2020) <https://tcdlaw.blogspot.com/2020/07/covid-19-and-cyber-security-averting.html>.

[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>.

[127] For the author's view on the ransomware attack suffered by the HSE, see the TriCon podcast hosted by Alan Eustace, 'Maria Grazia Porcedda on the HSE cyber-attack' <https://soundcloud.com/tcd-covid-observatory/special-maria-grazia-porcedda-on-the-hse-cyber-attack/s-Tk0qFZILc40> (June 2020).

[128] Eoin Butler, Life as a Covid Vaccine Volunteer, *The Irish Times* (13 June 2021).

on the National Incident Management System (NIMS) within the HSE found "lack of clear governance, leadership and management for NIMS within the HSE. 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]

Recommendations

Recommendations stemming from these pages are as follows:

- *Adopting an overarching instrument that contains the blueprint for data processing for pandemics*. 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 transfer of data to the HSE, in a clear, precise, and foreseeable manner. Such instrument should specify issues of controllership, purpose limitation and integrity and confidentiality of data, alongside other requirements found in the applicable law as discussed in these pages. The obligation to consult the DPC would help ensuring adherence to the law. The law should clarify when the processing of data concerning health is necessary and proportionate.
- *In the interim, and to the extent it is still relevant at the time this report is published, amending legislation* currently enabling the collection of passenger data, guests and members of the public attending hotels and premises serving food and drinks.
- *Issuing a facsimile data protection notice for all those entities that are processing 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 currently affixed to the walls (or shown on the website) of businesses.

[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>.

- *Aggregating and publishing documentation concerning the digital components of the CMP*, to match the level of transparency achieved for the Covid-19 app and enable public scrutiny, including from a cybersecurity perspective.
- Clarifying to what country VIS data are being transferred to and under what arrangements set out in Chapter 5 of the GDPR, as well as *opening up the DPIA carried out for the VIS to public consultation.*
- *Discussing due diligence concerning the uptake of technologies for continued tele-working,*[130] both from a health and safety and cybersecurity perspective.

Conclusions

This chapter appraised the compliance of pandemic data-driven measures adopted in Ireland with data protection legislation. EU Member states were, to begin with, relatively inexperienced in pandemics and consequently have been learning as they went along.[131] However, lessons learnt from other situations of emergency, like terrorism and the related data retention debate, are relevant when assessing the viability of measures adopted. Indeed, the relevance of data retention debates has not escaped commentators such as Kennedy,[132] 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.

Many commentators stress the potential inadequacy of national rules overseeing the state of emergency[133] and the consequences this carries for legality.[134] The conclusion, from a data protection perspective, is similar: the rationale of most interventions is fully justifiable, but

[130] Rana Foroohar, 'Big Tech's viral boom could be its undoing', *The Irish Times* (22 May 2020) <https://www.irishtimes.com/business/technology/big-tech-s-viral-boom-could-be-its-undoing-1.4257199?mode=sample&auth-failed=1&pw-origin=https%3A%2F%2F>.

[131] 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.

[132] Rónán Kennedy, 'Data Protection and COVID-19'.

[133] 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.

[134] 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).

the delivery does not always appear sound. A systematic reading of the applicable law in light of fundamental rights suggests that data-driven measures that process data without the necessary safeguards could amount to undue restrictions and could be challenged on rule of law grounds. Of concern is not only digital processing, but also processing done manually or rudimentary technology.

The applicable law provides the blueprint 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. It is recommended to review data-driven measures with a view to incorporating the necessary safeguards.

CHAPTER 2: CONTACT TRACING APPLICATIONS: THE IRISH EXPERIENCE

David Fennelly

Introduction

One of the primary data protection challenges that emerged with the COVID-19 pandemic was that of contact tracing. In order to control the spread of the virus, effective contact tracing measures were essential, particularly prior to the development and distribution of vaccines. By its nature, contact tracing involves the processing of personal data, including health data. Indeed, in its recitals, the GDPR makes specific reference to "*contact tracing for contagious diseases*".[135] Technology – and, in particular, the high level of smart phone usage – offers the possibility of making a significant contribution towards effective contact tracing. At the same time, in the context of a pandemic such as COVID-19, it presents the risk of misuse or abuse of large volumes of sensitive personal data. The tension between these considerations has characterised the debate on contact tracing applications for COVID-19.[136] In this Chapter, we consider the Irish experience with this debate.

On 7 July 2020, the Irish health authorities, the Department of Health and the Health Service Executive ('HSE') launched the Irish contact tracing application, the COVID Tracker App. The App had three core functions: first, it alerts the user and close contacts in case of a positive result; second, it provides advice on symptoms; third, it provides an overview of national data in relation to COVID-19, including, in the course of 2021, statistics on vaccination. More recently, on 13 July 2021, the App was updated to provide users with the option to store the EU Digital COVID Certificate.

[135] Regulation (EU) 2016/679 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) ('GDPR'), recital 112.
[136] See e.g. Bradford, Aboy and Liddell, "COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes" (2020) 7(1) *Journal of Law and the Biosciences* 1-21.

In this chapter, we will first consider the process by which the COVID Tracker App came into being. Process is important in this context, not only because the GDPR requires impact assessment for high risk processing but also because it is essential for ensuring public trust. Second, we will consider the model of application used for digital contact tracing purposes. In Ireland, and internationally, this represented one of the most sensitive issues in the development of contact tracing applications. Third, we will consider the legal basis relied upon for the deployment of the COVID Tracker App and the principle of purpose limitation. Fourth, we will consider the issue of effectiveness of contact tracing apps by reference to the COVID Tracker App. Finally, by way of conclusion, we will offer some reflections on the Irish experience and consider how this might inform future debates about the processing of personal data for important public interest objectives. As we move to the next stage of combatting COVID-19, where the focus has shifted to vaccination, the experience with contact tracing apps provides a useful prism through which to consider broader debates about balancing the protection of personal data and other important public interest objectives, such as public health.

The Process

The COVID-19 pandemic has presented an unprecedented challenge for governments around the world and public health authorities in particular. It has necessitated far-reaching restrictions on fundamental rights and freedoms, which have had to be adopted and adapted within very short timeframes in line with the evolving public health situation. Against the backdrop of compelling public health exigencies, considerations of human rights, including privacy and data protection, may be side-lined.[137]

In the case of the COVID Tracker App, the Irish Government signalled that it would develop a mobile application to assist in contact tracing in late March 2020, when the country was in its

[137] For an important contribution to this debate in the Irish context, see Casey, Doyle, Kenny and Lyons, *Ireland's Emergency Powers During the Covid-19 Pandemic* (Irish Human Rights and Equality Commission, February 2021).

first period of lockdown.[138] It was not until July 2020 that the App was launched. The three month period between the announcement and the launch of the App was important not only for the technical development of the App but also for public debate and scrutiny of the proposed deployment of a contact tracing application in Ireland.

April 2020 marked a decisive month in the development of contact tracing apps. First, as discussed in the next section, there was major progress in the technical development of such apps, with the publication of a decentralised protocol and the announcement by Apple and Google of an exposure notification system which could be used on iPhones and Android devices.

Second, on a policy level, on 8 April 2020, the European Commission issued a recommendation on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis.[139] This called for a pan-European approach for the use of mobile applications, coordinated at Union level, *inter alia* "*for warning, preventing and contact tracing to help limit the propagation of the COVID-19 disease*".[140] According to the Commission, the experience of Member States in introducing contact tracing applications showed that, in order to increase acceptance, an integrated governance, encompassing a wide range of stakeholders, was useful to prepare and implement such measures.[141] The Commission tasked the eHealth Network with the task of operationalising the Recommendation and, on 15 April 2020, the eHealth Network published its initial report on contact tracing apps.[142]

[138] Mitchell and Rogan, Phone tracking app set to be used as next step to fight COVID-19, Business Post, (Dublin 29 March 2020) quoted in Henry and Nuding, "Ireland" in Institute for Internet and Just Society, *Privacy and COVID-19 – Country Reports*, 19 February 2021, p. 63. Henry and Nuding provide a valuable account of the Irish experience in addressing COVID-19 privacy challenges, including but not limited to the context of contact tracing.
[139] Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data.
[140] Commission Recommendation (EU) 2020/518, paragraph 1(1).
[141] Commission Recommendation (EU) 2020/518, recital 18.
[142] eHealth Network, *Mobile applications to support contact tracing in the EU's fight against COVID-19* (15 April 2020).

The Commission Recommendation recommended the close involvement of the Union's data protection authorities in the development of contact tracing apps. By 21 April 2020, the European Data Protection Board ('EDPB') – the independent body composed of the EU's data protection supervisory authorities – had adopted guidelines on the use of location data and contact tracing tools in the context of the COVID-19 outbreak.[143] In doing so, the EDPB emphasised the importance of a common European approach to these challenges and the necessity of these tools being used to empower rather than to restrict or stigmatise citizens.[144] Within its guidance, the EDPB drew attention to two features of the GDPR of particular importance in the development of new technologies: first, it stated that careful consideration should be given to the principle of data protection by design and by default;[145] second, it expressed its view that a data protection impact assessment (DPIA) would have to be carried out before implementing contact tracing apps and also strongly recommended the publication of such DPIAs.[146]

Third, at the national level, in light of developments in Europe and beyond, civil society became actively engaged on the issue of contact tracing apps. Perhaps the most important contribution to the national debate came on 29 April 2020 when the Irish Council for Civil Liberties and the Digital Rights Ireland led a group of civil society organisations, scientists and academics calling on the Irish health authorities to ensure that the contact tracing application would respect "*legality and human rights norms*". This group argued that, in developing the application, the Irish authorities should respect four overriding principles: embracing transparency and promoting trust; designing for privacy and data protection; limiting the purpose of the app; and getting it right first time. Referring to the EDPB recommendations, the group called for publication of the app's draft specification and user requirements, Data Protection Impact Assessment (DPIA), and source code as well as for input from experts and public scrutiny of what was proposed. Finally, the group called on the authorities to ensure

[143] European Data Protection Board, *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak* ('EDPB Guidelines'). For a discussion of the EU guidance, see Gover and Flett, 'European Commission and the EDPB lay out framework for privacy-compliant contact tracing apps' (2020) 26(5) *Computer and Telecommunications Law Review* 117.
[144] EDPB Guidelines, paragraphs 3-4.
[145] GDPR, Article 25.
[146] GDPR, Article 35.

purpose limitation "*by preventing mission creep, mandatory uptake, or discrimination against those who have not installed the app*".[147] These concerns were echoed in the months preceding the launch of the COVID Tracker App.[148]

On 26 June 2020, the Irish health authorities published the source code for the App, the information notice, and Data Protection Impact Assessment ('DPIA').[149] In terms of process, the DPIA records the consultation by the Department of Health and the HSE with their respective data protection officers.[150] Prior to publication, consultation also took place with the Data Protection Commission and the Office of the Attorney General.[151] The DPIA engages with the EDPB Guidelines.[152] The DPIA makes reference to a series of public and stakeholder consultations to support and inform the development and deployment of the App,[153] as well as the establishment of an App Advisory Committee which would support the HSE in the rollout, operation and development of the App, including by ensuring oversight of compliance with data protection law and guidance.[154] In terms of substance, the DPIA provides a relatively detailed assessment of the potential effects of the App on the protection of personal data, including the necessity and proportionality of the envisaged processing,[155] the data security measures in place,[156] and the principles of data minimisation and data retention.[157] The Irish Council for Civil Liberties and the Digital Rights Ireland welcomed the publication of the DPIA and source code, while raising concerns about the efficacy of the App.[158]

[147] See Irish Council for Civil Liberties/Digital Rights Ireland, Statement, 29 April 2020.
[148] See e.g. Irish Council for Civil Liberties/Digital Rights Ireland, *Submission to the Special Committee on COVID-19 Response on the HSE/ Department of Health's COVID-19 contact-tracing/symptom-tracking app and contact tracing*, 16 June 2020.
[149] Horgan-Jones, "HSE reveals key documents ahead of Covid-19 tracker app", *Irish Times*, 26 June 2020.
[150] HSE/Department of Health Data Protection Impact Assessment – COVID Tracker App ('DPIA'), pp. 24-26.
[151] According to the HSE website, the DPIA was "*finalised on the basis of feedback from the Attorney General's Office and from the Office of the Data Protection Commissioner*": see https://www.hse.ie/eng/services/news/newsfeatures/covid19-updates/covid-tracker-app/ (last accessed 20 July 2021).
[152] DPIA, pp. 23-24.
[153] DPIA, pp. 13-14.
[154] DPIA, p. 27.
[155] DPIA, pp. 17-20.
[156] DPIA, pp. 20-22.
[157] DPIA, pp. 50-54.
[158] Irish Council for Civil Liberties/Digital Rights Ireland, "ICCL and DRI raise questions on efficacy of HSE contact-tracing app", 26 June 2020.

Ultimately, the COVID Tracker App was launched on 7 July 2020. Within 48 hours, there were one million downloads of the App.[159] By October 2020, the Minister for Health described the app as "*one of the most successful in the world*".[160] As of July 2021, there had been over 2.6 million app registrations.[161]

While the high level of uptake of the App may be attributed to several factors, it is clear that the public debate and scrutiny informed the nature and form of the App ultimately adopted as well as the process by which it was adopted, including through the publication of the source code and DPIA. Commenting on the successful launch of the App, the HSE underlined that the App had been developed with "*privacy by design at its core*".[162] In September 2020, the Irish Council for Civil Liberties cited the COVID Tracker App as an example of "positive consultation".[163]

By proactively engaging with the concerns around privacy and data protection, the Irish health authorities not only identified potential problems and pitfalls in the rollout of the App but also helped to build public trust in the App ultimately adopted.[164]

The Model

One of the major debates in the development of contact tracing apps internationally has been the model used for these apps. On the one hand, certain contact tracing apps use a

[159] See the press release published on the website of the Health Service Executive, available at https://www.hse.ie/eng/services/news/media/pressrel/one-million-downloads-of-covid- tracker-app-in-48-hours.html (last accessed 21 July 2021).
[160] Department of Health, "Minister for Health welcomes launch of contact tracing apps in New York and New Jersey based on the Irish Contact Tracing App", Press Release, 2 October 2020.
[161] COVID Tracker App (last accessed 20 July 2021).
[162] https://www.hse.ie/eng/services/news/media/pressrel/one-million-downloads-of-covid-tracker-app-in-48-hours.html
[163] Irish Council for Civil Liberties, *Submission to Oireachtas Special Committee on the Covid-19 Response*, 3 September 2020.
[164] Julienne, Lavin, Belton, Barjaková, Timmons, and Lunn, *Behavioural pre-testing of COVID Tracker, Ireland's contact-tracing app* (ESRI Working Paper No. 687, December 2020). According to the authors, while almost one in five participants mentioned privacy concerns in relation to their likelihood of downloading the app, the inclusion of additional assurances regarding the privacy of users' data in the app successfully lowered participants' privacy concerns and boosted engagement.

'centralised' model which is based on the creation of a central database of contact tracing information. On the other hand, many contact tracing apps are based on a 'decentralised' model which allows users to receive exposure notifications without sharing personal data with public health authorities or creating a central database of contacts.

In early April 2020, an international consortium of researchers published a decentralised open protocol and code called Decentralised Privacy-Preserving Proximity Tracing (DP-3T).[165] This protocol allows smartphone users to be notified if they were in contact with an individual subsequently diagnosed with COVID-19 but did not require the development of a centralised database of contact tracing information.

On 10 April 2020, Apple and Google announced the introduction of an exposure notification system (often known as 'GAEN') which users could opt to implement at the operating system level in iPhones and Android smartphones and would be interoperable between iOS and Android devices.[166] This system was based on the DP-3T Protocol and was intended for use by national health authorities. In this way, an exposure notification system could be put in place without requiring the centralisation of contact tracing information and thereby creating the risk of such information being used beyond its intended purpose of contact tracing.[167]

In its Guidelines of 21 April 2020, the EDPB recognised that contract tracing apps could follow a centralised or decentralised approach:

> *Both should be considered viable options, provided that adequate security measures are in place, each being accompanied by a set of advantages and disadvantages. Thus, the conceptual phase of app development should always include thorough*

[165] For a valuable account of these issues, see Veale, "Sovereignty, Privacy and Contact Tracing Protocols" in Taylor, Sharma, Martin and Jameson (eds.) *Data Justice and COVID-19: Global Perspectives* (Meatspace Press, 2020), pp. 34-39.
[166] See the statements on the Google and Apple websites: https://www.google.com/covid19/exposurenotifications/; https://covid19.apple.com/contacttracing.
[167] DPIA, pp. 12, 18 and 25.

consideration of both concepts weighing up the respective effects on data protection/ privacy and the possible impacts on individual rights.[168]

However, while confirming that both approaches were permissible, in a footnote, the EDPB nonetheless noted that "*in general, the decentralised solution is more in line with the minimisation principle*".[169] The decentralised approach was also arguably more consistent with the principles of data protection by default and by design enshrined in Article 25 GDPR.[170]

Despite calls for a common approach to contact tracing apps, there remained divergent approaches across Europe. A number of EU Member States – including Bulgaria, Cyprus, France and Hungary – adopted a centralised approach.[171] Some did not deploy contact tracing apps. The majority of EU Member States opted for a decentralised approach.[172] In the United Kingdom, there was a high-profile about-turn on this issue: having initially announced that it would use a centralised model, the UK Government ultimately decided to adopt a decentralised approach.[173]

[168] EDPB Guidelines, paragraph 42.
[169] EDPB Guidelines, paragraph 42 (fn 18).
[170] EDPB Guidelines, paragraph 27.
[171] LibertiesEU, "COVID-19 Contact Tracing Apps in the EU", available online at https://www.liberties.eu/en/stories/trackerhub1-mainpage/43437 (last accessed 21 July 2021).
[172] See footnote 35 and see also European Commission, *Mobile applications to support contact tracing in the EU's fight against COVID-19 – Progress Reporting June 2020*. On national experiences, see e.g. Stehlíková, "The corona crisis, data protection and tracking apps in the EU: the Czech and Austrian COVID-19 mobile phone apps in the battle against the virus" (2021) 56(1) *Czech Journal of International Relations* 35-67; Skiljic, "'Stop COVID-19': The Croatian Application for Contact Tracing - Overview and Privacy-Related Uncertainties" (2020) 6 *European Data Protection Law Review* 433. For a broader review of the EU response, see Kędzior, "The right to data protection and the COVID-19 pandemic: the European approach" (2021) 21 *ERA Forum* 533–543.
[173] Department of Health and Social Care, *Next phase of NHS coronavirus (COVID-19) app announced*, Press Release, 18 June 2020. See the important report of the House of Commons and House of Lords Joint Committee on Human Rights, *Human Rights and the Government's Response to Covid-19: Digital Contact Tracing* (HC 343/HL Paper 59), 7 May 2020. See also Oswald and Grace, "The COVID-19 contact tracing app in England and "experimental proportionality"" (2021) *Public Law* 27-37; Guinchard, "Our digital footprint under Covid-19: should we fear the UK digital contact tracing app?" (2020) 35(1) *International Review of Law, Computers & Technology* 84-97.

In Ireland, after some uncertainty, it became clear that the Irish COVID Tracker App would adopt the decentralised approach. In their statement of 29 April 2020, the Irish Council for Civil Liberties ('ICCL') and Digital Rights Ireland called for a "*rights respecting decentralised approach, rather than a centralised one*", welcoming the reported rejection of the centralised architecture by the HSE.[174] In its DPIA, the HSE and Department of Health expressly acknowledged the privacy issues with a centralised model and expressed their commitment to decentralised design principle.[175]

While the decentralised model played an important role in addressing privacy concerns in the adoption of the App, the adoption of such an approach, undergirded by the Google/Apple exposure notification system, raised broader issues about the role of private and public power in protecting privacy and personal data. As Veale describes the position, the use of contact tracing apps based on this model effectively created "*de facto public-private partnerships*" between Apple and Google, on the one hand, and public health authorities, on the other.[176] While in one sense this reflects the reality of society's heavy dependence on particular forms of technology such as smartphones, it raises broader governance and ethical issues. One example of such an issue in this context was that, on Android devices, the exposure notification service is managed by Google and formed part of Google Play Services. It appears that Google Play Services contacts Google servers on a regular basis, "*potentially allowing fine-grained location tracking via IP address*", and also shares "*the phone IMEI, hardware serial number, SIM serial number, handset phone number and user email address with Google, together with fine-grained data on the apps running on the phone*". Leith and Farrell have described this as "*extremely troubling from a privacy viewpoint*".[177]

[174] Irish Council for Civil Liberties/Digital Rights Ireland, *Joint Statement*, 29 April 2020.
[175] DPIA, paragraph 7.4.
[176] Veale, "Sovereignty, Privacy and Contact Tracing Protocols" in Taylor, Sharma, Martin and Jameson (eds.) *Data Justice and COVID-19: Global Perspectives* (Meatspace Press, 2020), p. 36.
[177] Leith and Farrell, "Contact Tracing App Privacy: What Data Is Shared By Europe's GAEN Contact Tracing Apps", Proc IEEE INFOCOM 2021. The response of officials to these and related concerns is referenced in Brennan and Foxe, "Dept of Health officials dismissed criticism of COVID tracker app as 'incorrect'", Irish Examiner, 13 October 2020.

Thus, while the move towards decentralised models for contact tracing apps, supported by the Google/Apple exposure notification system, was broadly welcomed from a privacy point of view, that move was not without its challenges. In their pre-release report card on the COVID Tracker App, the ICCL and Digital Rights Ireland welcomed the adoption of a decentralised model but expressed concern that Google and Apple would have "*ultimate control over most of the EU's COVID-19 app ecosystem*".[178] While this is a valid concern, it must also be recognised that public health authorities, in Ireland and elsewhere, faced a difficult trade-off in trying to identify the most appropriate solution to the privacy and data protection issues presented by contact tracing apps. Even if the reliance on a decentralised model based around the Google/Apple exposure notification service may not have been ideal in all respects, it nonetheless offered significant privacy and data protection advantages compared to centralised models used in other jurisdictions.

The Legal Basis and the Principle of Purpose Limitation

Because the fight against COVID-19 so often requires the processing of special category personal data, such as health data, the identification of a lawful basis for processing is frequently a significant challenge. While in the ordinary course the processing of personal data requires a legal basis under Article 6 GDPR, in the case of special category personal data, processing is prohibited in the absence of a legal basis under Article 9(2) GDPR.

In its Guidelines, the EDPB identified a number of possible legal bases for contact tracing apps. According to the EDPB, the systematic and large scale monitoring of location and/or contacts between natural persons is "*a grave intrusion into their privacy*" and "*can only be legitimised by relying on a voluntary adoption by the users of each of the respective purposes*".[179] However, the mere fact that the use of contact-tracing applications takes place on a voluntary basis did not "*necessarily mean that the processing of personal data will necessarily be based on consent*".[180] In the view of the EDPB:

[178] Irish Council for Civil Liberties/Digital Rights Ireland, *Pre-Release Report Card on the HSE Covid-19 Tracker App*, 2 June 2020.
[179] EDPB Guidelines, paragraph 24.
[180] EDPB Guidelines, paragraph 29.

> *When public authorities provide a service based on a mandate assigned by and in line with requirements laid down by law, it appears that the most relevant legal basis for the processing is the necessity for the performance of a task in the public interest i.e. Article 6(1)(e) GDPR.*[181]

In accordance with Article 6(3) GDPR, this requires a lawful basis in EU or Member State law for the use of personal data, incorporating appropriate safeguards. Where a contact tracing app was based on another legal basis such as consent, the EDPB emphasized that the data controller must "*ensure that the strict legal requirements for consent are satisfied*".[182]

Because contact tracing apps may involve the processing of health data, such as infection status, a lawful basis under Article 9(2) would also be required. In this regard, the EDPB observed that processing of health data is allowed when it is necessary for reasons of public interest in the area of public health (Article 9(2)(i) GDPR) or for health care purposes (Article 9(2)(h) GDPR), while accepting that it might also be based on explicit consent under Article 9(2)(a) GDPR.

In addition to satisfying the requirements of the GDPR, it would also be necessary to comply with Directive 2002/58/EC, the ePrivacy Directive, because a contact tracing app involves the storage and/or access to information stored in the terminal of an electronic communications device.[183]

---

[181] EDPB Guidelines, paragraph 29.

[182] EDPB Guidelines, paragraph 32. Consent is defined in Article 4(11) GDPR as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". See also judgment of 1 October 2019, *Planet49*, C-673/17, EU:C:2019:801.

[183] Article 5(3) provides that Member States shall "*ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller*". However, this shall not prevent "*any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user*".

In the COVID Tracker App, the Irish health authorities decided to rely on consent as the legal basis for processing. According to the DPIA:

> *Clear, explicit consent in an intelligible and easily accessible form is sought for each of the personal data processing activities ... Having regard for the entirely voluntary and discretionary nature of downloading the app, and noting that the HSE and DoH cannot determine whether a person has installed the app or not, it is not considered that an "imbalance of power" (GDPR recital 43) arises....*[184]

In line with the digital age of consent in Ireland, the App was limited to persons that are 16 years or older.[185] In order to ensure that the user's consent is meaningful, the App settings allow users to opt in and out of particular functions, to upload but also to delete additional contact information or demographic data, and to clear exposure notifications if appropriate.[186] Finally, in line with the requirements of Article 5 of the ePrivacy Directive and Regulation 5 of the Irish implementing regulations, consent is also explicitly sought within the App prior to the collection of in-app metrics, in circumstances where the collection of this data was not strictly necessary for the provision of the service required.[187]

While the App does not generally involve the transfer of personal data outside the EU, the initial DPIA confirmed that one of its data processors – which processes the mobile number of users (obtained by the HSE outside the app through the existing contact tracing operations) in order to send an SMS message containing a code to a user who has been tested positive which enables that user to upload their keys – is based in the United States of America and hosts its servers outside the European Economic Area.[188] While the DPIA referred to this data processor as being certified under the EU-US Privacy Shield Framework, that framework was declared invalid by the Court of Justice of European Union on 16 July 2020.[189] In the updated

[184] DPIA, p. 15.
[185] DPIA, p. 12.
[186] DPIA, p. 6.
[187] Directive 2002/58/EC, Article 5; SI 336/2011, Regulation 5.
[188] DPIA, p. 23.
[189] Judgment of 16 July 2020, *Data Protection Commissioner v. Facebook Ireland & Schrems*, C-311/18, EU:C:2020:559.

DPIA published in July 2021, it is stated that this processor now relies on binding corporate rules as a basis for any international transfer of personal data involved in the provision of its service.[190]

In advance of the launch of the App, the Irish Council for Civil Liberties and Digital Rights Ireland questioned the legal basis of consent for the roll-out of the COVID Tracker App.[191] This may reflect, at least in part, a concern about the reliance by public authorities on consent as a legal basis having regard to the imbalance of power between data controller and data subject in such a context, a concern given expression in recital 43 to the GDPR and addressed in the DPIA. While the EDPB acknowledged the possibility of consent as a legal basis for contact tracing apps, it also appeared to express preference for an alternative legal basis under Articles 6 and 9 GDPR.

While it is certainly the case that consent has its weaknesses as a legal basis, particularly as it can be easily withdrawn,[192] there is nevertheless a good argument that reliance on consent in this particular context is more consistent with overarching concerns about the voluntary nature of the app and the need to empower, rather than restrict or stigmatise, the data subject. Of course, the effectiveness and validity of consent is bound up with the transparency of the information afforded to data subjects in respect of the processing of personal data and is also closely linked to compliance with the other fundamental data protection principles enshrined in Article 5 GDPR.

Within the scope of this short contribution, it is not possible to undertake an exhaustive analysis of the App's compliance with the principles in Article 5 GDPR. Many of these principles – such as the principles of lawfulness and transparency, data minimisation, storage limitation and integrity and confidentiality – are explicitly addressed in the DPIA. One of the

[190] Health Service Executive/Department of Health, *Data Protection Impact Assessment – COVID Tracker App*, Version 1.3, 14 July 2021 ('Updated DPIA').
[191] Irish Council for Civil Liberties/Digital Rights Ireland, *Pre-Release Report Card on the HSE Covid-19 Tracker App*, 2 June 2020.
[192] In August 2020, there were reports that many people uninstalled the app due to problems with battery drainage: see Foxe, "Covid-19 App: 150,000 Uninstalled App after August Battery Issue", Irish Examiner, 2 October 2020.

most important principles in this context is that of purpose limitation, enshrined in Article 5(1)(b) GDPR.

In its Guidelines, the EDPB stated that the purposes of contact tracing apps "*must be specific enough to exclude further processing for purposes unrelated to the management of the COVID-19 health crisis (e.g. commercial or law enforcement purposes)*".[193] In advance of the launch of the App, the ICCL and Digital Rights Ireland also emphasized the importance of purpose limitation and the dangers of mission creep, criticising in particular the additional symptom tracking function.[194]

In the DPIA, the App is described as having two functions: first, to support the national public health response to COVID-19 by (a) enhancing the existing HSE contact tracing operation and (b) monitoring and mapping the spread of COVID-19 symptoms; second, to support members of the public during the COVID-19 crisis by (a) providing COVID-19 related news, information, and national updates on the app and (b) storing a personal record of symptoms on the app. According to the DPIA, the symptom tracking information – which users can choose to provide - is used to "*create an anonymous collective daily overview of the progression of COVID-19 symptoms and an indicator of the spread of the virus informing public health policy interventions*".[195] Although certain demographic information is requested for this purpose, the view is expressed that this would not reveal a person's identity and would simply be used to give statistical insights into COVID-19 symptoms in the country. This information, in anonymous form, is then securely transferred to the Central Statistics Office where it contributes to the identification of symptom progression across the State.[196] The DPIA also confirms that the HSE will not use IP addresses – which are communicated between the app and the HSE servers through the use of the App – for identification purposes.[197] The DPIA repeatedly emphasizes that the personal data processed through the App is used for the stated purposes and only in the context of the COVID-19 crisis.

[193] EDPB Guidelines, paragraph 26.
[194] Irish Council for Civil Liberties/Digital Rights Ireland, *Joint Statement*, 29 April 2020; Irish Council for Civil Liberties/Digital Rights Ireland, *Pre-Release Report Card on the HSE Covid-19 Tracker App*, 2 June 2020.
[195] DPIA, p. 5.
[196] DPIA, pp. 5 and 17.
[197] DPIA, p. 7.

As of July 2021, a new function was added to the COVID Tracker App, allowing users to upload their EU Digital COVID Certificate ('DCC'). According to the updated DPIA published in July 2021, this is a standalone feature provided primarily for the convenience of users and the DCC data is not shared with other features within the App.[198] The DCC can be deleted at any time and, if users want to use the App for storing the DCC only, the other features of the App can be disabled. In the wake of this announcement, the ICCL and Digital Rights Ireland have called on the Data Protection Commission to investigate the use of the App for this purpose.[199] The addition of this feature certainly marks the move of the App beyond contact tracing to serve a broader purpose for users. This being so, the question arises as to whether the integration of these functions in a single App is the appropriate course or whether a separate App for this distinct purpose would be preferable. On the one hand, the additional function is optional and many users may find it a very useful addition to the utility of the App. On the other hand, even if it has such benefits, it is essential that there be clarity and safeguards around the use, accessibility and security of the personal data on the DCC once uploaded on the COVID Tracker App.

The Effectiveness of the COVID Tracker App?

Finally, over a year on from the launch of the COVID Tracker App, it is necessary to consider whether it has served as an effective tool in the fight against COVID-19. Even before the App was launched, questions were raised as to whether it would be effective to achieve its intended purpose.

[198] Updated DPIA, p. 7. The Updated DPIA also provides information on the progress towards EU interoperability of contact tracing apps: Updated DPIA, pp. 5-6. On this issue, see Commission Implementing Decision (EU) 2020/1023 and EDPB, *Statement on the data protection impact of the interoperability of contact tracing apps*, 16 June 2020.

[199] See Meskill, *Investigation sought on GDPR compliance of Covid app*, 20 July 2021, available online at https://www.rte.ie/news/ireland/2021/0720/1236291-covid-tracker-app-gdpr/ (last accessed 21 July 2021).

In the public debate preceding the launch of the App, the Irish Council for Civil Liberties and Digital Rights Ireland raised concerns about the lack of any evidence in support of the efficacy of contact tracing apps. In their pre-release report card, it was argued that not only was there no clear evidence that the app accurately detects close contacts to Covid-19 but that the app signalling accuracy varied substantially depending on user environments.[200]

Following the launch of the App, as noted above, it was heralded as "*one of the most successful in the world*" and served as a model for contact tracing apps in other jurisdictions.[201] However, recent studies demonstrate that the efficacy of the App in contributing towards its primary purpose of contact tracing remains uncertain. In April 2021, Farrell and Leith examined six months of data from the App between October 2020 and April 2021. Based on their analysis of these statistics, they concluded that only 25% of the expected number of tested-positive app-users uploaded keys which allowed the App to serve its function of contact tracing, with this number on a downward trajectory.[202]

Further study and analysis of this issue – informed by the experience of the health authorities – may be helpful in shedding further light on the efficacy and utility of the App. In this regard, it is important to recall that the digital contact tracing forms one part of an overall contact tracing strategy, which has fluctuated in line with the rise and fall of COVID-19 over the eighteen months. In those cases where the App has been effective in notifying close contacts, it is likely to have made a contribution, however modest, to combatting the spread of COVID-19.[203] It is also important to situate the App within the wider context of the number and range of apps that mobile phone users use, often without any meaningful scrutiny and transparency as to the underlying processing operations. While there is a heavy onus on public authorities

[200] Irish Council for Civil Liberties/Digital Rights Ireland, *Pre-Release Report Card on the HSE Covid-19 Tracker App*, 2 June 2020.
[201] Department of Health, "Minister for Health welcomes launch of contact tracing apps in New York and New Jersey based on the Irish Contact Tracing App", Press Release, 2 October 2020.
[202] Farrell and Leith, "Irish Covidtracker App Key Upload Shortfalls", 14 April 2021, available online at https://down.dsg.cs.tcd.ie/tact/ie-stats.pdf (last accessed 21 July 2021).
[203] See in this regard Jacquemard, *eHealth in Ireland: Social and Ethical Values in Irish Policy on eHealth, Oireachtas Library & Research Service Spotlight* (3/2021), 31 March 2021, pp. 37-39.

rolling out apps intended for mass usage, the wider context in terms of user experience and expectation cannot be entirely ignored in assessing the relative utility of the App.

As with any new technology or tool, there are inevitable limitations on the extent to which effectiveness and efficacy can be assessed in advance of roll-out and implementation. While a "test-before-deployment" strategy may be preferable as a matter of general principle,[204] it is not always practical, particularly in the context of novel challenges which call for urgent responses. What is important from the purpose of privacy and data protection is that, where the efficacy of a new technology or data processing operation is uncertain, there is rigorous impact assessment in advance of deployment.

Conclusion

The debate about contact tracing apps in Ireland and internationally has brought into public focus broader debates about the balance between privacy and data protection, on the one hand, and the pursuit of important public interest objectives, such as public health, on the other, particularly in the context of a far-reaching and fast-evolving public health crisis. In an early intervention in March 2020, the EDPB emphasized that data protection rules "*do not hinder measures taken in the fight against the coronavirus pandemic*" and must be respected even in exceptional times.[205] Nevertheless, data protection rules – particularly having regard to the strict limitation on the processing of health data – have presented challenges for public authorities and private actors in responding to COVID-19. In the case of the COVID Tracker App, while the development and deployment of this app has not been without its critics, it has managed to strike a reasonable balance between the protection of privacy and data protection and the public interest in safeguarding health through contact tracing, both in terms of substance and process. In terms of substance, the choice of a decentralised model, as well as relatively clear limitations on purpose and an emphasis on the user's consent and control, were important features of the COVID Tracker App. Just as importantly, in terms of

[204] Farrell and Leith, "Irish Covidtracker App Key Upload Shortfalls", p. 2.
[205] European Data Protection Board, *Statement on the processing of personal data in the context of the COVID-19 outbreak*, 19 March 2020.

process, there was a greater degree of transparency, public engagement and public scrutiny around the COVID Tracker App than is generally the case in major public initiatives of this kind. Indeed, this process arguably helped to build a relatively high level of public trust in the App, evidenced by the number of registrations in the months following its launch. The recent decision to include an additional function on the App relating to the Digital COVID Certificate underlines the need for ongoing vigilance and review, particularly as we move into a new phase in tackling COVID-19. However, the experience to date with the COVID Tracker App – characterised by transparency and proactive and constructive engagement – arguably offers a useful lesson which may be drawn on and developed in confronting other significant data protection challenges in the public sector, both in the context of COVID-19 and beyond.

Recommendations

In light of the issues addressed in this chapter, it is recommended that:

- Building on the experience with the COVID Tracker App, greater effort should be made to promote transparency, public consultation and engagement in the development of significant public sector and public-private projects that involve large scale processing of personal data, including through the timely publication of Data Protection Impact Assessments.
- Careful consideration must be given to the core data protection principles enshrined in Article 5 GDPR – including the principles of data minimisation, purpose limitation and storage limitation – at all stages of the design and development of significant public sector and public-private projects that involve large scale processing of personal data.
- In the context of the COVID Tracker App, caution is required in adding new and further functions, such as the feature allowing the uploading of the COVID Digital Certificate. Where it is desired to offer new functions and features which differ from those originally provided for, providing a separate application which data subjects may or may not choose to download and use is in principle the preferable approach.

- In order to assess the effectiveness of the COVID Tracker App in a holistic fashion with a view to informing future decision-making and data protection practices, the Health Service Executive and/or the Department of Health should support the carrying out of independent research and analysis of the experience with, and the utility of, the App in contributing to contact tracing efforts during the COVID-19 pandemic.

CHAPTER 3: DATA SHARING BETWEEN PUBLIC BODIES DURING COVID-19

Róisín Á Costello

Introduction

The ongoing public health context generated by COVID-19 has drawn particular attention to the issue of data sharing as both State departments as well as public bodies like the HSE seek to co-ordinate data collection and to map vectors for disease transmission and service need. The Data Protection Commissioner's request to the Department of Social Protection concerning its access to the travel details of individuals in receipt of social welfare, as well as the revelations concerning the State's creation of dossiers on autistic children using information shared by the HSE and other bodies have drawn particular attention to just how data is shared, and how transparent the processes of such sharing are in Irish law and policy.

The Data Protection Commission (DPC) has emphasised the need for transparency in public sector use of data. In particular the Commission has noted the need to ensure data subjects are informed about how their personal information is used and for what purpose, who can access the information, and how the sharing of their data will impact them. This echoes the decision of the CJEU in *Bara*[206] to the effect that public sector use of personal data should be undertaken in a manner which reinforces the data protection rights of individuals. Yet the operation of data sharing between public bodies is often clear in principle but opaque in practice.

The Legal Basis for the Collection and Sharing of Health Data

[206] Case C-201/14 *Bara & Ors* EU:C:2015:638.

Where data is to be shared between public bodies there must, of course, be an initial legal basis under the GDPR through which the data can be lawfully collected and processed – either under Article 6, or Article 9.

In the case of COVID-19, certain data which may be collected and processed - such as location data, travel data or contact information, for example, is personal data which can be processed in accordance with one of the legal basis outlined in Article 6. The GDPR notes in Article 6(1), however, that public bodies should not rely on the legitimate interest basis under Article 6 in the performance of their tasks. Although a number of alternative basis for lawful processing under Article 6 are present in many cases, in the case of public bodies in the current public health context, the appropriate legal basis is likely to be found in Articles 6(1)(a) which requires the presence of consent or (e) which provides lawful processing is present where "*processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.*"

Article 6(3) GDPR notes that where the basis for processing is (1)(e) the official authority which is being exercised must be laid down in EU or national law, and that the law should meet an objective of public interest and be proportionate to the aim pursued by the law relied on. In this respect, the Irish Data Protection Commissioner has recommended that the conditions of data sharing arrangements between public bodies should be outlined clearly and in adequate detail either in primary legislation (or in secondary legislation with a primary legislative basis) to ensure there is no room for confusion or doubt as to the nature of the arrangement and thus providing the desired level of legal certainty. The DPC made these comments, specifically in the context of the passage of the Data Sharing and Governance Act 2019 which is examined in the following section.

In respect of health data, the position is (perhaps counterintuitively) somewhat clearer. Special category data is defined under Article 9 GDPR as data which reveals the racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, or is composed of genetic data or biometric data which uniquely identifies a natural person or data concerning an individual's health or sex life or sexual orientation. Article 9 provides for a

presumptive ban on the collection of special category data but accepts that such data may be processed in the presence of one the legal basis outlined in Article 9(2). In the current context, the most relevant of the provisions listed are Article 9(2)(h) and (i). These provisions permit special category data to be processed in order to provide occupational or preventative medical services (h) or in order to serve the public interest in the area of public health - in particular in the protection against serious cross-border threats to health (i).

Article 52 of the Irish Data Protection Act 2018 lays out specific requirements in respect of Article 9(2)(h) providing that it grounds an exemption from the prohibition under Article 9 only in the listed circumstances. The list itself is relatively narrow, providing that subsection (h) will be satisfied only where processing of such data is necessary,

- For the purposes of preventative and occupational medicine,
- For the assessment of the working capacity of an employee,
- For medical diagnosis,
- For the provision of medical care, treatment or social care,
- For the management of health or social care systems or services, or
- Pursuant to a contract with a health practitioner, and

Where, under s.52(2) such processing is undertaken by or under the responsibility of,

- A health practitioner, or
- A person who in the circumstances owes the data subject a duty of confidentiality.

This list would seem to limit the potential for reliance on (h) by public authorities on the basis of both the requirement for a relationship of confidentiality in s.52(2) and the exhaustive list in s.52(1).

Section 53 of the Data Protection Act 2018 reflects the provisions of Article 9(2)(i) in respect of the public interest and public health providing that the processing of special categories of data shall be permissible where such processing is necessary, echoing the provisions of the

GDPR itself and retaining the relatively broad character of the basis provided in the Regulation.

There would seem, therefore to be a range of variously specific legal basis on which public bodies can rely in the collection and processing of personal data – and particularly broad basis permitting such processing where the public interest and public health are concerned. The processing of such data, and its sharing must comply with the data protection principles and informational requirements outlined by the GDPR.

Processing and Sharing: The Data Protection Principles and Informational Requirements

Under the GDPR processing of personal data should only be conducted in accordance with the data protection principles outlined in Article 5 including the need for purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability. More generally, personal data must be obtained and processed in a transparent manner and in accordance with the specific obligations to provide data subjects with information which are contained in Articles 12, 13 and 14 GDPR.

At the most general and fundamental level, Article 12 GDPR requires that information provided to data subjects be concise, transparent, intelligible, and easily accessible. In particular, clear and plain language must be used about what data is to be collected and how it will be used. If data will be shared with other public bodies, or may be shared with them, Article 12 would require that the data subject be informed of this fact.

Pursuant to Article 13 GDPR, where personal data are gathered directly from the data subject, a data controller must inform the data subject of the identity and contact details of the data controller and DPO, the purpose and legal basis for any data sharing, the recipients of the data, whether the data will be transferred to non-EU states, the length of time for which it will be retained, the rights the data subject has, whether the provision of personal data is a statutory requirement or obligation, and the existence of any automated decision making processes that will be applied to the data. The person whose data is being collected must thus

be informed not only if it will be shared (under Article 12) but what legal authority the processor has to share the data in Irish law.

In the alternative, where the personal data has been obtained by the public body otherwise than directly from the data subject, Article 14 GDPR provides that a data controller must provide the information outlined in Article 13 and then, within a reasonable period, must also provide information on the categories of personal data concerned and the source from which the data were obtained including whether they were obtained from a publicly available source.

The only general exception to the requirement to provide information under Article 13 GDPR, is where the data subject is already in possession of the information which must otherwise be provided. Thus, under Article 14 GDPR, where the personal data has been obtained from a source other than the data subject, public bodies are not be required to furnish information to which the data subject already has access, or where provision of the information would be impossible, involve disproportionate effort, seriously impair the objectives of the data processing, or where the processing is required by law or the personal data must remain confidential subject to a professional or statutory obligation of secrecy.

The requirements of Article 13 and 14 are subject to certain exceptions under Article 23 GDPR which provides that specific Member State or Union Law may restrict the scope of rights and obligations under Articles 13 and 14 where the requirements listed as satisfied. This requires, in particular, that to lawfully impose a restriction, any measure must be of limited scope and applied in a strictly necessary, proportionate and specific manner.

The Data Protection Act 2018 contains certain provisions dealing with the restrictions of rights of data subjects. Sections 59-61 in particular give further effect to the provisions of Article 23 GDPR. The relevant sections for the purposes of data processing during COVID-19, are largely Articles 60 and 61. Article 60 provides for a restriction the obligations under Articles 13 and 14 for important objectives of general public interest and where such restrictions are necessary and proportionate to ensure a range of public objectives. However, the exceptions listed do not provide for limitations in respect of public health and it is now generally

understood that any exemptions established under the 2018 Act should be strictly interpreted in order to protect and uphold the fundamental rights of data subjects.[207] As a result the informational requirements of the GDPR remain largely unaltered by the current public health context.

The Data Sharing and Governance Act 2019

The result of this landscape is that data sharing must take place only where there is a significant degree of transparency as to the objectives, scope and limits of such sharing. However, as part of the Irish government's e-Government strategy, additional requirements are now to be imposed on public bodies sharing personal data under the Data Sharing and Governance Act 2019.

Prior to the 2019 Act entering into force data sharing in and between public service bodies was regulated on a sectoral basis with discrete pieces of legislation dealing with equally discrete sharing for defined policy purposes as required by Article 6(3) GDPR. Thus, data concerning birth registrations were forwarded by the General Register Office to the Department of Employment Affairs and Social Protection to generate child benefit claims while data was shared by the Student Universal Support Ireland (SUSI) with various Government Departments and the Revenue Commissioners share data with a number of sources, including the Property Registration Authority.

This patchwork approach led to increasing concerns about the complexity of data sharing agreements and transparency as to the movement of data between public sector bodies. In that context, the 2019 Act was introduced in order to provide a unified legislative basis for public bodies to share personal data subject to purposive, administrative and technical requirements and protections. However, different types of data attract divergent treatment under the Act.

[207] See, *Delcourt v Belgium* App no. 2689/65 (ECHR, 17 January 1970); *Klass v Germany* App no. 5029/71 (ECHR, 1978); C- 293/12 & C- 594/12 *Digital Rights Ireland*.

Section 5 of the 2019 Act states that its provisions (with the exception of Parts 5[208] and 8[209] and Chapter 3 of Part 9) do not apply to 'special category' data. Health data is thus generally not subject to the provisions of the Act. However, such data may come under the control of Ministerial Regulations pursuant to the exception in Chapter 3 of Part 9 which states (in ss.63-6) that the Minister may provide for the introduction of rules, guidelines and governance standards applicable to both normal and special category data for one of the purposes outlined in s.64(2). Such purposes include the improvement of data quality and accuracy, the promotion of a consistent approach to data management and sharing and increasing the usefulness of information held in order to improve the performance of public bodies.

Data which is not considered to be 'special category' data can be shared between public bodies in accordance with s.5 of the Act. This kind of data must be collected in accordance with one of the legal basis outlined in Article 6 of the GDPR and shared in accordance with the provisions of s.13.

Section 13 provides that a public body may disclose personal data to another public body where that sharing is for the purpose of the performance of a function of one of the bodies involved, one of the conditions outlined in s.13(2)(a)(ii) are met and such sharing occurs in compliance with a data sharing agreement as required by ss.15-22 of Part 4.

Where a basis for sharing is not present under s.13, sharing of personal data can be accomplished through another mechanism provided for in law. Thus, the CSSO receive and share data under the Health Research Regulations 2018 and the Statistics Act 1993, while the Department of Social Protection and the Revenue Commissioners share data on the basis of the Social Welfare Acts.

[208] Which provides for data sharing in respect of the public service pension scheme.
[209] Which provides for the creation of a personal data access portal.

The salient point to note in respect of the 2019 Act and the COVID-19 pandemic, however, is that the provisions under s.15-22 which govern the creation of Data Sharing Agreements as well as s.63-66 dealing with governance of data including special category data, were not commenced until 7 July 2021. This is hardly ideal given the large volumes of data (including special category data) which have been collected by public bodies over the last eighteen months and whose sharing between bodies remains undocumented in the terms which the Act now requires.

The exclusion of special category data and the absence of Ministerial Regulations outlining the mechanisms for the sharing of such data leave the position for public health data largely unchanged. Thus, while non special category data can be shared for one of the broadly drawn, functional reasons outlined in s.13 the public bodies involved are not obliged to publish details as to the agreements in respect of such sharing. Instead they must only satisfy the informational requirements under the GDPR and the 2018 Act.

The result is that it remains challenging to ascertain precisely what health data is being shared by public bodies, and on what basis, in the way the 2019 Act envisions. In the context of COVID-19 the HSE does note, in respect of data sharing, that the data collected by the Covid Tracker App is anonymised and shared with the Central Statistics Office for statistical reporting and analysis.[210] Separately, and in respect of vaccination, the HSE notes that there are data sharing agreements in place with private hospitals for the purposes of vaccination[211] and that data collected will only be shared 'on a strict need to know basis for specific purposes relating to the management of the programme' and will only be accessed by,

- HSE staff involved in pre-vaccination, vaccine administration and post-vaccination tasks as well as general management of the programme,
- External professionals such as GPs and pharmacists in relation to their patients,
- Service providers administering vaccines,
- External suppliers for the purposes of managing and maintaining IT systems,

[210] HSE DP Impact Assessment for the COVID Tracker App, para 7.3.
[211] Vaccine Information System for COVID-19 Vaccination Programme (2021), p.9.

- The Health product regulatory authority for monitoring vaccine safety, and
- Other government agencies for the purposes of preparing anonymised statistical reports.

This description somewhat obfuscates whether such data is in fact shared with these bodies and parties or simply accessed by them but is also notably broad in its range. The list includes both public bodies – in the form of government Departments and the HPRA for example, as well as undefined list of 'service providers' specified as neither public nor private and a category of GPs and pharmacists whose relationship to the HSE may, similarly, be variously defined depending on their contractual status. Nor are the data sharing agreements with private hospitals alluded to in the HSE document available for inspection online at the time of writing. The extent to which individual data has already and may further diffuse through this network of actors is thus hard to gauge, as it the associated compliance with data protection principles.

The provisions of the Data Sharing Act would be illuminating if applied to this web of actors – though the Act will notably fail to capture data which is shared with bodies not defined as public in the terms of the Act, and s.9(1) in particular. There are thus vanishing points under the scope of the Act at which public health data can continue to be shared out of public view.

More fundamentally, and on the presumption that data has been both collected and processed on the correct legal basis, the issue which remains hardest to determine retrospectively is whether the requirement for proportionality was satisfied in sharing personal data during the pandemic and prior to the commencement of the relevant sections of the 2019 Act.

The requirement for proportionality in the processing of personal data has been emphasised, in particular, by the CJEU in *Digital Rights Ireland*.[212] In that case the Court emphasised that in processing personal data the emphasis should be on whether the means used was

[212] Case C-293/12 *Digital Rights Ireland* EU:C:2013:238.

appropriate to meet the legitimate objectives pursued by the legislation at issue, and whether it exceeded the limits of what was appropriate and necessary in order to achieve those objectives.

In this respect, it must of course be noted that the public health exemptions provided for in both the European Convention of Human Rights and the Charter of Fundamental Rights, as well as the public health basis for processing provided under the GDPR have remained untested prior to the current public health emergency. However, the HSE is given broad scope to respond to public health emergencies by s.7 of the Health Act 2004 which provides that "the object of the Executive is to use the resources available to it in the most beneficial, effective and efficient manner to improve, promote and protect the health and welfare of the public." Such provisions operate in addition to the powers provided under the Infectious Diseases Regulations 1981[213] (as amended) by virtue of the Infectious Diseases (Amendment) Regulations 2020.[214] In may be that the proportionality of sharing will thus be measured as against subsequent assessments as to the limits of public health exceptions and qualifications under European and ECHR law. However, present provision in Irish law mean that the any assessment of the existence, extent and proportionality of data sharing during the COVID-19 pandemic is difficult to assess.

Conclusion

The result of the existing legal landscape is that the extent to which data has been shared among public bodies, and which public bodies shared such data during the COVID-19 pandemic is difficult to gauge for those not actively involved in the system. While the broad principles of the operation of data sharing may be easily discernible – as the example of HSE, used here, illustrates – the practical operation of sharing is less clear.

The Data Sharing and Governance Act 2019 is well positioned to resolve this tension moving forward – at least in respect of the public bodies to which the act applies, and in respect of

[213] SI 390/1981.
[214] S.I. No. 53/2020.

certain categories of captured data. However, the Act will not resolve the issues with sharing between public bodies (as defined within the Act) and those actors outside its scope, an issue of particular importance given the sensitivity of public health data, and concerns in other jurisdictions about third party access to and processing of such data. Nor does the Act, absent the introduction of Ministerial Regulations, provide comprehensively for the sharing of health data in a manner which would clarify how such data is presently shared between the bodies covered by the legislation's provisions.

Moving forward, and in order to ensure that public health data is shared and processed in a manner which is secure, transparent and in the service of the public interest rather than private use, the following steps should be considered,

- Provision should be made without delay by way of Ministerial Regulations for the sharing of special category data concerning health and the governance of same under ss.63-66 of the Data Sharing and Governance Act 2019.
- Particular concern should be afforded to ensuring that the sharing of health data between public bodies is mapped in order to facilitate clarity about who has access to, and control of data within organisations and Departments, when and where data is being duplicated and, based on this information, how the security of such data and its sharing can be facilitated and ensured most effectively.
- Serious consideration should be given to the introduction of similar governance and transparency requirements for the sharing of public data, and in particular public health data, with third parties i.e., non-State actors.

DISCLAIMER

The information provided in this document is not legal advice or professional advice of any other kind, and should not be considered to be such, or relied or acted upon in that regard. If you need legal or other professional advice, you should consult a suitably qualified person.

To the extent permitted by law, Trinity College Dublin and the authors of this document, and their respective servants or agents, assume and accept no responsibility for, and give no guarantees, undertakings or warranties concerning, the accuracy, clarity, comprehensiveness, completeness, timeliness, fitness-for-purpose, up-to-date nature, reliability, or otherwise, of the information provided in this document, and do not accept any liability whatsoever in respect of, or arising from, any errors or omissions or any reliance on, or use of, such information.

Whilst we have taken reasonable care in preparing this document, to the extent permitted by law, we accept no responsibility for any loss or damage claimed to arise from any reliance on, or action taken by any person or organisation, wherever they are based, as a result, direct or otherwise, of, information contained in, or accessed through, this document, whether such information is provided by us or by a third party.